# Table of Contents

Table of Contents .................................................................................................................. 2

Copyright and Trademarks .................................................................................................. 3

About Silver Peak traditional HA ......................................................................................... 4

Deploy a traditional HA in the data center ......................................................................... 6
  Set up Orchestrator by completing the following tasks. ...................................................... 7
  Enable IPsec UDP ................................................................................................................... 8
  Set up VRRP .......................................................................................................................... 10
    About VRRP priority .......................................................................................................... 10
    About VRRP preemption ..................................................................................................... 10
    Set up VRRP with different priority levels ....................................................................... 11
  Set up IP SLA ....................................................................................................................... 13
  Enable a traditional HA in the deployment profile ............................................................. 15

Optional configuration steps ............................................................................................... 16
  Set up BGP ......................................................................................................................... 17
  Set up OSPF ........................................................................................................................ 22
    Set up OSPF on the first EdgeConnect appliance ............................................................ 22
    Set up OSPF on the second EdgeConnect appliance ....................................................... 28

Troubleshooting .................................................................................................................... 33

Support .................................................................................................................................. 34

Related Documentation ....................................................................................................... 35
Copyright and Trademarks

Silver Peak Traditional High Availability Deployment Guide

Date: January 2020

Copyright © 2020 Silver Peak Systems, Inc. All rights reserved. Information in this document is subject to change at any time. Use of this documentation is restricted as specified in the End User License Agreement. No part of this documentation can be reproduced, except as noted in the End User License Agreement, in whole or in part, without the written consent of Silver Peak Systems, Inc.

Trademark Notification

Silver Peak, the Silver Peak logo, and all Silver Peak product names, logos, and brands are trademarks or registered trademarks of Silver Peak Systems, Inc. in the United States and/or other countries. All other product names, logos, and brands are property of their respective owners.

Warranties and Disclaimers

THIS DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SILVER PEAK SYSTEMS, INC. ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMissions IN THIS DOCUMENTATION OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS DOCUMENTATION. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL SILVER PEAK SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENTATION. THIS DOCUMENTATION MAY INCLUDE TECHNICAL OR OTHER INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENTATION. SILVER PEAK SYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENTATION AT ANY TIME.

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
About Silver Peak traditional HA

A traditional Silver Peak high availability (HA) deployment is similar to Silver Peak EdgeHA, but with a layer 2 switch between the Silver Peak EdgeConnect and the internet service provider (ISP) on the WAN side. A traditional HA deployment can be simple or complex, depending on your organization's needs. Unlike an EdgeHA configuration that's typically simple to deploy, a traditional HA has various configuration options on the LAN side, such as BGP and OSPF.

A common deployment is deploying a traditional HA in a router mode configuration, with VRRP support on the LAN-side.

**NOTE** If you are unsure if a traditional HA is the right choice for your organization, refer to the Silver Peak EdgeHA Getting Started Guide.

![Diagram](image)

*Figure 1: A typical traditional HA deployment.*
When setting up your Silver Peak EdgeConnect devices for high availability, make sure you meet the following requirements.

- The packet flow is symmetric.
- All packets should terminate on one or the other EdgeConnect appliance.
- Make sure VRRP displays accurately the tunnel availability on the LAN-side.
- Configure DHCP relay on both EdgeConnect appliances.
- The EdgeConnect appliances are in an active-standby deployment.

To set up an HA configuration specific to your organization's needs, contact your Silver Peak Technical Assistance Center (TAC) representative.
Deploy a traditional HA in the data center

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

- Add at least two EdgeConnect appliances to Orchestrator.
- Confirm the tunnels are in IPsec UDP mode.
Set up Orchestrator by completing the following tasks.

The following tasks describe how to configure a sample traditional HA in the data center. 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.

- Set up VRRP
- Set up IP SLA
- Enable a traditional HA in the deployment profile
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.

Select 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.

**Tunnel Settings**  

![Tunnel Settings](image)

*Figure 2: IPsec UDP tunnel settings.*

Make sure each EdgeConnect appliance has a unique IPsec UDP port.

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.

4. Select **Save**.

![Orchestration Settings](image)

---

**Orchestration Settings**

- Apply Overlays
- Reset All Flows
- Auto Save Appliance Changes
- Apply Templates
- Idle Time: 300 Sec
- Auto Flow Re-Classify: 60 (0..65535) Sec

**IPSec UDP Settings**

- Default Port: 10002
- Increment Port By: 1000

![Figure 3](image)

**Figure 3:** IPSec UDP Orchestrator settings.
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 a traditional HA, 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

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Interface</th>
<th>State</th>
<th>Admin</th>
<th>Virtual IP</th>
<th>Advertisement Timer</th>
<th>Priority Config</th>
<th>Priority State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>lan0</td>
<td>master</td>
<td>Up</td>
<td></td>
<td>1</td>
<td>129</td>
<td>129</td>
</tr>
<tr>
<td>2</td>
<td>lan0</td>
<td>backup</td>
<td>Up</td>
<td></td>
<td>1</td>
<td>128</td>
<td>128</td>
</tr>
</tbody>
</table>

*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 traditional high availability set up. The state is either true if the VRRP instance on an interface is the master, or false if the VRRP instance is in another state, such as backup or init.

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

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.
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

<table>
<thead>
<tr>
<th>Monitor</th>
<th>VRRP Monitor ▼</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Ian0 ▼</td>
</tr>
<tr>
<td>Monitor Sampling Interval</td>
<td>1 Sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>Modify Subnet Metric ▼</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down Action</td>
<td>2</td>
</tr>
<tr>
<td>Up Action</td>
<td>Default Subnet Action ▼</td>
</tr>
<tr>
<td>Comment</td>
<td>optional</td>
</tr>
</tbody>
</table>

*Figure 5: IP SLA rule.*
Enable a traditional HA in the deployment profile

Enable a traditional HA in Silver Peak Orchestrator by completing the following steps.

TIP 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, navigate to the appliance side bar on the left side of the screen.
2. Determine which two EdgeConnect appliances create an HA pair.
   NOTE You can create an HA configuration with more than two appliances.
3. Right-click the first appliance and select Modify Appliance.
4. In the Site Name field, enter a name for the location of the appliance.
5. Select OK.
6. Right-click the second appliance and select Modify Appliance.
7. In the Site Name field, enter the same location that you entered for the first appliance.
8. Select OK.

By giving both EdgeConnect appliances the same site name, you created an HA pair.
Optional configuration steps

You can set up a traditional high availability deployment using different types of routing protocols. Contact and work with your Silver Peak system engineer or representative to figure out what deployment options meet your organization's needs.

Configure the routing protocols before you deploy your HA configuration.

- Set up BGP
- Set up OSPF
Set up BGP

In a traditional HA deployment, you can set up BGP on the LAN side with a preferred route to one of the service providers. In this configuration, the routers on the WAN side use BGP to direct traffic to multiple Silver Peak EdgeConnect appliances.

Use BGP routing in an active-backup deployment and in conjunction with subnet sharing. When load balancing, the EdgeConnect appliances advertise the same metric. If you deploy an active-backup load balance configuration, the active connection advertises lower metrics than the backup connection.

![BGP Configuration Diagram](image)

*Figure 6: BGP configuration.*

**NOTE** Refer to the *Subnet Sharing Metric for OSPF and BGP Learned Routes Tech Note* for more information about subnet sharing.

You can set up BGP in one of three ways. Refer to the *BGP Tab* section of the *Silver Peak Orchestrator Operator’s Guide*. 
With a branch router.

With a branch transit router.

With a provider edge router.

**TIP** Use eBGP as your default BGP deployment.

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 first EdgeConnect appliance.
   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](image)

*Figure 7: Basic BGP information.*

Add BGP peers.

1. Select **Add**.
2. In the **Peer IP** field, enter a name 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. In the **Metric Delta** field, enter a number to set up primary and backup paths to the same destination. The higher the number, the higher the cost to advertise routes to this peer.

6. From the **Peer Type** list, select the type of route that appliances are allowed to advertise to this BGP peer.

7. In the **Local Preference** field, enter the default value, **100**.

8. 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.

9. 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.

10. In the **Input Metric** field, enter a number that is advertised when the route is shared.
    
    For example, **50** for the primary appliance and **70** for the secondary appliance. If you use route maps to set the MED to or from the appliance, you can set the Input Metric to **0**.

11. In the **Keep Alive Timer** field, enter a number that specifies the interval, in seconds, between keep alive signals to a peer.

12. 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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer IP</td>
<td>192.168.1.4</td>
</tr>
<tr>
<td>Peer ASN</td>
<td>23</td>
</tr>
<tr>
<td>Enable Imports</td>
<td>✔</td>
</tr>
<tr>
<td>Peer Type</td>
<td>Branch</td>
</tr>
<tr>
<td>Admin Status</td>
<td><img src="#" alt="UP" /> <img src="#" alt="DOWN" /></td>
</tr>
<tr>
<td>Local Preference</td>
<td>100</td>
</tr>
<tr>
<td>MED</td>
<td>0</td>
</tr>
<tr>
<td>AS Prepend Count</td>
<td>0 (0..10)</td>
</tr>
<tr>
<td>Input Metric</td>
<td>0</td>
</tr>
<tr>
<td>Keep Alive Timer*</td>
<td>30 (0.65535) Sec</td>
</tr>
<tr>
<td>Hold Timer*</td>
<td>90 (0.65535) Sec</td>
</tr>
</tbody>
</table>

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

---

Figure 8: Standard BGP configuration.

Specify advertising routes.

1. Navigate to the **Route Export Policies for Peer Type** section.
2. Select the check boxes to specify which routes to advertise to this peer.

### Route Export Policies for Peer Type: **Branch**

<table>
<thead>
<tr>
<th>Route</th>
<th>Use Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Locally configured</td>
<td>✔</td>
</tr>
<tr>
<td>2. Learned via subnet sharing</td>
<td>✔</td>
</tr>
<tr>
<td>3. Learned from a local BGP branch peer</td>
<td>✔</td>
</tr>
<tr>
<td>4. Learned from a local BGP branch-transit peer</td>
<td>✔</td>
</tr>
<tr>
<td>5. Learned from a local BGP PE router</td>
<td>✔</td>
</tr>
<tr>
<td>6. Remote BGP</td>
<td>✔</td>
</tr>
<tr>
<td>(learned via subnet sharing, but originally from a BGP peer)</td>
<td>✔</td>
</tr>
<tr>
<td>7. Remote BGP branch-transit peer</td>
<td>✔</td>
</tr>
<tr>
<td>(learned via subnet sharing, but originally a BGP-transit peer)</td>
<td>✔</td>
</tr>
<tr>
<td>8. Learned from a local OSPF peer</td>
<td>✔</td>
</tr>
<tr>
<td>9. Learned from a Remote OSPF peer</td>
<td>✔</td>
</tr>
</tbody>
</table>

Figure 9: 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 up OSPF

Traditional HA deployment with OSPF configuration on the LAN side with a different link costs where one EC appliance is preferred. OSPF replaces VRRP in a traditional HA deployment. Make sure to note the following:

- Enable IPsec UDP
- Do not set up VRRP or create an IP SLA

![Diagram of Traditional configuration with OSPF](image)

Figure 10: Traditional configuration with OSPF.

**NOTE** Refer to the Subnet Sharing Metric for OSPF and BGP Learned Routes Tech Note for more information about subnet sharing.

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 **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**.

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, such as **100**.

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**.
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.

*Figure 11: OSPF configuration.*
4. The EdgeConnect with the lower number is the preferred route for outbound traffic. In this example, E2, with a cost of 10, is the preferred route. Configure the same OSPF cost on the LAN router interface.

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 12: 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 EC2 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
Automatically advertise local LAN subnets ✓
Automatically advertise local WAN subnets ✓
Metric for automatically added subnets 50
Redistribute OSPF routes to Silver Peak peers ✓
  Metric 50
  Filter Tag 100

Figure 13: 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  
Router ID  
Redistribute BGP routes to OSPF  
Metric Type  
Metric  
Tag  
Redistribute Silver Peak peers routes to OSPF  
Metric Type  
Metric  
Tag  
Redistribute local routes to OSPF  
Metric Type  
Metric  
Tag  

*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 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

<table>
<thead>
<tr>
<th>Interface</th>
<th>lan0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>0.0.0.0 = 0</td>
</tr>
</tbody>
</table>

(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.)

<table>
<thead>
<tr>
<th>Cost</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>1</td>
</tr>
<tr>
<td>Admin Status</td>
<td>UP  DOWN</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>10 (1..65535) Sec</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>40 (1..65535) Sec</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>1 (1..450) Sec</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>4 (1..65535) Sec</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Comment</td>
<td></td>
</tr>
</tbody>
</table>

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 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
Redistribute OSPF routes to Silver Peak peers

Metric
70
Filter Tag
100

Figure 16: Add route metric and filter tag.
Troubleshooting

Try using the following suggestions when troubleshooting issues that occur in a traditional HA deployment.

- 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 an appliance fails, the failure does not affect the tunnels on the other appliance.

- When an appliance is back up after experiencing downtime, there might be downtime when traffic moves between appliances again. This depends on the VRRP preemption, subnet metrics, and IP SLA.
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 EdgeHA 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](https://www.silver-peak.com).