silver peak®

Silver Peak

# Unity EdgeConnect High Availability (HA) Deployment Guide

**April 11, 2022**
**Rev B**

# Table of Contents

# Copyright and Trademarks

EdgeConnect High Availability (HA) Deployment Guide

Date: April 2022

**Trademark Notification**

**Warranties and Disclaimers**

Silver Peak Systems, Inc.
2860 De La Cruz Boulevard
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support

# Support

For product and technical support, contact Silver Peak Systems at either of the following:

**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 techpubs@silver-peak.com.

- If you have comments or feedback about the interface, send an e-mail to usability@silver-peak.com.

# Related Documentation

- Silver Peak High Availability Getting Started Guide.

- Silver Peak Traditional High Availability Deployment Guide.

- **Release Notes** provide information on new software features, system bugs, and software compatibility.

- All user documentation is available at https://www.silver-peak.com.

# About Silver Peak EdgeHA

Silver Peak EdgeHA provides continuous, uninterrupted uptime in the event of a connection failure by using a pair of Silver Peak EdgeConnect appliances that are deployed in an active-standby setup. Silver Peak 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 Silver Peak 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 Silver Peak EdgeHA Getting Started Guide.
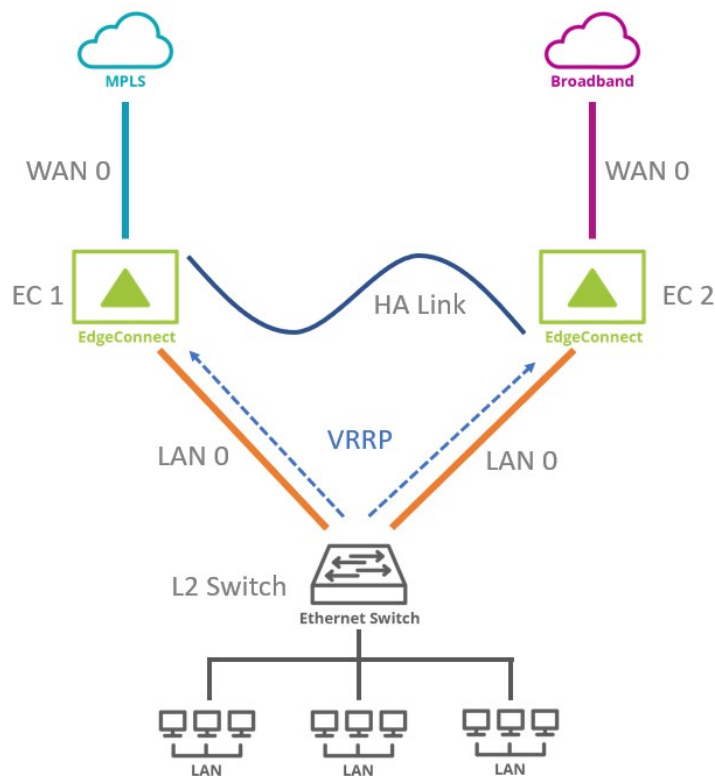


*Figure 1: A typical EdgeHA configuration in a branch network.*

When setting up your Silver Peak 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 a different site name.

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

**WARNING**  Silver Peak 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 Silver Peak Technical Assistance Center (TAC) representative.

- Enable IPsec UDP

- Set up VRRP

- Set up IP SLA

- Enable EdgeHA in the deployment page

# 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** Silver Peak 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**.
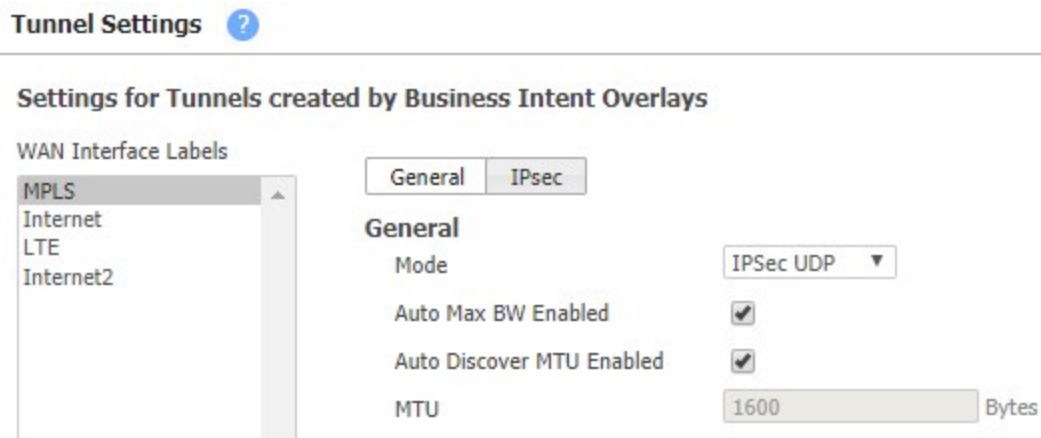


*Figure 2: IPsec UDP tunnel settings.*

## 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**.



*Figure 3: 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 Silver Peak 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**.



*Figure 4: 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 | VRRP Monitor ▼ |
| Interface | lan0 ▼ |
| Monitor Sampling Interval | 1 | Sec |

Actions

| Down Action | Modify Subnet Metric ▼ |
| Delta | 2 |
| Up Action | Default Subnet Action ▼ |
| Comment | optional |

*Figure 5: 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 different from the Initial Config Wizard by selecting **Configuration > System and Networking > Initial Config Wizard** from the Appliance Manager. If the devices have identical site names, the HA device links will be created with each other with unpredictable behavior until the site-name is re-configured post deployment.

## 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 **MPLS** for the first interface and **Internet** for the second interface.

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

8. From the **FW Mode** list, select **Allow All** for the interface with the MPLS label.

9. From the **FW Mode** list, select **Stateful+SNAT** for the interface with the Internet 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.
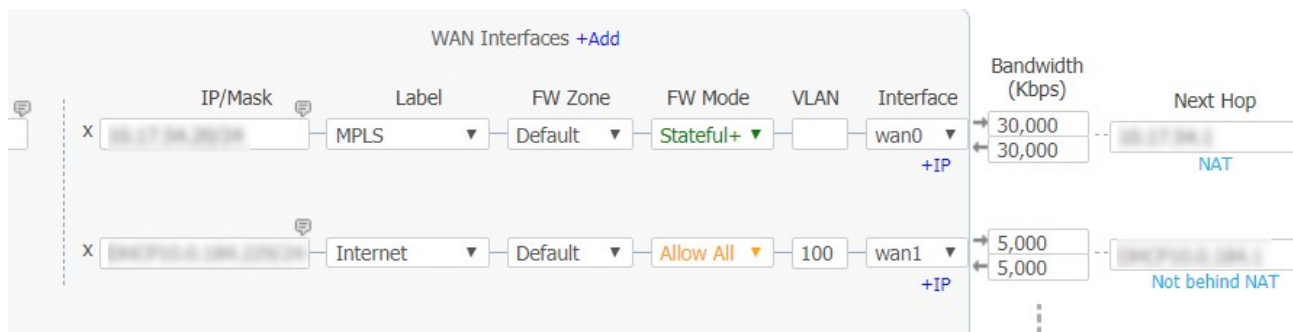
13. Select **Apply**.

*Figure 6: 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 **MPLS** for the first interface and **Internet** for the second interface.

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

8. From the **FW Mode** list, select **Allow All** for the interface with the MPLS label.

9. From the **FW Mode** list, select **Stateful+SNAT** for the interface with the Internet 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.
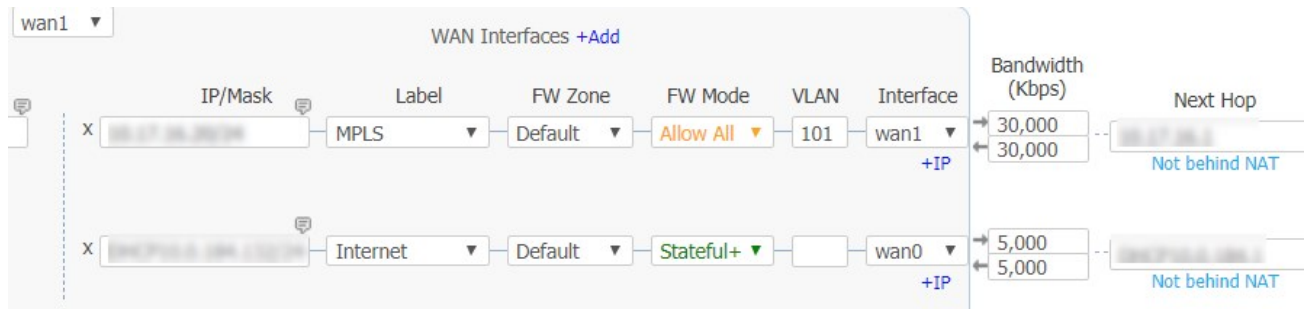
13. Select **Apply**.

*Figure 7: An HA deployment example.*

# Enable EdgeHA in the deployment page

Enable EdgeHA in Silver Peak 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**  Make sure to configure the LAN and WAN interfaces for both appliances and make sure 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.
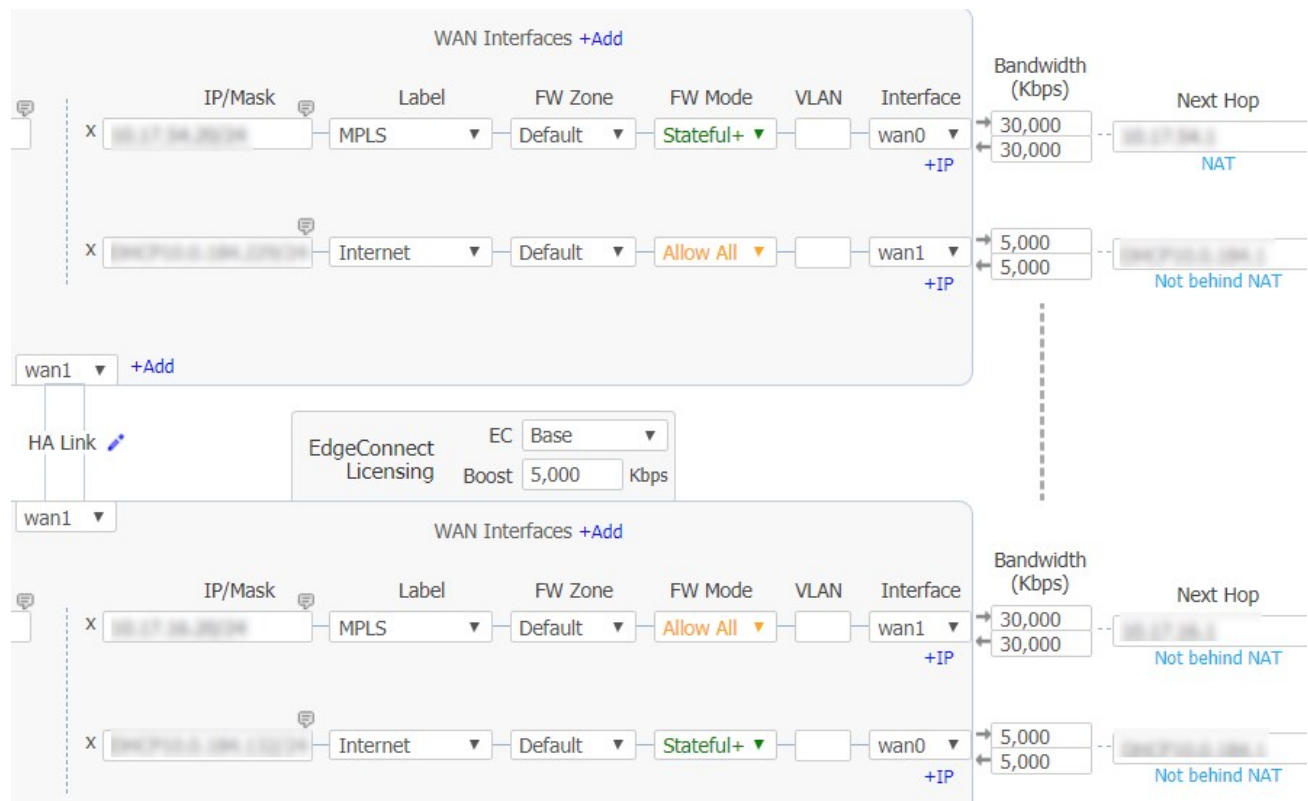
7. Select **Apply**.

*Figure 8: 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.
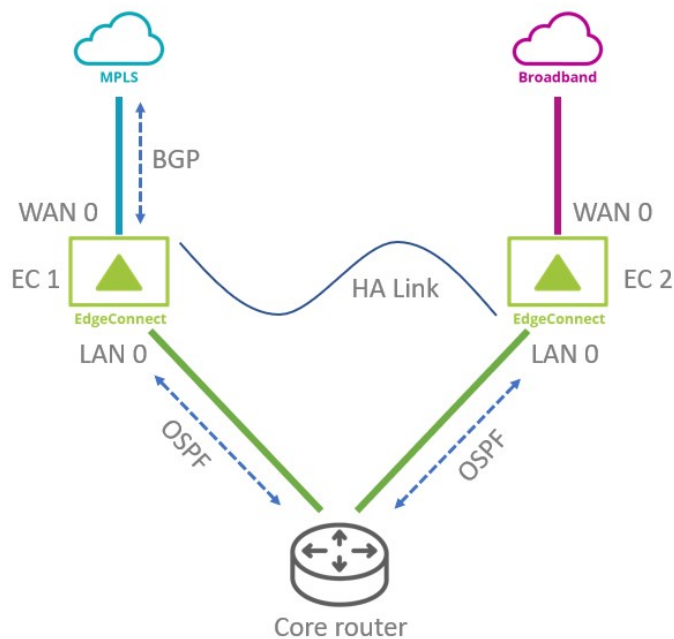
- Do not set up VRRP or create an IP SLA.

*Figure 9: 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

- Set the admin distance

- Set up OSPF routing on the LAN side

# 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.



*Figure 10: 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.



*Figure 11: 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**.

Figure 12: 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 Silver Peak location through Silver Peak 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.

4. For the BGP PE field, enter a number higher than the other subnet shared routes in the list.

5. Select **Apply**.

## Admin Distance ❓

| 8 Rows, 1 Selected | Search | |
|---|---|
| **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 | 25 |

*Figure 13: Admin distance with BGP PE set to the highest value.*

# Set up OSPF routing on the LAN side

The Silver Peak appliance acts like an autonomous system border router (ASBR), redistributing routes from both the Silver Peak 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.

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 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**.

*Figure 14: 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**.



*Figure 15: 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**.



*Figure 16: 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**.



*Figure 17: 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 sof 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 | lan0 ▾ |
| Area ID | 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 | 20 | |
| Priority | 1 | |
| Admin Status | UP   DOWN | |
| Hello Interval | 10 | (1..65535) Sec |
| Dead Interval | 40 | (1..65535) Sec |
| Transmit Delay | 1 | (1..450) Sec |
| Retransmit Interval | 4 | (1..65535) Sec |
| Authentication | None ▾ | |
| Comment | | |

*Figure 18: 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 | ☑ |
| Automatically advertise local LAN subnets | ☑ |
| Automatically advertise local WAN subnets | ☐ |
| Metric for automatically added subnets | 50 |
| Redistribute OSPF routes to Silver Peak peers | ☑ |
| Metric | 70 |
| Filter Tag | 100 |

*Figure 19: 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.

    a. In the Orchestrator main screen, select **Monitoring** > **Active & Recent Flows** .

    b. Under **Bytes Transferred**, select **Last 5m**.

    c. Highlight the HA appliances.

    d. Under both **Inbound Bytes** and **Outbound bytes**, check for flows with 0 bytes.

    e. If a flow has 0 outbound bytes, then the LAN interface of the appliance where the flow originates is not receiving traffic.

    f. 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.

    g. If there are no outbound bytes, check the LAN device to make sure the traffic is redirected.

    h. 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. Refer to "Silver Peak Appliance Manager Operator's Guide" for steps on how to add a 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.