



HPE Aruba Networking EdgeConnect High Availability (HA) Deployment Guide



Hewlett Packard
Enterprise

July 2024
Rev E

Table of Contents

Copyright and Trademarks	3
Support	4
Related Documentation	4
About HPE Aruba Networking EdgeHA	5
Deploy EdgeHA	7
Set up Orchestrator by completing the following tasks	7
Enable IPsec UDP	7
Set up VRRP	9
Set up IP SLA	12
Set up the HA link	13
Enable EdgeHA in the deployment page	16
Set up OSPF with EdgeHA	18
Task list	19
Set up e-BGP routing on the WAN side	19
Set the admin distance	22
Set up OSPF routing on the LAN side	23
Troubleshooting	32
What happens when an appliance fails?	32



Copyright and Trademarks

EdgeConnect High Availability (HA) Deployment Guide

Date: July 2024

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba EULA](#).

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America



Support

For product and technical support, contact Support using any of the following methods:

1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com/support

We're dedicated to continually improving the usability of our products and documentation.

If you have suggestions or feedback for our documentation, send an e-mail to sp-techpubs@hpe.com.

Related Documentation

- EdgeConnect High Availability Getting Started Guide.
- EdgeConnect Traditional High Availability Deployment Guide.
- **Release Notes** provide information on new software features, system bugs, and software compatibility.
- All EdgeConnect SD-WAN Edge Platform documentation is available at <https://www.arubanetworks.com/website/techdocs/sdwan/>



About HPE Aruba Networking EdgeHA

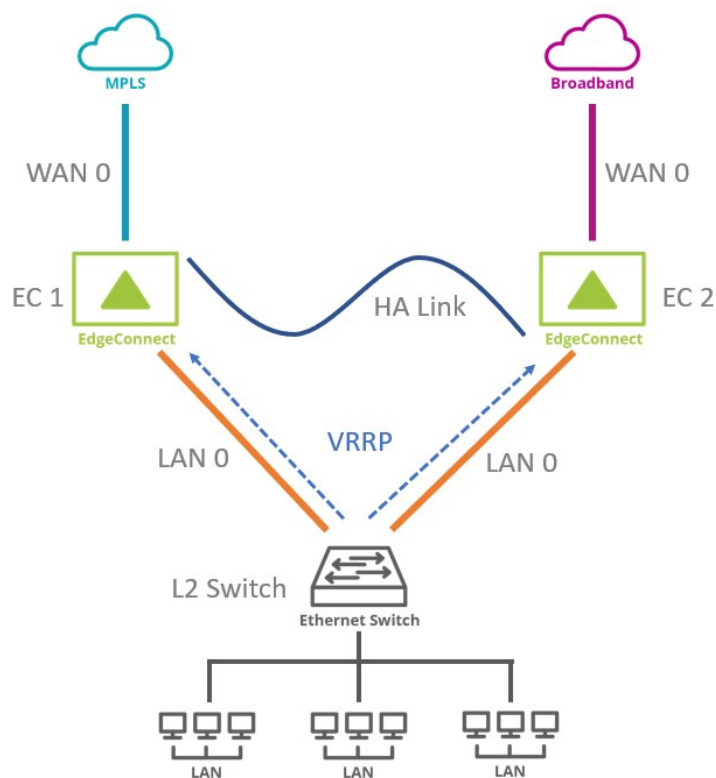
HPE Aruba Networking EdgeHA provides continuous, uninterrupted uptime in the event of a connection failure by using a pair of EdgeConnect appliances that are deployed in an active-standby setup. HPE Aruba Networking EdgeHA configurations are in-line router deployments.

An EdgeHA deployment has two EdgeConnect appliances connected by an HA (high availability) link, which the appliances use to share a single IP address on the WAN side and one public IP address for each service provider. The HA link is connected by an unused interface on each appliance.

EdgeHA does not need layer 2 switches between the EdgeConnect appliance and the service provider on the WAN side. EdgeHA also eliminates the need for additional equipment and setup for your high availability deployment.

NOTE An EdgeHA deployment does not support **mgmt** interfaces for the HA link between the EdgeConnect appliances.

NOTE If you are unsure if EdgeHA is the right choice for your organization, refer to the High Availability Getting Started Guide.



A typical EdgeHA configuration in a branch network.



When setting up your HPE Aruba Networking EdgeConnect devices for high availability, verify you meet the following requirements.

- The packet flow is symmetric.
- All packets should terminate on one or the other EdgeConnect appliance.
- VRRP accurately displays tunnel availability on the LAN-side.
- Each appliance is configured with the same site name.

TIP As an optional step, configure DHCP Relay on both EdgeConnect appliances.

WARNING HPE Aruba Networking does not support flow redirection with EdgeHA.



Deploy EdgeHA

Before you can configure high availability, make sure your Orchestrator is set up correctly.

- Use Orchestrator version 8.4 or later.
- Add at least two EdgeConnect appliances to Orchestrator.
- Use EdgeConnect version 8.1.7 or later.

Set up Orchestrator by completing the following tasks

The following tasks describe how to configure a sample EdgeHA in a branch. To set up an HA environment that is unique to your organization's needs, contact and work with your HPE Aruba Networking Technical Assistance Center (TAC) representative.

- [Enable IPsec UDP below](#)
- [Set up VRRP on page 9](#)
- [Set up IP SLA on page 12](#)
- [Enable EdgeHA in the deployment page on page 16](#)

Enable IPsec UDP

As part of your traditional HA deployment, enable IPsec UDP support in Orchestrator to provide IPsec encrypted protection. This is a one-time change that you do not need to set up for every site.

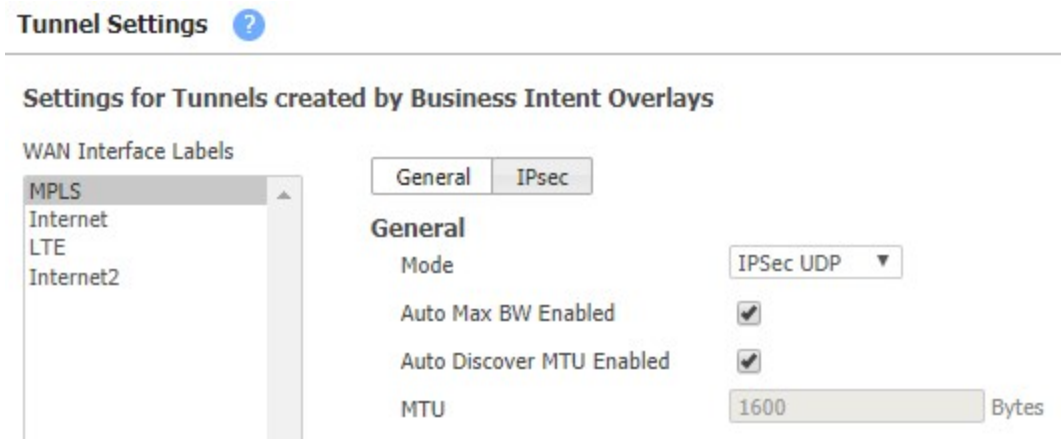
NOTE IPsec UDP mode is enabled by default on Orchestrator 8.2.0 or later. If you are upgraded from Orchestrator 8.1 or earlier, you must manually enable IPsec UDP mode by completing the following steps.

Complete the following steps to enable IPsec UDP.

1. From the Orchestrator main screen, select **Orchestrator**.
2. From **Tools**, select **Tunnel Settings**.
The Tunnel Settings screen displays.
3. Select the **General** tab.
4. From the **Mode** list, select **IPSec UDP**.



5. Select **Save**.



IPsec UDP tunnel settings.

Make sure each EdgeConnect appliance has a unique IPsec UDP port

Confirm Global Orchestrator settings increment port numbers

1. From the Orchestrator main screen, select **Orchestrator**.
2. From **Tools**, select **Orchestrator Settings**.
The Orchestration Settings screen displays.
3. In the **Default Port** field, enter a unique port number, such as port **12000**.
4. Click **Save** and go back to **Orchestrator Settings**.
5. In the Increment Port By field, enter a number, such as **1**, for ports to increment when tunnels must be built between common IP endpoints.
6. Select **Save**.



Orchestration Settings ? ×

Apply Overlays	<input checked="" type="checkbox"/>
Reset All Flows	<input type="checkbox"/>
Auto Save Appliance Changes	<input checked="" type="checkbox"/>
Apply Templates	<input checked="" type="checkbox"/>
Idle Time	<input type="text" value="60"/> Sec
Auto Flow Re-Classify	<input type="text" value="60"/> (0..65535) Sec
Inter-region Routing	<input type="checkbox"/>

IPSec UDP Settings

Default Port	<input type="text" value="12000"/>
Increment Port By	<input type="text" value="1"/>

IPsec UDP Orchestrator settings.

Change IPsec UDP port number on Device B

1. In the device tree, select Device B.
2. Navigate to Administration > System Settings.
3. Click the edit icon next to Device B. The System Settings window opens.
4. Change the IPsec UDP port number to 12100.
5. Click Apply.
6. Navigate to Configuration > Navigation > Tunnels.
7. Ensure that all underlay tunnels are UP for Device A and Device B and in IPsec mode.

Set up VRRP

Virtual Router Redundancy Protocol (VRRP) enables gateway redundancy on EdgeConnect appliances in a high availability (HA) deployment. Deploy the appliances in Router mode to use this feature.

VRRP often works in conjunction with subnet sharing when an appliance uses redundant HPE Aruba Networking appliances with Policy-Based Routing (PBR).



About VRRP priority

VRRP priority determines which EdgeConnect appliance is the initial VRRP master. In EdgeHA, configure VRRP for two EdgeConnect appliances with different VRRP priorities.

The EdgeConnect appliance with the higher VRRP priority is the master.

About VRRP preemption

After a failure occurs in the HA configuration, VRRP preemption determines that the EdgeConnect appliance with the highest priority assumes primary responsibility after coming back online.

Example: You have two EdgeConnect appliances, **EC1** and **EC2**. **EC1** has the higher priority value.

1. If **EC1** goes down but **EC2** is still up, **EC2** becomes the master.
2. When **EC1** is available again and **EC2** is still up, **EC1** takes over as the master because preemption is on.

To decide whether you should enable preemption, consider the following.

- If both of your HA appliances have identical resources, such as CPU and memory, turn preemption off. This is the recommended use case.
- If your HA appliances have different resources or licensing, if the original VRRP master is available again, a lack of resources or different licensing can cause flow resets and service disruptions.



Set up VRRP with different priority levels

Set up VRRP on two EdgeConnect appliances with the first appliance having the higher priority level.

Enable VRRP on the first EdgeConnect appliance

1. From the Orchestrator main screen, select **Configuration**.
2. Under **NETWORKING**, select **VRRP**.
The VRRP screen displays.
3. Select the pencil icon next to the first EdgeConnect appliance that you want to configure with VRRP.
A new configuration screen displays.
4. Select **Add VRRP**.
5. In the **Group ID** field, enter a number, such as **1**.
6. From the **Interface** list, select **lan0**.
7. In the **Virtual IP** field, type an IP address for the VRRP group.
8. In the **Priority** field, type a number for the VRRP priority for this appliance, such as **129**.
9. For **Preemption**, if your appliances have the same resources and licensing, deselect the check box.
10. Select **Apply**.

Enable VRRP on the second EdgeConnect appliance

1. From the Orchestrator main screen, select **Configuration**.
2. Under **NETWORKING**, select **VRRP**.
The VRRP screen displays.
3. Select the pencil icon next to the first EdgeConnect appliance that you want to configure with VRRP.
A new configuration screen displays.
4. Select **Add VRRP**.
5. In the **Group ID** field, enter a number, such as **1**.
6. From the **Interface** list, select **lan0**.
7. In the **Virtual IP** field, type an IP address for the VRRP group.
8. In the **Priority** field, type a number smaller than 129, such as **128**.
9. For **Preemption**, if your appliances have the same resources and licensing, deselect the check box.
10. Select **Apply**.



VRRP ?

Add VRRP

2 Rows, 1 Selected

Group ID	Interface ▲	State	Admin	Virtual IP	Advertisement Timer	Priority Config	Priority State
1	lan0 ▼	master	Up		1	129	129
2	lan0	backup	Up		1	128	128

EC1 has the higher VRRP priority.

Set up IP SLA

An IP SLA rule monitors the VRRP state on the LAN side of the EdgeHA high availability set up. The state is either true if the VRRP on an interface is the master, or false if the VRRP is in another state, such as **backup** or **init**.

If an appliance fails on the LAN-side, then IP SLA either increases the subnet metrics or lowers the VRRP priority.

NOTE Set up IP SLA only if you are using VRRP.

1. From the Orchestrator main screen, select **Configuration**.
2. From **TCAs**, select **IP SLA**.
The IP SLA screen displays.
3. Select the pencil icon next to the first EdgeConnect appliance.
A new screen displays.
4. Select **Add**.
The IP SLA Rule screen displays.
5. From the **Monitor** list, select **VRRP Monitor**.
6. From the **Interface** list, select an interface that you configured for VRRP, such as **lan1**.
7. In the **Monitor Sampling Interval** field, enter **1**.
8. From the **Down Action** list, select **Modify Subnet Metric**.
9. In the **Delta** field, enter a number greater than or equal to **2**.

The number you enter depends on your Subnet Sharing metrics and your fail-over and fail-back behavior.



10. From the **Up Action** list, select **Default Subnet Action**.
11. In the **Comment** field, enter an optional, descriptive comment.
12. Select **Add**.
The screen closes.
13. Select **Apply**.
14. Repeat the previous steps for the second EdgeConnect appliance.

IP SLA Rule

ON
OFF

Monitor

Monitor ▼

Interface ▼

Monitor Sampling Interval Sec

Actions

Down Action ▼

Delta

Up Action ▼

Comment

IP SLA rule.

Set up the HA link

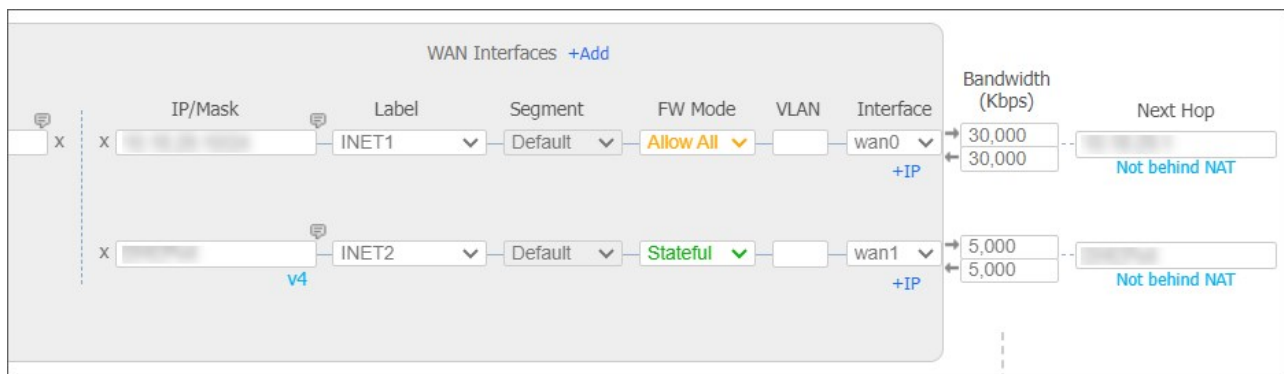
An HA link connects two EdgeConnect appliances in an EdgeHA deployment. When an appliance turns off or goes offline, traffic from the appliance fails over through the HA link to the other appliance. Setting up the HA link requires you to set a VLAN for each interface label.

TIP To see details of the HA link and the EdgeConnect appliance deployment, right-click an appliance in Orchestrator and select **Appliance Manager**. You can also verify the appliance site names are identical from the Initial Config Wizard by selecting **Configuration > System and Networking > Initial Config Wizard** from the Appliance Manager.



Set up the WAN interface of the first appliance.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **Deployment**.
The Deployment screen displays.
3. Select the pencil icon next to your first EdgeConnect appliance.
A new screen displays.
4. On the **WAN Interfaces** side of the deployment screen, make sure there are two interfaces. If there is only one interface, select **+Add**.
5. In the **IP/Mask** fields, enter an IPv4 address and subnet mask for each WAN interface.
6. From the **Label** list, select an option from the drop-down menu, such as **INET1**, for the first interface and another option, such as **INET2**, for the second interface.
7. Leave the **FW Zone** lists as **Default**.
8. From the **FW Mode** list, select **Allow All** for the first interface. In this example, for the interface with the INET1 label.
9. From the **FW Mode** list, select **Stateful+SNAT** for the second interface. In this example, for the interface with the INET2 label.
10. In the **VLAN** field, enter **100** for the interface with the Internet label.
11. In the **Bandwidth** fields, enter values for the bandwidth of each interface.
12. In the **Next Hop** fields, enter the IPv4 address of each interface's next hop. The **wan1** next hop is the peer appliance IP for the HA link.
13. Select **Apply**.



An HA deployment example.



Set up the WAN interface of the second appliance.

1. From the Orchestrator main screen, select **Configuration**.

2. From **NETWORKING**, select **Deployment**.

The Deployment screen displays.

3. Select the pencil icon next to your second EdgeConnect appliance.

A new screen displays.

4. On the **WAN Interfaces** side of the deployment screen, make sure there are two interfaces. If there is only one interface, select **+Add**.

5. In the **IP/Mask** fields, enter an IPv4 address and subnet mask for each WAN interface.

6. From the **Label** list, select an option from the drop-down menu, such as **MPLS1**, for the first interface and another option, such as **MPLS2**, for the second interface.

NOTE When assigning labels to the secondary appliance they must differ from the labels used for the primary appliance. If the same labels are assigned for both appliances an error message is displayed.

7. Leave the **FW Zone** lists as **Default**.

8. From the **FW Mode** list, select **Allow All** for the first interface. In this example, the interface with the MPLS1 label.

9. From the **FW Mode** list, select **Stateful+SNAT** for the second interface. In this example, the interface with the MPLS2 label.

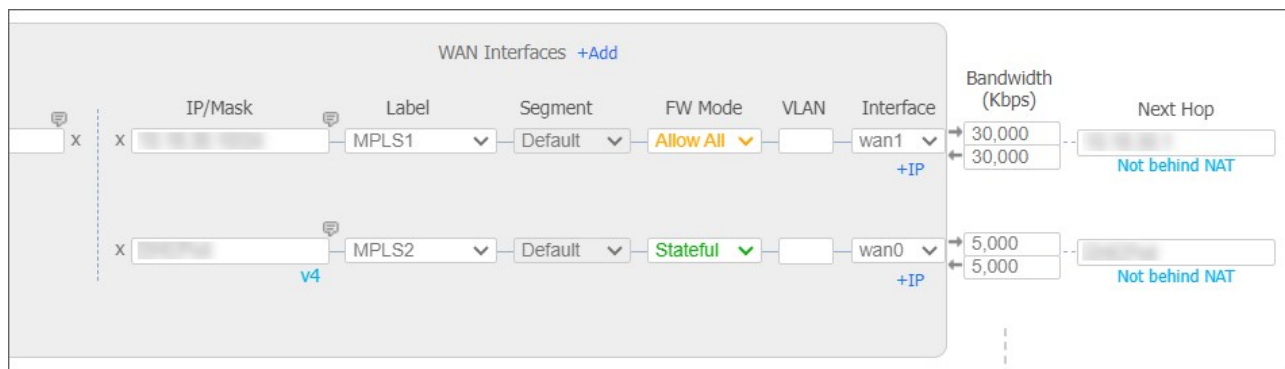
10. In the **VLAN** field, enter **101** for the interface with the Internet label.

11. In the **Bandwidth** fields, enter values for the bandwidth of each interface.

12. In the **Next Hop** fields, enter the IPv4 address of each interface's next hop. The wan1 next hop is the peer appliance IP for the HA link.

13. Select **Apply**.





An HA deployment example.

Enable EdgeHA in the deployment page

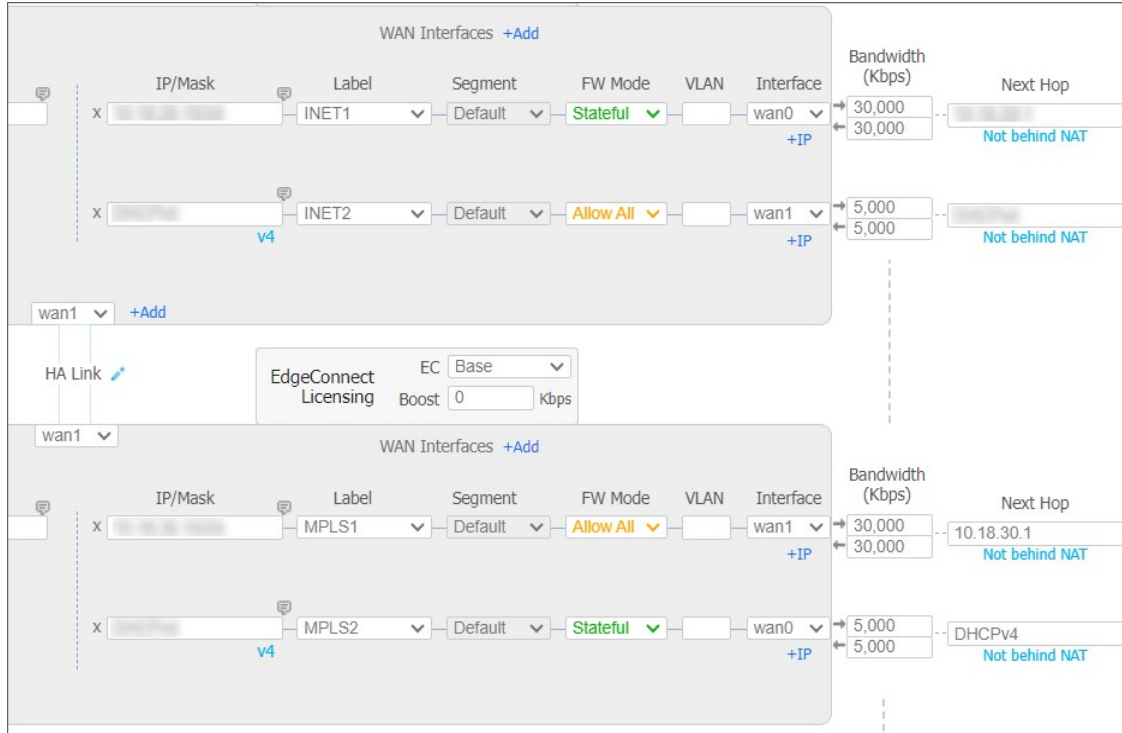
Enable EdgeHA in HPE Aruba Networking Orchestrator. Configure one of your two EdgeConnect appliances to create a high availability link between the two appliances.

NOTE Do not set up HA by selecting the appliance in **Tree View**.

NOTE Configure the LAN and WAN interfaces for both appliances and verify both appliances are in Router mode.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **Deployment**.
The Deployment screen displays.
3. Select the pencil icon next to your first EdgeConnect appliance.
A new screen displays.
4. Select the **EdgeConnect HA** check box.
An online help screen displays.
5. Close the help screen.
6. From the **HA Peer** list, select your second EdgeConnect appliance as a peer.
A second deployment section displays with an HA link in between the two sections.
7. Select **Apply**.





An HA deployment profile example.



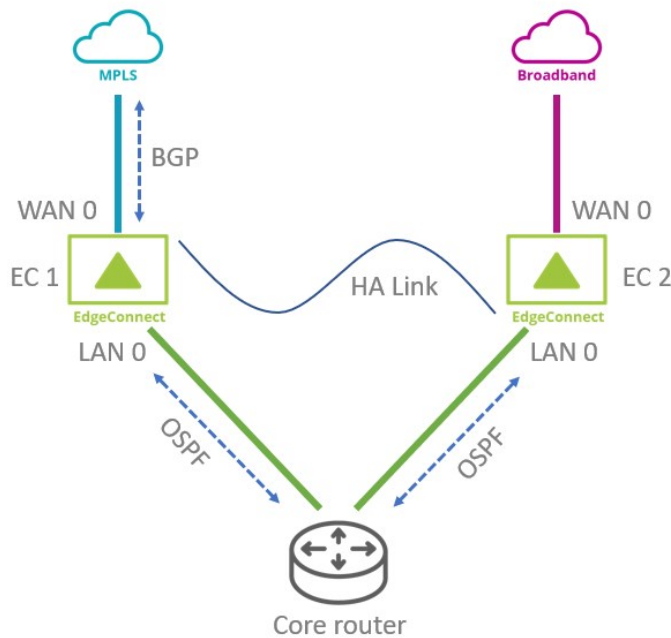
Set up OSPF with EdgeHA

This scenario describes how to set up OSPF as an option in your EdgeHA environment.

OSPF replaces VRRP in an EdgeHA deployment. Make sure you pay attention to the following.

Make sure you enable IPsec UDP.

Do not set up VRRP or create an IP SLA.



Traditional HA configuration with OSPF.

The following table shows an example of OSPF parameters in a sample traditional HA configuration.

	EdgeConnect appliance 1 (EC 1)	EdgeConnect appliance 2 (EC 2)
Tag	100	100
Filter	100	100
Cost	10	20
Redistribution metric	50	70



Task list

Complete the following tasks to set up OSPF.

- [Set up e-BGP routing on the WAN side below](#)
- [Set the admin distance on page 22](#)
- [Set up OSPF routing on the LAN side on page 23](#)

Set up e-BGP routing on the WAN side

Set up an external Border Gateway Protocol (EBGP) configuration on the WAN side MPLS network. The EdgeHA configuration redistributes OSPF routes learned from the LAN side to the BGP. BGP routes are also redistributed to OSPF when connecting to non-service provider sites.

Set up BGP.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **BGP**.
The BGP screen displays.
3. Select the pencil icon next to the EdgeConnect appliance that connects to the MPLS network.
A new screen displays.
4. Slide the **Enable BGP** option to the right.
5. In the **Autonomous System Number** field, enter a number for the autonomous system.
6. In the **Router ID** field, enter an IPv4 address.
7. For **Redistribute OSPF routes to BGP**, select the check box to enable subnet sharing of OSPF routes.



BGP Information ?

Enable BGP	<input checked="" type="checkbox"/>
Autonomous System Number	<input type="text" value="1"/>
Router ID	<input type="text" value=""/>
Redistribute OSPF routes to BGP	<input checked="" type="checkbox"/>
Filter Tag	<input type="text" value="0"/>

Basic BGP information.

Add BGP peers.

1. Select **Add**.
2. In the **Peer IP** field, enter a name for the for the BGP peer.
3. In the **Peer ASN** field, enter a number for the BGP autonomous system number.
4. For **Enable Imports**, select the check box to allow learned routes from this BGP peer.
5. From the **Peer Type** list, select **PE-Router** as the type of route that appliances are allowed to advertise to this BGP peer.
6. In the **Local Preference** field, enter the default value, **100**.
7. In the **MED** field, enter a number if two or more routes have the same local preference length and AS path length. The route with the lower value is the preferred route.
8. In the **AS Prepend Count** field, enter a number to allow the advertising device to increment the AS path count with a local AS number.
9. In the **Input Metric** field, enter a number that is advertised when the route is shared.
10. In the **Keep Alive Timer** field, enter a number that specifies the interval, in seconds, between keep alive signals to a peer.
11. In the **Hold Timer** field, enter a number that specifies how long to wait before dropping a session when a peer can't be reached.



Add Peer

Peer IP	<input type="text" value="192.168.1.4"/>
Peer ASN	<input type="text" value="23"/>
Enable Imports	<input checked="" type="checkbox"/>
Peer Type	<input type="text" value="PE-router"/>
Admin Status	<input type="button" value="UP"/> <input type="button" value="DOWN"/>
Local Preference	<input type="text" value="100"/>
MED	<input type="text" value="0"/>
AS Prepend Count	<input type="text" value="0"/> (0..10)
Input Metric	<input type="text" value="0"/>
Keep Alive Timer*	<input type="text" value="30"/> (0..65535) Sec
Hold Timer*	<input type="text" value="90"/> (0..65535) Sec

* Timer changes only take effect when BGP session is reset.
Admin Down, Up for changes to take effect immediately.

BGP configuration with PE-router peer type.

Specify advertising routes.

1. Navigate to the **Route Export Policies for Peer Type** section.
2. Select **Use Defaults**.



Route Export Policies for Peer Type: PE-router	Use Defaults
1. Locally configured	<input checked="" type="checkbox"/>
2. Learned via subnet sharing	<input type="checkbox"/>
3. Learned from a local BGP branch peer	<input checked="" type="checkbox"/>
4. Learned from a local BGP branch-transit peer	<input checked="" type="checkbox"/>
5. Learned from a local BGP PE router	<input type="checkbox"/>
6. Remote BGP (learned via subnet sharing, but originally from a BGP peer)	<input type="checkbox"/>
7. Remote BGP branch-transit peer (learned via subnet sharing, but originally a BGP-transit peer)	<input type="checkbox"/>
8. Learned from a local OSPF peer	<input checked="" type="checkbox"/>
9. Learned from a Remote OSPF peer	<input type="checkbox"/>

Route export policies.

Optional: Enable MD5 password to authenticate the TCP session with the BGP peer.

1. Select the **Enable MD5 Password** check box.
2. In the **Password** field, enter a password.
3. In the **Confirm Password** field, re-enter the password.

Set the admin distance

Set the admin distance so subnets shared over BGP-PE is the preferred option. This ensures that traffic routes to a remote HPE Aruba Networking location through HPE Aruba Networking bonded tunnels instead of MPLS.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **Admin Distance**.
The Admin distance screen displays.
3. Select the pencil icon next to the EdgeConnect appliance with BGP enabled.
A new screen displays.



- For the BGP PE field, enter a number higher than the other subnet shared routes in the list.
- Select **Apply**.

Admin Distance ?

8 Rows, 1 Selected		Search <input type="text"/>
Type	Distance ▲	
Local		1
Subnet Shared - Static Routes		10
BGP Branch		20
BGP Transit		20
OSPF		20
Subnet Shared - BGP Remote		20
Subnet Shared - OSPF Remote		20
BGP PE	<input type="text" value="25"/>	

Admin distance with BGP PE set to the highest value.

Set up OSPF routing on the LAN side

The EdgeConnect appliance acts like an autonomous system border router (ASBR), redistributing routes from both the HPE Aruba Networking subnet sharing fabric and the BGP learned routes into the OSPF domain with the core routers.

Set up OSPF on the first EdgeConnect appliance

Set the OSPF metric, type, and tag.

- From the Orchestrator main screen, select **Configuration**.
- From **NETWORKING**, select **OSPF**.

The OSPF screen displays.

- Select the pencil icon next to the EdgeConnect appliance that connects to the MPLS network.

A new screen displays.



4. Select the **Enable OSPF** check box.
The previously greyed out sections are enabled.
5. In the **Router ID** field, enter an IP address that the remote peer uses to identify the EC1 appliance.
6. For **Redistribute BGP routes to OSPF**, select the check box.
 1. For **Metric Type**, select **E1**.
 2. For **Metric**, leave the value as **0**.
 3. For **Tag**, enter a tag value for route distribution by the appliance to the core, such as **100**.
7. For **Redistribute Silver Peak peers routes to OSPF**, select the check box.
 1. For **Metric Type**, select **E1**.
 2. For **Metric**, leave the value as **0**.
 3. For **Tag**, enter a tag value for route distribution by the appliance to the core, such as **100**.
8. For **Redistribute local routes to OSPF**, select the check box.
 1. For **Metric Type**, select **E1**.
 2. For **Metric**, leave the value as **0**.
 3. For **Tag**, enter a tag value for route distribution by the appliance to the core, such as **100**.
9. Select **Apply**.

OSPF ?

Enable OSPF	<input checked="" type="checkbox"/>
Router ID	192.168.1.1
Redistribute BGP routes to OSPF	<input checked="" type="checkbox"/>
Metric Type	E1 ▾
Metric	0
Tag	100
Redistribute Silver Peak peers routes to OSPF	<input checked="" type="checkbox"/>
Metric Type	E1 ▾
Metric	0
Tag	100
Redistribute local routes to OSPF	<input checked="" type="checkbox"/>
Metric Type	E1 ▾
Metric	0
Tag	100

OSPF configuration.



Add an interface.

1. Select **Add**.

The Add Interface screen displays.

2. From the **Interface** list, select **lan0**.
3. In the **Area ID** field, enter the area number that specifies the area where the interface is located.
4. In the **Cost** field, enter a number that specifies the overhead required to send packets across an interface, such as **10**.

The EdgeConnect with the lower number is the preferred route for outbound traffic. In this example, EC1, with a cost of 10, is the preferred route.

5. In the **Priority** field, enter a number that specifies the router priority level.
6. For **Admin Status**, specifies whether the interface is set to admin **UP** or **DOWN**.
7. In the **Hello Interval** field, enter a number that specifies the time, in seconds, between the hello packets that a router sends to an OSPF interface.
8. In the **Dead Interval** field, enter a number that specifies the number of seconds that a router's hello packets have not been seen before its neighbors determine the OSPF router as down.
9. In the **Transmit Delay** field, enter a number that specifies the number of seconds needed to transmit a link state update packet.
10. In the **Retransmit Interval** field, enter a number that specifies the number of seconds between retransmissions.
11. From the **Authentication** list, select the type of encryption for the OSPF interface.
12. In the **Comment** field, enter an option text comment about this interface.
13. Select **Add**.



Add Interface ✕

Interface	<input type="text" value="lan0"/>
Area ID	<input type="text" value="0.0.0.0"/> = 0
(Area ID is the same for all interfaces. It can be an integer between 0 and 4294967295, or it can take a form similar to an IP address, A.B.C.D.)	
Cost	<input type="text" value="10"/>
Priority	<input type="text" value="1"/>
Admin Status	<input checked="" type="button" value="UP"/> <input type="button" value="DOWN"/>
Hello Interval	<input type="text" value="10"/> (1..65535) Sec
Dead Interval	<input type="text" value="40"/> (1..65535) Sec
Transmit Delay	<input type="text" value="1"/> (1..450) Sec
Retransmit Interval	<input type="text" value="4"/> (1..65535) Sec
Authentication	<input type="text" value="None"/>
Comment	<input type="text"/>

Add an OSPF interface.

Set filtering metrics.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **Routes**.
The Routes screen displays.
3. Select the pencil icon next to the first EdgeConnect appliance.
A new screen displays.
4. For **Redistribute OSPF routes to Silver Peak peers**, select the check box.
5. For **Metric**, enter a number for the redistribution metric, such as **50**.

Setting a lower redistribution metric on EC1 ensures that the traffic returning from a remote location routes to the local primary EC. This ensures symmetric traffic flow.

6. For **Filter Tag**, enter a number to filter tags.
7. Select **Apply**.



Routes

Use shared subnet information	<input checked="" type="checkbox"/>
Automatically advertise local LAN subnets	<input checked="" type="checkbox"/>
Automatically advertise local WAN subnets	<input type="checkbox"/>
Metric for automatically added subnets	<input type="text" value="50"/>
Redistribute OSPF routes to Silver Peak peers	<input checked="" type="checkbox"/>
	<input type="text" value="50"/>
	<input type="text" value="100"/>

Add route metric and filter tag.

Set up OSPF on the second EdgeConnect appliance

Set the OSPF metric, type, and tag.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **OSPF**.
The OSPF screen displays.
3. Select the pencil icon next to the EdgeConnect appliance that connects to an internet service provider.
A new screen displays.
4. Select the **Enable OSPF** check box.
The previously greyed out sections are enabled.
5. In the **Router ID** field, enter an IP address that the remote peer uses to identify the EC2 appliance.
6. For **Redistribute BGP routes to OSPF**, select the check box.
 1. For **Metric Type**, select **E2**.
 2. For **Metric**, leave the value as **0**.
 3. For **Tag**, enter a tag value for route distribution by the appliance to the core.



7. For **Redistribute Silver Peak peers routes to OSPF**, select the check box.
 1. For **Metric Type**, select **E2**.
 2. For **Metric**, leave the value as **0**.
 3. For **Tag**, enter a tag value for route distribution by the appliance to the core.
8. For **Redistribute local routes to OSPF**, select the check box.
 1. For **Metric Type**, select **E2**.
 2. For **Metric**, leave the value as **0**.
 3. For **Tag**, enter a tag value for route distribution by the appliance to the core, such as **100**.
9. Select **Apply**.

OSPF ?

Enable OSPF	<input checked="" type="checkbox"/>
Router ID	<input type="text" value="192.168.1.1"/>
Redistribute BGP routes to OSPF	<input checked="" type="checkbox"/>
Metric Type	<input type="text" value="E2"/>
Metric	<input type="text" value="0"/>
Tag	<input type="text" value="100"/>
Redistribute Silver Peak peers routes to OSPF	<input checked="" type="checkbox"/>
Metric Type	<input type="text" value="E2"/>
Metric	<input type="text" value="0"/>
Tag	<input type="text" value="100"/>
Redistribute local routes to OSPF	<input checked="" type="checkbox"/>
Metric Type	<input type="text" value="E2"/>
Metric	<input type="text" value="0"/>
Tag	<input type="text" value="100"/>

OSPF configuration.

Add an interface.

1. Select **Add**.
The Add Interface screen displays.
2. From the **Interface** list, select **lan0**.
3. In the **Area ID** field, enter a number or an IP address that specifies the area where the interface is located.



4. In the **Cost** field, enter a number larger than what you entered for the first appliance, such as **20**.
The EdgeConnect with the lower number is the preferred route for outbound traffic.
5. For **Admin Status**, specifies whether the interface is set to admin **UP** or **DOWN**.
6. In the **Hello Interval** field, enter a number that specifies the time, in seconds, between the hello packets that a router sends to an OSPF interface.
7. In the **Dead Interval** field, enter a number that specifies the number of seconds that a router's hello packets have not been seen before its neighbors determine the OSPF router as down.
8. In the **Transmit Delay** field, enter a number that specifies the number of seconds needed to transmit a link state update packet.
9. In the **Retransmit Interval** field, enter a number that specifies the number of seconds between retransmissions.
10. From the **Authentication** list, select the type of encryption for the OSPF interface.
11. In the **Comment** field, enter an option text comment about this interface.
12. Select **Add**.



Add Interface



Interface	<input type="text" value="lan0"/>
Area ID	<input type="text" value="0.0.0.0"/> = 0
(Area ID is the same for all interfaces. It can be an integer between 0 and 4294967295, or it can take a form similar to an IP address, A.B.C.D.)	
Cost	<input type="text" value="20"/>
Priority	<input type="text" value="1"/>
Admin Status	<input checked="" type="checkbox"/> UP <input type="checkbox"/> DOWN
Hello Interval	<input type="text" value="10"/> (1..65535) Sec
Dead Interval	<input type="text" value="40"/> (1..65535) Sec
Transmit Delay	<input type="text" value="1"/> (1..450) Sec
Retransmit Interval	<input type="text" value="4"/> (1..65535) Sec
Authentication	<input type="text" value="None"/>
Comment	<input type="text"/>

Add an OSPF interface.

Set filtering metrics.

1. From the Orchestrator main screen, select **Configuration**.
2. From **NETWORKING**, select **Routes**.
The Routes screen displays.
3. Select the pencil icon next to the first EdgeConnect appliance.
A new screen displays.
4. For **Redistribute OSPF routes to Silver Peak peers**, select the check box.
5. For **Metric**, enter a number for the redistribution metric that is larger than the one you entered for the first appliance, such as **70**.
6. For **Filter Tag**, enter a number to tag routes, such as **100**.
7. Select **Apply**.



Routes ?

Use shared subnet information	<input checked="" type="checkbox"/>
Automatically advertise local LAN subnets	<input checked="" type="checkbox"/>
Automatically advertise local WAN subnets	<input type="checkbox"/>
Metric for automatically added subnets	<input type="text" value="50"/>
Redistribute OSPF routes to Silver Peak peers	<input checked="" type="checkbox"/>
	<input type="text" value="70"/>
	<input type="text" value="100"/>

Add route metric and filter tag.



Troubleshooting

Try using the following suggestions when troubleshooting issues that occur in an EdgeHA deployment.

- Make sure your EdgeHA deployment has symmetric flow by completing the following steps.
 1. In the Orchestrator main screen, select **Monitoring > Active & Recent Flows** .
 2. Under **Bytes Transferred**, select **Last 5m**.
 3. Highlight the HA appliances.
 4. Under both **Inbound Bytes** and **Outbound bytes**, check for flows with 0 bytes.
 5. If a flow has 0 outbound bytes, then the LAN interface of the appliance where the flow originates is not receiving traffic.
 6. If a flow as 0 inbound bytes, then the remote appliance is either not receiving traffic or sending the traffic to the wrong appliance. Check the flows on the remote appliance in the outbound tunnel for the same flow.
 7. If there are no outbound bytes, check the LAN device to make sure the traffic is redirected.
 8. If there are outbound bytes to the other HA appliance, the route metric is not preferred properly.
- Changing ports in Orchestrator won't change the same ports on EdgeConnect appliances that use site names. To work around this issue, change the UDP port field In Orchestrator.
- To monitor the health of the tunnels, look up the **ipsec_udp** flows in the other EdgeConnect appliance's flow table.
- Changing the Tunnel Health Retry count and the Flow Reclassification value to small numbers can reduce failover time.
- If your Orchestrator version is earlier than 8.2.x, manually add **169.254.0.0/16** to your list of internal subnets. This prevents problems with VLANs and next hop gateway unreachable alarms. Later versions list 169.254.0.0/16 as a default subnet.

What happens when an appliance fails?

Try using the following suggestions to troubleshoot an appliance failure.

- During a high availability deployment, one or more EdgeConnect appliances might fail or experience downtime.
- Change the IP SLA delta value to a number greater than or equal to **2**. Otherwise, the subnet sharing doesn't converge quickly.



- Change the value of the secondary appliance to a number lower than the value of the primary appliance. The appliance sending the traffic can then use the proper tunnel with faster speed and efficiency.

