



# SteelHead™ SD User Guide

Models 570-SD, 770-SD, 3070-SD

SteelHead SD 2.12, SteelConnect 2.12

May 2019

© 2019 Riverbed Technology, Inc. All rights reserved.

Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

Akamai® and the Akamai wave logo are registered trademarks of Akamai Technologies, Inc. SureRoute is a service mark of Akamai. Apple and Mac are registered trademarks of Apple, Incorporated in the United States and in other countries. Cisco is a registered trademark of Cisco Systems, Inc. and its affiliates in the United States and in other countries. EMC, Symmetrix, and SRDF are registered trademarks of EMC Corporation and its affiliates in the United States and in other countries. IBM, iSeries, and AS/400 are registered trademarks of IBM Corporation and its affiliates in the United States and in other countries. Juniper Networks and Junos are registered trademarks of Juniper Networks, Incorporated in the United States and other countries. Linux is a trademark of Linus Torvalds in the United States and in other countries. Microsoft, Windows, Vista, Outlook, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and in other countries. Oracle and JInitiator are trademarks or registered trademarks of Oracle Corporation in the United States and in other countries. UNIX is a registered trademark in the United States and in other countries, exclusively licensed through X/Open Company, Ltd. VMware, ESX, ESXi are trademarks or registered trademarks of VMware, Inc. in the United States and in other countries.

This product includes Windows Azure Linux Agent developed by the Microsoft Corporation (<http://www.microsoft.com/>). Copyright 2017 Microsoft Corporation.

This product includes software developed by the University of California, Berkeley (and its contributors), EMC, and Comtech AHA Corporation. This product is derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

The SteelHead Mobile Controller (virtual edition) includes VMware Tools. Portions Copyright © 1998-2016 VMware, Inc. All Rights Reserved.

NetApp Manageability Software Development Kit (NM SDK), including any third-party software available for review with such SDK which can be found at <http://communities.netapp.com/docs/DOC-1152>, and are included in a NOTICES file included within the downloaded files.

For a list of open source software (including libraries) used in the development of this software along with associated copyright and license agreements, see the Riverbed Support site at <https://support.riverbed.com>.

This documentation is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed. This documentation may not be copied, modified or distributed without the express authorization of Riverbed and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.



Riverbed Technology  
680 Folsom Street  
San Francisco, CA 94107  
[www.riverbed.com](http://www.riverbed.com)

Part Number  
712-00328-01

# Contents

<b>Welcome to SteelHead SD .....</b>	<b>7</b>
Documentation and release notes .....	7
Contacting Riverbed .....	7
 <b>1 - Introducing SteelHead SD .....</b>	 <b>9</b>
Overview of the SteelHead SD .....	9
Routing features by model .....	11
Hardware and software requirements .....	12
NIC support .....	12
Firewall requirements .....	12
Ethernet network compatibility .....	13
SNMP-based management compatibility .....	13
Next steps .....	13
 <b>2 - Configuring Virtual SteelHead WAN Optimization.....</b>	 <b>15</b>
Overview of WAN optimization on the virtual SteelHead.....	15
Assigning the in-path IP address and default gateway in SCM .....	16
Enabling WAN Optimization in SCM .....	17
Identifying the primary IP address of the SteelHead .....	19
Enabling WAN optimization on the virtual SteelHead instance .....	19
Configuring the in-path interface and default gateway .....	19
Troubleshooting .....	21
 <b>3 - Configuring DHCP Options in Zones on SteelHead SD .....</b>	 <b>23</b>
Configuring DHCP options on SteelHead SD LAN clients .....	23
Overriding DNS on guest zones on SteelHead SD.....	24
 <b>4 - Configuring Local Subnet Discovery on SteelHead SD .....</b>	 <b>27</b>
Overview of local subnet discovery .....	27
Routing criteria .....	27

Defining global subnet discovery at the organization level .....	28
Defining local subnet discovery .....	30
<b>5 - Configuring AutoVPN on SteelHead SD .....</b>	<b>33</b>
Overview of AutoVPN on SteelHead SD.....	33
Configuring AutoVPN on SteelHead SD .....	34
<b>6 - Defining VLAN Trunk Ports on SteelHead SD .....</b>	<b>37</b>
Overview of multizone VLAN trunk mode on SteelHead SD.....	37
Defining trunk mode on ports .....	38
<b>7 - Configuring BGP, OSPF, Static Routing, and Route Retraction on SteelHead SD .....</b>	<b>41</b>
Configuring BGP on SteelHead SD.....	41
BGP on SteelHead SD overview.....	42
Enabling BGP and configuring BGP neighbors on SteelHead SD .....	42
Configuring BGP routing policies.....	44
Configuring BGP path selection .....	45
Configuring BGP inbound and outbound prefixes .....	46
Configuring BGP route redistribution.....	47
Configuring conditional default-route originate routing .....	48
Configuring the BGP origin-type attribute.....	49
Enabling multi exit discriminator (MED) settings.....	51
Configuring BGP route summarization.....	52
Resetting BGP sessions.....	54
Viewing BGP status.....	55
Configuring OSPF with ABR on SteelHead SD .....	55
Introducing OSPF with ABR .....	56
Creating an OSPF network.....	56
Configuring OSPF interfaces .....	59
Creating OSPF areas.....	60
Configuring redistribution settings for OSPF .....	62
Configuring OSPF route summarization.....	64
Viewing OSPF status.....	65
Defining static routes on SteelHead SD appliances.....	66
Route retraction for SteelHead SD .....	67
<b>8 - Configuring BGP and OSPF Routing Policies on SteelHead SD.....</b>	<b>69</b>
Overview of routing policies on SteelHead SD.....	69
What are routing policies? .....	70
Basic steps .....	72
Creating routing IPv4 prefix lists .....	72
Creating routing community lists .....	73

Creating routing AS path lists .....	74
Configuring route maps.....	76
<b>9 - Configuring LAN-Side Internet Breakout on SteelHead SD .....</b>	<b>85</b>
Overview of LAN-side internet breakout on SteelHead SD .....	85
Configuring LAN-side internet breakout.....	86
Troubleshooting .....	89
<b>10 - Configuring High Availability on SteelHead SD .....</b>	<b>91</b>
Overview of HA on SteelHead SD.....	91
Symmetric and asymmetric uplink connectivity .....	92
Layer 2 and Layer 3 support at the branch.....	93
Failure conditions.....	94
Prerequisites .....	94
Configuring a SteelHead SD HA pair .....	94
Configuring the AUX port on the HA pair .....	95
Configuring the LAN zone for the SteelHead SD HA pair .....	95
Assigning the LAN zone to the SteelHead SD HA pair .....	96
Configuring the appliances in an HA pair .....	97
Configuring a standby LAN HA link .....	98
Monitoring a high-availability pair .....	101
Troubleshooting .....	103
<b>11 - Configuring QoS Shaping on SteelHead SD .....</b>	<b>105</b>
QoS shaping on SteelHead SD .....	105
SteelHead SD QoS shaper.....	105
If you set the QoS priority in a traffic rule.....	106
Configuring QoS shaping on SteelHead SD .....	107
<b>12 - Health Check and Reporting on SteelHead SD .....</b>	<b>109</b>
Checking SteelHead SD connectivity to SCM.....	109
Viewing the SteelHead SD HA status .....	110
Displaying underlay ARP tables .....	110
Displaying FIB tables .....	111
Displaying BGP peer tables .....	112
Displaying OSPF neighbors and routes .....	112
Displaying NTP server status.....	113
Enabling SNMP reporting and logging .....	114
Exporting syslog messages to an external syslog server .....	114

Exporting Netflow data .....	115
<b>A - Port Mapping for SteelHead SD .....</b>	<b>117</b>
SteelHead SD 570-SD and 770-SD appliances .....	117
Physical ports .....	117
CVM ports .....	117
Physical port to flows port mapping .....	117
Service chain virtual machines .....	117
vSwitch mapped VM ports .....	118
Bridged VM ports for internal communication .....	119
SteelHead SD 3070-SD appliance .....	119
Physical ports .....	119
CVM ports .....	119
Physical port to flows port mapping .....	119
SVM ports .....	119
RVM ports .....	120
vSH ports .....	120
<b>B - TOS, DSCP, QoS Traffic Class Table .....</b>	<b>121</b>
TOS, DSCP, and QoS Traffic Classes Table .....	121

# Welcome to SteelHead SD

Welcome to the *SteelHead SD User Guide*. SteelHead SD combines SD-WAN and cloud networking capabilities (powered by SteelConnect) with Riverbed WAN optimization (powered by RiOS) into a single appliance.

This guide describes how to configure the Riverbed SteelHead SD (SteelHead SD) when used in conjunction with SteelConnect SDI-2030 and SDI-5030 gateways.

This guide is written for network administrators familiar with administering and managing WANs.

For a high-level look at how SteelConnect works, see the *SteelConnect Manager User Guide*.

## Documentation and release notes

The most current version of all Riverbed documentation can be found on the Riverbed Support site at <https://support.riverbed.com>.

See the Riverbed Knowledge Base for any known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings. To access the Riverbed Knowledge Base, log in to the Riverbed Support site at <https://support.riverbed.com>.

Each software release includes release notes. The release notes list new features, known issues, and fixed problems. To obtain the most current version of the release notes, go to the Software and Documentation section of the Riverbed Support site at <https://support.riverbed.com>.

Examine the release notes before you begin the installation and configuration process.

## Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - Problems installing, using, or replacing Riverbed products? Contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415-247-7381 outside the United States. You can also go to <https://support.riverbed.com>.
- **Professional services** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email [proserve@riverbed.com](mailto:proserve@riverbed.com) or go to <http://www.riverbed.com/services/index.htm>.

- **Documentation** - Have suggestions about the online documentation or printed materials? Send comments to [techpubs@riverbed.com](mailto:techpubs@riverbed.com).



# Introducing SteelHead SD

This topic provides an overview of the SteelHead SD. It includes these sections:

- [“Overview of the SteelHead SD” on page 9](#)
- [“Routing features by model” on page 11](#)
- [“Hardware and software requirements” on page 12](#)
- [“Next steps” on page 13](#)

This guide doesn't provide detailed information about configuring and managing SD-WAN or WAN optimization features. For details, see the *SteelConnect Manager User Guide* and the *SteelHead User Guide*.

This guide assumes you have installed your SteelHead SD appliances. For details, see the *SteelHead SD Installation Guide*.

## Overview of the SteelHead SD

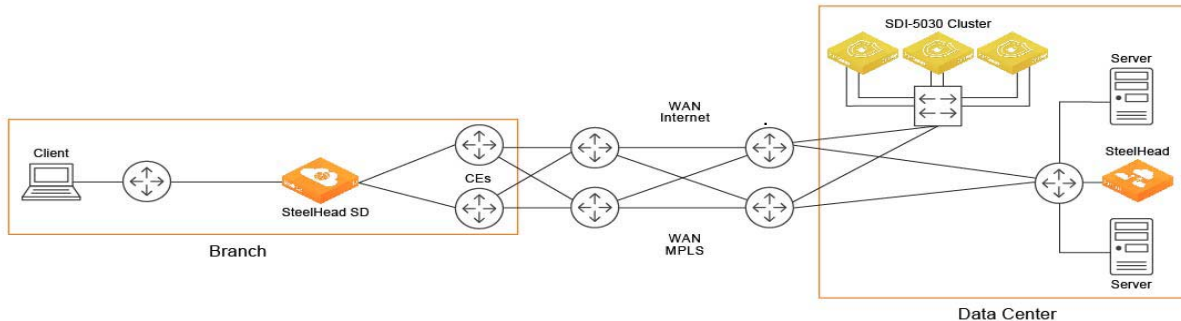
SteelHead SD combines SD-WAN and cloud networking capabilities (powered by SteelConnect) with Riverbed WAN optimization (powered by RiOS) into a single appliance. SteelHead SD seamlessly integrates advanced SD-WAN functionality with industry-leading WAN optimization, security, and visibility services all in one streamlined appliance. SteelHead SD WAN optimization reduces bandwidth utilization and accelerates application delivery and performance, while providing SteelConnect integration in the SteelOS environment.

SteelHead SD provides you with the ability to quickly provision branch sites and deploy applications remotely. At the same time, applications are optimized to ensure performance and reduce latency with zero touch provisioning.

Typically, SteelHead SD appliances and the SteelConnect SDI-2030 gateway are located in the branch office in conjunction with SteelConnect SDI-5030 gateways at the data center. The SteelConnect SDI-2030 gateway can also be deployed inline as a 1-Gbps data center gateway with active-active HA. The SteelConnect SDI-2030 gateway can also serve as a very large branch office box with high throughput requirements. The SteelConnect SDI-2030 gateway doesn't support WAN optimization capabilities.

SteelHead SD advanced routing and high availability (HA) features are supported on the SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. For details, see the *SteelHead SD User Guide* and the *SteelConnect Manager User Guide*.

Figure 1-1. SteelHead SD deployment



SteelHead SD supports these configuration modes:

- **SD-WAN and WAN optimization** - In this configuration, WAN optimization runs as a service on top of SD-WAN. The SteelCentral Controller for SteelHead (SCC) or the SteelHead Management Console handles management and configuration of the WAN optimization features. Also, SteelHead CLI-based management is supported for WAN optimization settings. You connect to the Management Console via the primary port, which also uses DHCP to acquire its IP address. For details on configuring WAN optimization features, see the *SteelCentral Controller for SteelHead User Guide* and the *SteelHead User Guide*.
- **SD-WAN only** - In this configuration, WAN optimization is not required. SCM handles the management and configuration of SD-WAN features. SCM connectivity requires one of the WAN ports that are used as uplink ports. Only the SD-WAN service can be enabled or disabled via SCM. The SD-WAN service upgrades are managed via SCM. SCM pushes the new software version according to the schedule that you set up. For details on configuring SD-WAN features, see the *SteelConnect Manager User Guide* and the *SteelHead SD User Guide*.

For details on SteelHead SD software architecture and new features for SteelHead SD, see the *SteelHead SD Installation Guide*.

## Routing features by model

Feature	SteelHead-SD 570-SD, 770-SD, 3070-SD	SDI-2030	SDI-130	SDI-330	SDI-1030	SDI-5030	SDI-VGW
eBGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
iBGP	Yes	Yes	No	No	No	No	No
OSPF single area	Yes	Yes	Yes	Yes	Yes	No	No
OSPF multi-area ABR	Yes	Yes	No	No	No	No	No
ASBR	Yes	Yes	Yes* (Underlay routing inter-working solution)	Yes* (Underlay routing inter-working solution)	Yes* (Underlay routing inter-working solution)	No	Yes* (Underlay routing inter-working solution)
Route retraction	Yes	Yes	No	No	No	Yes	No
Default route originate	OSPF/BGP	OSPF /BGP LAN and WAN	OSPF only LAN	OSPF only LAN	OSPF only LAN	BGP only	OSPF only LAN
Overlay route injection in LAN	Yes	Yes	No	No	No	Yes	No
Local subnet discovery	Yes	Yes	No	No	No	Yes	No
Static routes	Yes	Yes (LAN and WAN)	Yes	Yes	Yes	Yes	Yes
VLAN support (LAN side)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

\*SCM 2.9 and later support an underlay routing interworking solution that bridges BGP and OSPF. For details, see the *SteelConnect Manager User Guide*.

## Hardware and software requirements

Riverbed component	Hardware and software requirements
SteelHead SD appliance	<p>The SteelHead SD 570-SD and 770-SD appliances are desktop models.</p> <p>The SteelHead SD 3070-SD appliance requires a 19-inch (483 mm) four-post rack. For details, see the <i>Rack Installation Guide</i>.</p>
Virtual SteelHead (vSH)	<p>SteelHead SD requires the RiOS 9.8.1 vSH image, which is contained within the SteelConnect 2.12 image.</p> <p>The SteelHead Management Console has been tested with all versions of Chrome, Mozilla Firefox Extended Support Release version 38, and Microsoft Internet Explorer 11.</p> <p>JavaScript and cookies must be enabled in your web browser.</p>
SteelConnect Manager (SCM)	<p>SteelHead SD requires SteelConnect 2.12.</p> <p>SCM supports the latest version of the Chrome browser. SCM requires a minimum screen resolution of 1280 x 720 pixels. We recommend a maximum of 1600 pixels for optimal viewing.</p>
SteelCentral Controller for SteelHead (SCC)	<p>We recommend you have SCC 9.9.0 installed if you are managing vSHs with WAN optimization enabled on SteelConnect 2.12.</p>

## NIC support

Network interface card (NICs) are supported on the SteelHead SD 3070-SD appliances for nonbypass traffic. SteelHead SD 570-SD and 770-SD appliances do not support NICs.

**Note:** For SteelHead SD 3070-SD appliances, bypass NICs are not required for SteelConnect gateway deployments since LAN traffic requires network address translation (NAT) before it reaches the service provider network.

You can install these NICs in the SteelHead SD 3070-SD for nonbypass traffic.

NICs	Size (*)	Manufacturing part #	Orderable part #
Two-Port 10-GbE Fiber SFP+	HHHL	410-00036-02	NIC-1-010G-2SFPP
Four-Port 10-GbE Fiber SFP+	HHHL	410-00108-01	NIC-1-010G-4SFPP

\*HHHL = Half Height, Half Length

For details on NICs, see the *Network and Storage Card Installation Guide*.

## Firewall requirements

The SteelHead SD 570-SD, 770-SD, 3070-SD, and SDI-2030 support stateful application-based firewalls at the network edge. For details on SteelConnect firewall and security features, see the *SD-WAN Deployment Guide*.

All communication is sourced from the site out to the SteelConnect management service. There's no need to set up elaborate firewall or forwarding rules to establish the dynamic full-mesh VPN or to gain connectivity to the cloud. After you register an appliance, it receives its assigned configuration automatically. For details on SteelConnect firewall requirements, see the *SteelConnect Manager User Guide*.

Make sure the firewall ports 80 and 443 are open so that software installation and SCM operations aren't blocked. For details on SteelConnect default ports, see the *SteelConnect Manager User Guide*.

## Ethernet network compatibility

The SteelHead SD appliance supports these Ethernet networking standards.

Ethernet standard	IEEE standard
Ethernet Logical Link Control (LLC)	IEEE 802.2 - 1998
Fast Ethernet 100BASE-TX	IEEE 802.3 - 2008
Gigabit Ethernet over Copper 1000BASE-T (All copper interfaces are autosensing for speed and duplex.)	IEEE 802.3 - 2008
Gigabit Ethernet over Fiber 1000BASE-SX (LC connector)	IEEE 802.3 - 2008
Gigabit Ethernet over Fiber 1000BASE-LX	IEEE 802.3 - 2008
Gigabit Ethernet over Fiber 10GBASE-LR Single Mode	IEEE 802.3 - 2008
Gigabit Ethernet over 10GBASE-SR Multimode	IEEE 802.3 - 2008

## SNMP-based management compatibility

SteelConnect provides support for SNMPv1 and v2c polling, and event logging are supported on the SDI-130, SDI-330, SDI-1030, SDI-5030, and virtual gateways. SNMP v1, v2c, and v3 are supported in SCM (and only visible by a realm administrator). SNMP reporting is supported on SteelHead SD SD-570, SD-770, SD-3070 and 2030-SDI appliances located at the branch. For details, see the *SteelConnect Manager User Guide*.

The virtual SteelHead supports proprietary MIBs accessible through SNMP, SNMPv1, SNMPv2c, and SNMPv3, although some MIB items might only be accessible through SNMPv2 and SNMPv3. For details on the WAN optimization service MIB, see the *SteelHead User Guide*.

## Next steps

Make sure you read the *SteelConnect Manager User Guide*. It contains detailed information about how to design and organize your network of SteelHead SD appliances and SteelConnect gateways.

Next steps

# Configuring Virtual SteelHead WAN Optimization

This topic describes how to enable SteelHead WAN optimization for SteelHead SD 2.0. It includes these sections:

- [“Overview of WAN optimization on the virtual SteelHead” on page 15](#)
- [“Assigning the in-path IP address and default gateway in SCM” on page 16](#)
- [“Enabling WAN Optimization in SCM” on page 17](#)
- [“Enabling WAN optimization on the virtual SteelHead instance” on page 19](#)
- [“Troubleshooting” on page 21](#)

---

**Important:** These instructions assume you have created an organization, site, zones, and uplinks for the SteelHead SD appliance. For details, see the *SteelConnect Manager User Guide*. For detailed information on installing SteelHead SD, see the *SteelHead SD Installation Guide*.

---

## Overview of WAN optimization on the virtual SteelHead

When you enable WAN optimization on the virtual SteelHead, you perform the initial configuration within SCM. You must also configure settings on the virtual SteelHead instance itself, using the SteelHead Management Console, the CLI, or the SteelCentral Controller for SteelHead (SCC).

When enabling WAN optimization, keep these guidelines in mind:

- To enable WAN optimization, the location where the SteelHead SD is installed must have at least one LAN zone. The in-path IP address in the virtual SteelHead instance must match the address in SCM.
- The LAN port must be configured as a single-zone uplink for the SteelHead WAN optimization service. If you do not enable the LAN port, SteelConnect won't see either the SteelHead WAN optimization service or the clients on the LAN side of the network.
- The default gateway in the virtual SteelHead instance must be the IP address for the LAN zone in SCM.
- If the LAN port of the SteelHead SD appliance is on a VLAN trunk, make sure to configure the VLAN ID on the virtual SteelHead in-path interface.
- Depending on the in-path rules you have defined, the virtual SteelHead instance optimizes any traffic received from SteelConnect via the LAN interface.

- When WAN optimization is enabled in SCM, there is a momentary interruption to service as the SteelConnect is reconfigured with its SteelHead LAN and WAN interfaces.

When WAN optimization is enabled, a virtual SteelHead instance is automatically provisioned by the system. The primary port on the SteelHead SD appliance is connected directly to the primary interface of the virtual SteelHead instance.

The virtual SteelHead instance is configured with a single in-path interface pair (LAN/WAN). Unlike physical SteelHead appliances or their virtual equivalents that exist outside of an SD-WAN service-chained deployment, the number of in-path interfaces is irrelevant. For consistency and compatibility, the in-path interface pair is configured as LAN0\_0 and WAN0\_0.

## Assigning the in-path IP address and default gateway in SCM

The first step is to assign an in-path IP address within the LAN zone for the site. You choose an IP address for the LAN zone in which the SteelHead SD is installed. You will use this IP address to configure the in-path interface and default gateway on the virtual SteelHead instance.

These instructions assume that you have configured the primary and LAN ports on the SteelHead SD appliance in SCM:

- The LAN port is configured as a single-zone uplink for the SteelHead WAN optimization service. By default, the LAN port is disabled on SteelHead SD appliances unless it is explicitly enabled. If you don't enable the LAN port, SteelConnect won't see either the SteelHead WAN optimization service or the clients on the LAN side of the network.
- The primary port is configured as SteelHead Primary mode for the SteelHead SD appliance.

**Note:** If the LAN port attached to the SteelHead SD appliance is in a VLAN trunk, the virtual SteelHead instance must be given an IP address from one of the zones that is part of the trunk, and the virtual SteelHead in-path IP address must also be configured with the corresponding VLAN ID.

For details on configuring the primary and LAN ports, see the *SteelHead SD Installation Guide*.

### To assign the in-path IP address and the default gateway in SCM

1. In SCM, choose Network Design > Zones.
2. Select the zone with the SteelHead SD appliance to expand the pane. The IP tab is displayed.



- Under IPv4 Network, specify the LAN zone subnet. Write down this IP address. You will use this address when you configure the inpath0\_0 interface for WAN optimization on the virtual SteelHead instance.

Figure 2-1. Assigning the IP address for the in-path IP address and default gateway

The screenshot shows the configuration page for a device named 'Branch10\_1100'. The 'IP' tab is selected, showing the 'IPv4 network and gateway' section. Below this, there is a text input for 'IPv4 Network' containing '172.16.20.0/24' and another for 'IPv4 Gateway' containing '172.16.20.2'. At the bottom of this section are 'Cancel' and 'Submit' buttons. Below the IPv4 section is the 'IPv6 status, network, and gateway' section, which includes a toggle for 'Use IPv6' currently set to 'Off'.

For example, if the network IP address is 172.16.20.0/24, you can assign any IP address from 172.16.20.1 to 172.16.20.254 for the SteelHead in-path interface.

- Under IPv4 Gateway, specify the default gateway. Write down this IP address. You will use this address when you configure the default gateway for WAN optimization on the virtual SteelHead instance.

## Enabling WAN Optimization in SCM

You enable WAN optimization in SCM in the Appliances page under the Services tab. You also specify the virtual SteelHead instance in-path IP address. The in-path IP address must be within the LAN zone subnet that you have defined.

The WAN optimization service is disabled by default. When disabled, the WAN optimization service will not participate in any WAN optimization functionality. If disabled, any configuration related to WAN optimization service on this appliance will not be applied.

---

**Important:** Only zones that are attached to a physical port can be used to configure the SteelHead SD IP address. Choose Appliances > Port to attach a zone to a port.

---

### To enable WAN optimization

- Choose Appliances > Overview.

2. Select the SteelHead SD appliance to expand the page.
3. Select the Services tab.

Figure 2-2. Enabling WAN optimization in SCM

The screenshot shows the configuration page for a SteelHead SD appliance named '770-SD'. The 'Services' tab is selected, and the 'WAN optimization service' is configured. The service is currently 'Enabled'. The 'SteelHead zone' is set to 'Branch-5 -> LAN [1012]'. The 'SteelHead in-path IP Address' field is empty.

**770-SD** Actions ▾ ✕

Live IPs AutoVPN System dump Tools HA Routing BGP **Services** NetFlow

**Location**

---

**WAN optimization service**

WAN optimization service is disabled by default. When disabled, the WAN optimization service will not participate in any WAN optimization functionality. Any configuration related to WAN optimization service on this appliance will not be applied while the service is disabled. Enabling WAN optimization will disrupt network connectivity for a few minutes.

Only zones that are attached to a physical port can be used to configure the SteelHead-SD IP address. Choose Appliances > Port to attach a zone to a port.

WAN optimization service ⓘ **Enabled** Disabled

SteelHead zone ⓘ Branch-5 -> LAN [1012] ▾

SteelHead in-path IP Address ⓘ

4. Under WAN Optimization Service, fill out these required session attributes:
  - **WAN Optimization Service** - Click **Enabled** to enable the WAN optimization service for the selected SteelHead SD appliance. When disabled, the WAN optimization service will not participate in any WAN optimization functionality. If disabled, any configuration related to WAN optimization service on this appliance will not be applied.
  - **SteelHead Zone** - Select the zone to which this SteelHead SD appliance belongs. Only zones that are attached to a physical port can be used to configure the SteelHead SD IP address. Choose Appliances > Port to attach a zone to a port.
  - **SteelHead Inpath IP Address** - Specify the SteelHead in-path IP address. The IP address must be within the LAN zone subnet. This value tells SCM what in-path IP address you are using for the virtual SteelHead instance.
5. Click **Submit**.

After the WAN optimization service has been enabled within SCM, the SteelHead SD triggers the orchestration and provisioning of the virtual SteelHead instance. This action causes a momentary interruption to operations within SteelConnect because it is reconfigured with the SteelHead LAN and WAN interfaces.

As the virtual SteelHead instance boots within SteelHead SD, its primary interface tries to obtain an IP address via DHCP. It is important to ensure the SteelHead SD primary port is attached to a network where a DHCP service is available.

## Identifying the primary IP address of the SteelHead

You use the primary IP address to connect to the virtual SteelHead instance. You can identify the primary IP address of the SteelHead in one of the following ways:

- **When SteelConnect acts as the DHCP server** - You can set the SteelConnect virtual gateway to act as a DHCP server and identify the primary IP address for the SteelHead in SCM. To view the SteelHead primary IP address in SCM, choose Appliances > Overview and select the SteelHead SD appliance. The primary IP address is listed under the IPs tab. For details on configuring SteelConnect to act as a DHCP server, see the *SteelHead SD Installation Guide*.
- **When the SCC is used to manage SteelHeads** - If you are using the SCC to manage the WAN optimization service, you can obtain the primary IP address for each appliance in your network. SCC automatically registers all SteelHeads it detects in your network and provides the primary IP address for each in the Appliances page. For details on connecting to SCC, see the *SteelCentral Controller for SteelHead User Guide*.
- **When an external server acts as the DHCP server** - You can obtain the MAC address from the appliance and search for the primary IP address on the DHCP server console. You can find the MAC address on the appliance label or you can view it in SCM. To view the MAC address in SCM, choose Ports and select the primary port for the appliance. The MAC address is listed under the Info-Mode tab.

After you have discovered the primary IP address that has been leased to the virtual SteelHead instance, you simply log in to the management console user interface and complete the configuration of the virtual SteelHead instance.

## Enabling WAN optimization on the virtual SteelHead instance

To enable WAN optimization for SteelHead SD, you must configure the inpath0\_0 interface and default gateway for each appliance in your network using the SCC or the SteelHead Management Console.

### Configuring the in-path interface and default gateway

These instructions describe how to configure the in-path interface and default gateway using the SteelHead Management Console.

---

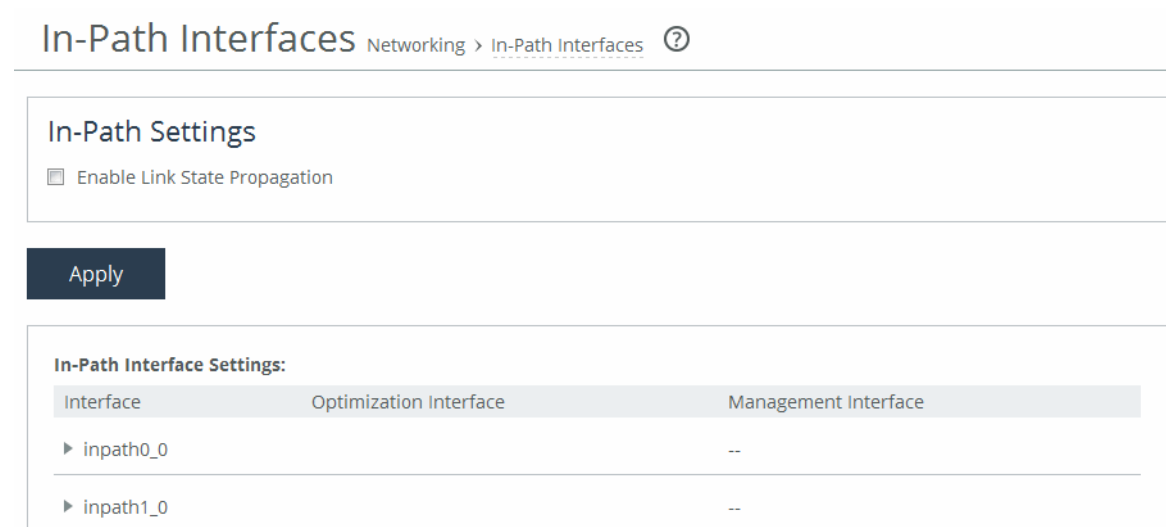
**Tip:** In the SCC, choose Manage: Appliances > Appliance Pages > In-Path Interfaces to modify the inpath0\_0 interface and default gateway. You can push the policy to the selected appliance.

---

## To configure the in-path interface and the default gateway in the SteelHead

1. Using the Primary IP address you obtained from SCM, SCC, or the DHCP server, enter it in the address bar of your web browser using HTTPS. The login page for the SteelHead Management Console is displayed.
2. Specify the default user login (**admin**) and password (**password**).
3. Click **Sign In** to display the Dashboard.
4. Choose **Networks > Networking: In-Path Interfaces**.

Figure 2-3. In-Path Interfaces page



**In-Path Interfaces** Networking > In-Path Interfaces ?

---

**In-Path Settings**

☐ Enable Link State Propagation

**Apply**

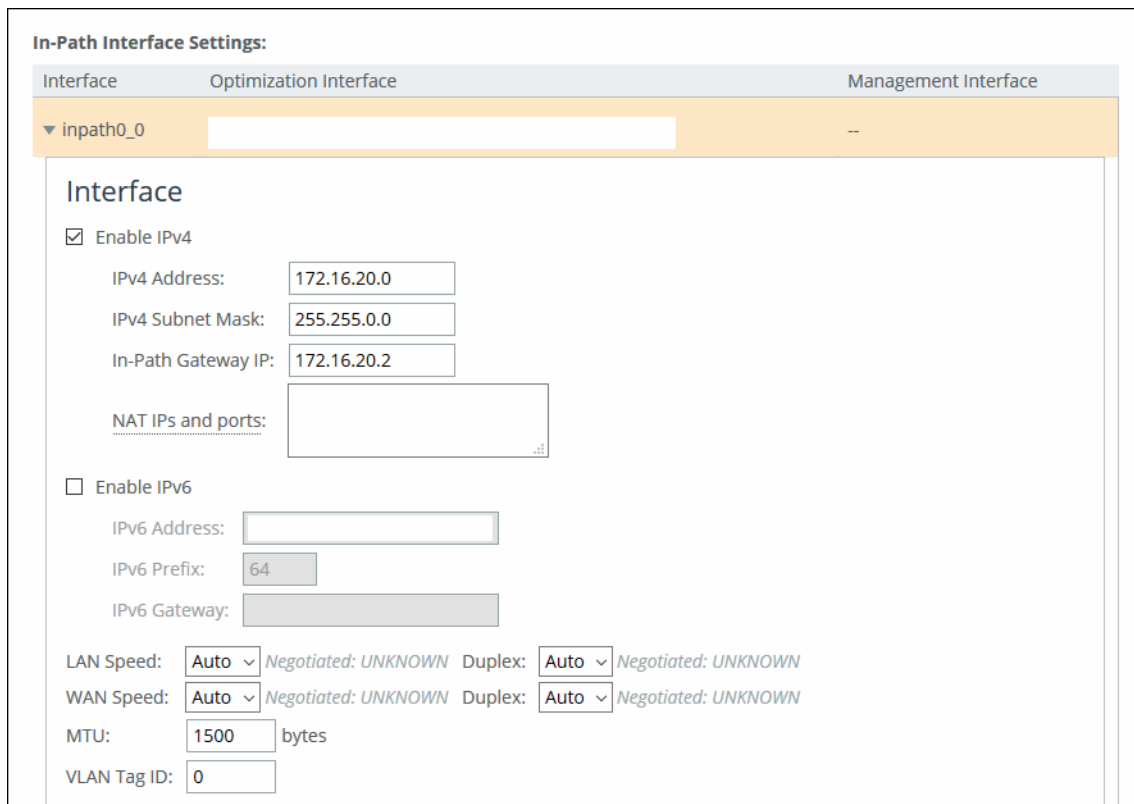
---

**In-Path Interface Settings:**

Interface	Optimization Interface	Management Interface
▶ inpath0_0		--
▶ inpath1_0		--

5. Select the interface to expand the page.

Figure 2-4. Configuring the in-path interface



**In-Path Interface Settings:**

Interface	Optimization Interface	Management Interface
▼ inpath0_0		--

**Interface**

☒ Enable IPv4

IPv4 Address:

IPv4 Subnet Mask:

In-Path Gateway IP:

NAT IPs and ports:

☐ Enable IPv6

IPv6 Address:

IPv6 Prefix:

IPv6 Gateway:

LAN Speed:  Negotiated: UNKNOWN Duplex:  Negotiated: UNKNOWN

WAN Speed:  Negotiated: UNKNOWN Duplex:  Negotiated: UNKNOWN

MTU:  bytes

VLAN Tag ID:

6. Type the IP address that you assigned in SCM. For details, see [“To assign the in-path IP address and the default gateway in SCM” on page 16](#).
7. Type the subnet mask address. The subnet mask on the in-path interface must match the subnet mask on the zone (typically /24, but it can be whatever you specified in the zone settings).
8. Type the IP address that you assigned in SCM for the default gateway. For details, see [“To assign the in-path IP address and the default gateway in SCM” on page 16](#).
9. If the LAN port is part of a VLAN trunk, enter the correct VLAN ID for the in-path.
10. Click **Apply**.
11. You can refine your in-path WAN optimization settings using the SteelHead Management Console. For details, see the *SteelHead User Guide*.

## Troubleshooting

The virtual SteelHead instance is accessible for management and diagnostics via primary and in-path interface.

You cannot ping the in-path interface for the virtual SteelHead instance.

You can ping the primary interface for virtual SteelHead instance.

TCP dumps can be taken to verify and examine traffic flows on following interfaces:

- In-path interface of virtual SteelHead instance
- Knet interfaces of the service virtual machine.

To gather and verify information, check these SteelHead reports:

- Current Connections
- In-path Rule Counters
- Throughput

# Configuring DHCP Options in Zones on SteelHead SD

This topic describes how to configure DHCP options in zones on SteelHead SD appliances. It includes these sections:

- [“Configuring DHCP options on SteelHead SD LAN clients” on page 23](#)
- [“Overriding DNS on guest zones on SteelHead SD” on page 24](#)

These procedures describe how to configure DHCP options in zones on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. For additional information, see the *SteelConnect Manager User Guide*.

## Configuring DHCP options on SteelHead SD LAN clients

SteelHead SD appliances support the ability to configure these DHCP options in zones:

- Preboot Execution Environment (PXE) boot using the Trivial File Transfer Protocol (TFTP)
- Session Initiation Protocol (SIP) server
- HTTP proxy

To create a zone and DHCP options on SteelHead SD LAN clients

1. Choose Network Design > Zones page and select the appliance.
2. Click **New Zone**.
3. Select the site from the drop-down list.
4. Type a name to describe the zone.
5. Optionally, specify the IPv4 network using the a.b.c.d/nn format. This IP address can be autoassigned.
6. When multiple SteelHead SD appliances are available, select the default gateway for this appliance. from the list.
7. Optionally, specify the VLAN tag. Every zone has a VLAN tagged assigned to it. If you leave this option blank the system will automatically assign a VLAN tag to the zone.
8. Click **Submit**.
9. Select the zone from the zones list.

10. Select the DHCP tab.

Figure 3-1. Configuring PXE boot support

The screenshot shows the 'Zones' configuration page on the left and the 'LAN' configuration page on the right. The 'LAN' page has tabs for IP, Gateways, DHCP, VLAN, WAN, Settings, ADDL Networks, and Learned Networks. The 'DHCP' tab is selected. Below the tabs, there is a hint: 'in the site will automatically provide DHCP to the zone using these settings. If you do not use automatic default gateway assignments, you need to manually enable DHCP service in a gateway assignment on the 'Gateways' tab.' Below this, there are fields for 'Range Start' (172), 'Range End' (172), and 'Lease Time' (12:00h). The 'Options' field is highlighted with a red circle and contains the following text:

```
# Example for TFTP boot (BOOTP/PXE)
option filename pxelinux.0
option servername server.mydomain.local
option serveraddress 19

# Example for NTP server
#option ntp-server,19,10.
```

At the bottom right of the 'Options' field, there are 'Cancel' and 'Submit' buttons.

11. To enable PXE boot, in the Options field type:

```
# Example for TFTP boot (BOOTP/PXE)
option filename pxelinux.0
option servername server.mydomain.local
option serveraddress xxx.xxx.x.x
```

12. To enable a SIP server, in the Options field type:

```
# Example for SIP server based on substring match of vendor ID
option vendor:Phone,sip-server,XXX.XXX.XXX.XXX
```

13. To enable a HTTP proxy, in the Options type:

```
# Example for HTTP proxy using vendor attributes
option vendor:Riverbed,42,"address:port"
```

14. Click **Submit**.

## Overriding DNS on guest zones on SteelHead SD

SteelHead SD appliances support the ability to override DNS settings on guest zones in Zones > DHCP tab: DHCP options.

By default, when a zone is created on SteelHead SD appliances, the appliance acts as a DNS server, which can be problematic for guest zones. You can specify a DNS server in DHCP options to avoid this issue.

### To create a guest zone and override DNS settings on SteelHead SD appliances

1. Choose Network Design > Zones page and select the appliance.
2. Click **New Zone**.
3. Select the site from the drop-down list.
4. Type *Guest* to describe the zone.



5. Under Guest zone, click **On**.
6. Optionally, specify the IPv4 network using the a.b.c.d/nn format. This IP address can be autoassigned.
7. When multiple SteelHead SD appliances are available, select the default gateway for this appliance from the list.
8. Optionally, specify the VLAN tag. Every zone has a VLAN tagged assigned to it. If you leave this option blank, the system will automatically assign a VLAN tag to the zone.
9. Click **Submit**.
10. Select the guest zone from the zones list.
11. Select the DHCP tab.

Figure 3-2. Configuring a DNS server on a guest zone

The screenshot shows the SteelHead SD configuration interface. On the left, the 'Zones' panel lists several zones, including 'branch-site-3 > Guest' (VLAN 1013), which is highlighted. On the right, the 'Guest' configuration panel is shown with the 'DHCP' tab selected. The 'DHCP server' section contains a text area for 'Options' with the following content:

```
# Example for NTP server
#option ntp-server,192.168.0.4,10.10.0.5

# Example for DNS server
#option dns-server,192.168.0.1,192.168.0.2
option dns-server,8.8.8.8

# Example for domain search
```

The 'Options' field is highlighted with a red circle. At the bottom right of the configuration panel are 'Cancel' and 'Submit' buttons.

12. In the Options field, enter the public DNS servers and the public DNS server option, for example,

```
# Example for DNS server
option dns-server,192.168.0.1,192.168.0.2
option dns-server,8.8.8.8
```

Multiple DNS servers are separated by a comma.

13. Click **Submit**.



# Configuring Local Subnet Discovery on SteelHead SD

This topic describes how to configure SteelHead SD to discover global and local subnets on the LAN side of the network. It includes these topics:

- [“Overview of local subnet discovery” on page 27](#)
- [“Routing criteria” on page 27](#)
- [“Defining global subnet discovery at the organization level” on page 28](#)
- [“Defining local subnet discovery” on page 30](#)

These procedures describe local and global subnet autodiscovery for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. For detailed information, see the *SteelConnect Manager User Guide*.

## Overview of local subnet discovery

SteelHead SD provides the ability to discover subnets at the zone and site level in a branch. Local subnet discovery identifies routes that are local to a particular branch. These routes can be reached from other sites or branches using the overlay tunnels. Local subnet discovery allows you to define a set of routing criteria so that routes that match the criteria are qualified as subnets local to the branch.

Ideally, all routes learned over the LAN interfaces of an appliance, on a particular branch, should be qualified as routes local to that branch. However, this qualification isn't always straight forward. Consider the case where OSPF is configured with both the LAN zones and the WAN uplinks attached to it. In this case, OSPF will not be able to differentiate the routes that it learns over the LAN zones from the ones that it learns over the WAN uplinks.

A similar problem can arise when BGP is the chosen protocol where an iBGP neighbor is established with the LAN router and an eBGP neighbor is established with the provider-edge router over the WAN uplink. Here BGP will not be able to call out the local subnets implicitly. Another case to consider is when the appliance is placed behind a branch router, it loses the notion of LAN zones and WAN uplinks. The local subnet autodiscovery feature provides a means for identifying subnets that are local to a branch.

## Routing criteria

Local subnet discovery allows you to define a set of routing criteria so that routes that match the criteria are qualified as subnets local to the branch. The routing criteria are:

- **Zone inclusion list** - You select one or more of the configured LAN zones. Routes whose next-hop interface matches one of the selected zones are qualified as local subnets. Preexisting zones that are directly connected to a site are added to the list automatically. You can also manually add other zones. Zones deleted from a site are automatically removed from the list.
- **Uplink inclusion list** - You select one or more of the configured WAN uplinks. Routes whose next-hop interface matches one of the selected WAN uplinks are qualified as local subnets. For example, you might want to attract traffic towards a site for transit purposes. If Site A wants to connect to Site C through Site B. Site B can learn Site C networks via the underlay and make Site A traffic bound for Site C to be forwarded to Site C.
- **Community inclusion list** - You specify a community to include all the routes that carry that community string. The routes matching the community in the community list are reported as local subnets. You can specify multiple communities.
- **Tag inclusion list** - You specify a tag to include all the routes that include the tag. All the routes matching the tag are reported as local subnets from the configured site. You can specify multiple tags.
- **Network prefix inclusion list** - You configure a list of prefixes. If a route for one of the prefixes in the list is received, it is qualified as a local subnet.
- **Next-hop inclusion list** - You configure a list of next-hop prefixes. All routes whose next-hop matches one of the entries in the list are qualified as a local subnet.
- **Community exclusion list** - You specify a tag to exclude all the routes that include the tag. All the routes matching the tag are reported as local subnets from the configured site. You can specify multiple tags.
- **Tag exclusion list** - You specify a tag list to include. You can specify multiple tags. The routes matching the tag list are reported as local subnets. You can list more than one community.
- **Network prefix exclusion list** - You configure a list of prefixes. If a route for one of the prefixes in the list is received, it's not qualified as a local subnet.

**Note:** SteelConnect SDI-2030 and SDI-5030 gateways don't allow you to define routing criteria based on zones and uplinks.

For SteelHead SD, you can create inclusion and exclusion lists at the organization, zone, and site level. For example, you could create an umbrella subnet 10.0.0.0/8 inclusion list at the organization level and then drill down to a particular site to exclude 10.0.0.0/16.

Inclusion lists are applied first, and then exclusions lists will be applied.

## Defining global subnet discovery at the organization level

Users can add an organization level subnet discovery rule under the Global Subnet Discovery tab. This rule will be applied to all sites, unless they are specifically overridden by the site-level subnet discovery rule.

### To define global subnet discovery for an organization

1. Choose Organizations.

2. Select the Global Subnet Discovery tab.

Figure 4-1. Defining organization level subnet discovery

The screenshot shows the RVBD web interface. At the top, there is a navigation bar with tabs: Name / Location, Networking Defaults, Transit, Social Media, Wi-Fi Manager, Numbering Pools, Maintenance, Data Retention, SNMP, Logging, and System Dump. Below this is a sub-navigation bar with tabs: NetFlow, SSH, Legal Disclaimer, Appliance Threshold, Appliance Login, and Global Subnet Discovery (which is highlighted). A note states: "These global defaults will apply to all sites with a SteelHead 570-SD/770-SD/3070-SD/SDI-2030/SDI-5030 Gateway appliance. You can override them on a per site basis." The main content area is divided into two sections: "Inclusion List" and "Exclusion List". The "Inclusion List" section has a table with columns "Included Network / Next-Hop" and "Type". Above the table are buttons "Add Network" and "Add Next-Hop". Below the table is the text "No globally included networks or next-hops". The "Exclusion List" section has a table with columns "Excluded Network" and "Type". Above the table is a button "Excluded Network". Below the table is the text "No globally excluded networks".

3. Click Add Network.

Figure 4-2. Defining included networks

The screenshot shows a dialog box titled "New Included Network". It has a text input field labeled "New Included Network" with a help icon (?) and the value "10.0.0.0/8". At the bottom right, there are two buttons: "Cancel" and "Submit".

4. Specify the IPv4 address, including the network prefix to be included in local subnet autodiscovery.
5. Click **Submit**.
6. Click Add Next Hop.

Figure 4-3. Defining the next hop

The screenshot shows a dialog box titled "New Included Next-Hop". It has a text input field labeled "New Included Next-Hop" with a help icon (?) and the placeholder text "Enter an IPv4 address". At the bottom right, there are two buttons: "Cancel" and "Submit".

7. Specify the IPv4 address for the local-subnet next hop from SteelConnect appliance in this site.
8. Click **Submit**.
9. Click Excluded Networks.

Figure 4-4. Defining excluded networks

The screenshot shows a dialog box titled "New Excluded Network". It has a text input field labeled "New excluded network" with a help icon (?) and the placeholder text "Prefix to be excluded from local subnet discovery". At the bottom right, there are two buttons: "Cancel" and "Submit".

10. Specify the IP address, including the network prefix, to be excluded from local subnet autodiscovery.
11. Click **Submit**.

## Defining local subnet discovery

After you have defined subnet discovery at the organization level, you can drill down to particular sites to define inclusion and exclusion lists. For OSPF routes, make sure that your branch has the LAN zone and WAN uplink attached to it before you begin. For BGP routes, make sure that your branch has the iBGP neighbor defined for the LAN router and the eBGP neighbor defined for the WAN router.

You can also configure community list and tags for subnet autodiscovery. This feature enables the discovery of subnets based on the community or tag present in the route. You can specify the community list and tag for both inclusion and exclusion network lists.

### To define local subnet discovery

1. Choose Network Design to display the sites for the organization.
2. Select the site for which you want to define local subnet discovery.
3. Select the Local Subnet Discovery tab.
4. Select the zone to discover all of the LAN-side subnets routed through the zone's peers. The list includes automatically populated and manually added zones. Preexisting zones that are directly connected to a site are added to the list automatically. You can manually add other zones. Zones deleted from a site are automatically removed from the list.
5. Select the uplink from the Uplinks inclusion list.
6. Under Inherit global, click **On** to globally include subnets and next hops. Whatever subnets were configured for inclusion or exclusion at the organization level can be inherited at the site level.

Figure 4-5. Defining site level subnet discovery

The screenshot displays the 'Local Subnet Discovery' configuration page for 'branch-site-2'. The left sidebar shows a list of sites, including 'branch-site-2', 'branch-office-2', 'branch-site-3', 'branch-office-3', 'branch-site-4', 'branch-office-4', and 'dc-site-1'. The main content area is titled 'branch-site-2' and contains the 'Local Subnet Discovery' tab. Below the title, a note states: 'Applies to any appliance: 570-SD/770-SD/3070-SD/SDI-2030/SDI-5030 Gateway appliance in this site. The inclusion lists will be applied first, then the exclusion lists will be applied.'

The configuration includes the following sections:

- Inclusion List:**
  - Zones inclusion list:** Includes 'branch-site-2 -> LAN [1003]' and 'branch-site-2 -> LAN2 [1004]'.
  - Uplinks inclusion list:** Currently 'Nothing selected'.
  - Inherit global:** Set to 'On'.
  - Community:** Set to '(Optional) Nothing selected'.
  - Tags:** Set to 'Select community tags to create a list'.
- Table of Included Networks:**

	Included Network / Next-Hop	Type
<a href="#">Edit</a> <a href="#">Delete</a>	172.16.4.0/24	Included network
<a href="#">Edit</a> <a href="#">Delete</a>	172.16.5.0/24	Included network
- Exclusion List:**
  - Inherit global:** Set to 'On'.

7. Optionally, specify a community list to include all the routes that carry that community string. The routes matching the community in the community list are reported as local subnets. You can specify multiple communities separated by a comma.

8. Optionally, specify a tag to include all the routes that carry that tag. All the routes matching any tag are reported as local subnets from the configured site. You can specify multiple tags separated by a comma.
9. Click **Add Network**.
10. Specify a network prefix and click **Submit**.
11. Click **Add Next Hop**.
12. Enter the IPv4 address for the next hop, and click **Submit**.
13. Click **Submit**.

### To exclude subnets from local subnet discovery

1. Choose Network Design to display the sites for the organization.
2. Select the site for which you want to define local subnet discovery.
3. Select the Local Subnet Discovery tab.
4. Under Exclusion List, click **On** to globally exclude subnets and next hops. Whatever subnets were configured for inclusion or exclusion at the organization level can be inherited at the site level.

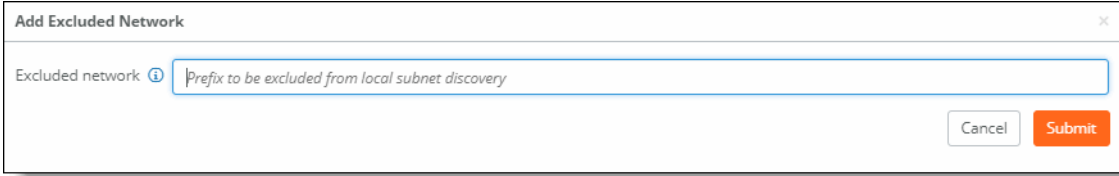
Figure 4-6. Configuring excluded subnets

The screenshot displays the SteelHead SD interface for configuring local subnet discovery at the site level. On the left, the 'Sites' list shows several sites, including 'branch-site-2'. The right pane shows the configuration for 'branch-site-2', with the 'Local Subnet Discovery' tab selected. Under the 'Exclusion List' section, the 'Inherit global' toggle is set to 'On'. Below this, the 'Community' and 'Tags' fields are empty, indicating no specific exclusions are configured at the site level. The 'Included Network / Next-Hop' table lists two networks: 172.16.4.0/24 and 172.16.5.0/24, both marked as 'Included network'. The 'Excluded Network' table is empty, indicating 'No globally excluded networks'.

5. Optionally, specify a community list to exclude all the routes that carry that community string. The routes matching the community in the community list are not reported as local subnets. You can specify multiple communities separated by a comma.
6. Optionally, specify a tag to exclude all the routes that carry that tag. All the routes matching any tag are not reported as local subnets from the configured site. You can specify multiple tags separated by a comma.

7. Click **Submit**.
8. Click **Excluded Networks**.

Figure 4-7. Excluding networks

A screenshot of a web-based dialog box titled "Add Excluded Network" with a close button (X) in the top right corner. The dialog contains a label "Excluded network" followed by a blue circular icon with a question mark. To the right of the label is a text input field with a light blue border and a placeholder text "Prefix to be excluded from local subnet discovery". At the bottom right of the dialog are two buttons: a "Cancel" button with a light gray background and a "Submit" button with an orange background.

9. Specify the network prefix to be excluded from local subnet discovery.
10. Click **Submit**.



# Configuring AutoVPN on SteelHead SD

This topic describes how to configure AutoVPN on SteelHead SD appliances. It includes these sections:

- [“Overview of AutoVPN on SteelHead SD” on page 33](#)
- [“Configuring AutoVPN on SteelHead SD” on page 34](#)

These procedures describe how to configure AutoVPN on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. For additional information, see the *SteelConnect Manager User Guide*.

## Overview of AutoVPN on SteelHead SD

AutoVPN is a SteelConnect feature that connects multiple sites with a secure, full-mesh virtual private network (VPN) without tedious manual configuration. AutoVPN is a fast way to create a resilient VPN backbone between all your sites; however, SteelConnect also provides SwitchVPN to make a zone available in a remote site and Classic VPN for use with third-party gateways.

AutoVPN links the SteelHead SD appliances and SteelConnect gateways at an organization’s sites. SteelConnect automatically sets up a full-meshed VPN configuration in minutes. By default, AutoVPN is on and includes any zones you configure.

For details on configuring AutoVPN in Leaf mode, RouteVPN, and SwitchVPN, see the *SteelConnect Manager User Guide*.

You can configure these options for AutoVPN:

- **AutoVPN priority** - If there are several uplinks available, the system compares the priority and selects the uplink with the higher priority. It is also possible to explicitly disable AutoVPN usage for an uplink. This setting is available on SteelConnect gateways and SteelHead SD appliances.
- **AutoVPN IPv4 target address** - This setting defines the IPv4 address that remote sites use to connect AutoVPN tunnels. By default, the external IP facing towards the internet is used. You can specify an internal interface address, in case it is routed by upstream equipment. You can also specify a custom IPv4 address that remote sites should use when connecting to this uplink. This setting is available on SteelConnect gateways and SteelHead SD appliances.

- **Override AutoVPN port** - Enables a different AutoVPN port for this uplink at the site level. The port is used for the source and target ports for this uplink. The AutoVPN port can only be overridden for SteelHead SD 570-SD, 770-SD, and 3070-SD, and SDI-2030 appliances. A use case for this setting is if you have two high-availability (HA) appliances that have the same public IP. Tunnels with the two HA appliances can't be established, as they would appear identical. Overriding the AutoVPN port ensures tunnels with the two HA appliances are using different ports and can be established.

## Configuring AutoVPN on SteelHead SD

This section describes the procedures for configuring AutoVPN on SteelHead SD.

### To configure AutoVPN on SteelHead SD

1. Choose Network Design > Uplinks page and select the appliance.
2. Click the **AutoVPN** tab.

Figure 5-1. Configuring the AutoVPN

The screenshot shows the configuration page for an uplink named "-Internet-Uplink-1". The "AutoVPN" tab is selected. The page contains two main sections:

- AutoVPN priority**: A description states that this defines the order of preference for uplinks. The "AutoVPN priority" dropdown is set to "Normal".
- AutoVPN IPv4 target address**: A description states that this defines how to determine the IPv4 address for remote sites. The "AutoVPN IPv4 selection" dropdown is set to "Auto-Detect Internet IPv4 (recommended for internet uplinks)".

Below these sections are two toggle controls:

- Override AutoVPN port**: A description states that this can only be overridden for specific appliances. The toggle is currently set to "On".
- AutoVPN Port**: A text input field containing the value "4500".

Each section and the toggle controls have "Cancel" and "Submit" buttons.

3. Under AutoVPN priority, select one of these options:
  - **Don't use this uplink for AutoVPN** - Disables AutoVPN on this uplink.
  - **Low** - Sets the uplink to the lowest priority.
  - **Normal** - Sets the uplink to the normal priority.
  - **High** - Sets the uplink to the high priority.
4. Click **Submit**.

5. Under AutoVPN IPv4 target address, select one of these options:
  - **Auto-Detect Internet IPv4 (recommended for internet uplinks)** - The system automatically detects the external IP that is facing towards the internet. This is the default setting.
  - **Internal Interface IPv4 (recommended for private WAN)** - Specify an internal IPv4 IP address. Use the internal interface address, if it is routed by upstream equipment.
  - **Specify custom IPv4** - Specify a custom IPv4 target IP address that remote sites can use when connecting to this uplink.
6. Click **Submit**.
7. Under Override AutoVPN port, click **On** to enable a different AutoVPN port for this uplink. The port is used for the source and target ports for this uplink. The default setting is **Off**.

If you have two high-availability (HA) sites that have the same public IP. You must override the AutoVPN port to ensure tunnels between the two HA sites are established.
8. Specify the port number.
9. Click **Submit**.



# Defining VLAN Trunk Ports on SteelHead SD

This topic describes how to configure VLAN trunk ports for multiple zones on SteelHead SD. It includes these sections:

- [“Overview of multizone VLAN trunk mode on SteelHead SD” on page 37](#)
- [“Defining trunk mode on ports” on page 38](#)

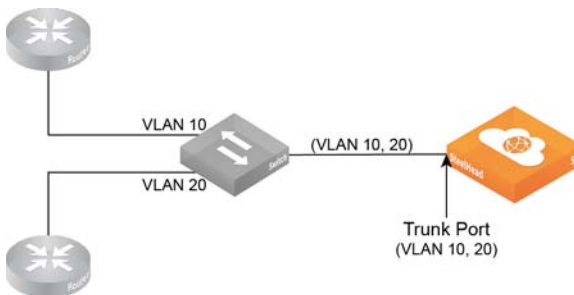
These procedures describe how to configure multizone VLAN trunk ports on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. For details on VLANs, see the *SteelConnect Manager User Guide*.

## Overview of multizone VLAN trunk mode on SteelHead SD

Multiple VLANs are very common in Layer 2 (L2) network environments on the LAN side. With this feature, you can configure multiple VLANs on the same LAN port (that is, trunk port functionality). VLANs are used for segmenting networks at L2 and provide basic security for network traffic by limiting broadcast domains and network flooding.

SteelHead SD supports trunk mode VLANs for zones. You can define a trunk port on a zone and configure it with different VLANs. For example, you can have a trunk port on the LAN side with two zones configured with different VLANs.

Figure 6-1. Multiple zones with different VLANs



## Defining trunk mode on ports

To define trunk mode ports

1. Choose Network Design > Zones to create a zone for the SteelHead SD. For details, see the *SteelConnect Manager User Guide*.

2. Click the VLAN tab.

Figure 6-2. Creating a VLAN trunk

The screenshot shows the 'Branch10\_1100' configuration window in the SteelHead SD interface. The 'VLAN' tab is selected in the top navigation bar. The 'VLAN tag' section has a text input field containing '1100'. Below this, the 'Policy tags' section shows a dropdown menu with 'Nothing selected'. The 'Management zone' section has a toggle switch for 'Management Zone' set to 'On'. The 'VLAN Specifications' section includes input fields for 'MTU' (1500) and 'ARP aging timeout' (3600), and a toggle switch for 'Enable VLAN' set to 'On'. 'Cancel' and 'Submit' buttons are located at the bottom right of the configuration area.

3. Specify a VLAN tag, if necessary. Every zone has a VLAN tag assigned. If you leave this field empty, the system picks a free VLAN ID from the pool.
4. Click **Submit**.
5. Choose Appliances > Ports to configure the trunk port.
6. Select the site and appliance from the drop-down list.

- Click the port for which you want to create the VLAN trunk. For example, LAN0\_0.

Figure 6-3. Creating a LAN trunk port

**LAN0\_0**

**Info/Mode** | MACs/Devices | Counters

**Info**

Port label LAN0\_0

Link status **Up** 1G

STP status *Unknown*

STP priority Disabled

Site branch-site-2

Appliance branch-site-2

▶ [HA] 770-SD HA Backup

Type Discrete

MAC FA:16:3E:FA:0D:10

LLDP *Unknown*

remote

RX bytes 3795947 ~ 3706k +574

RX packets 46773 ~ 45k +7

RX errors ...

TX bytes 3708630 ~ 3621k +574

TX packets 45910 ~ 44k +7

TX errors ...

**Mode**

Port mode Trunk Port

Zones Nothing selected

Cancel Submit

**Port Description**

Port description Port description (limit 16 characters)

- Under Port mode, select Trunk Port from the drop-down list.

---

**Important:** For 2030 appliances, if the port has already been set to either Singlezone or Trunk Port, you must first disable the port before making a change to the Port mode. For example, if the port is already set to Singlezone, you must first disable the port, then set the port to Trunk Port.

---

- Click **Submit**.
- Navigate back to Appliances > Zones to enable VLAN on the configured port.
- Under Management Zones, click **On** and **Submit** to activate multizone (VLAN trunk) connectivity for this zone.
- Under VLAN Specifications, to enable VLAN click **On** and **Submit** to enable VLAN on the trunk port you have configured.
- Optionally, you can define:
  - MTU** - The MTU is the largest physical packet size, measured in bytes, that a network can send. The default value is 1500.

- **ARP aging timeout** - Sets how long, in seconds an ARP entry stays in the cache before the cache refreshes. The default value is 1500.

Figure 6-4. VLAN enabled on the trunk port for the zone

The screenshot shows the configuration page for a zone named 'Branch10\_1100'. The 'VLAN' tab is selected in the top navigation bar. The page contains the following sections:

- VLAN tag**: A text field labeled 'VLAN Tag' with the value '1100'.
- Policy tags**: A section with a note: 'When assigning policy tags to a zone, users that match one of the tags will be automatically assigned to this zone when they connect one of their devices to the network.' Below this is a 'Policy tags' field with a dropdown menu showing 'Nothing selected'.
- Management zone**: A section with a note: 'Activate if this zone is the management zone for the site. Switches and access points will use this zone to configure their own dynamic IPs with DHCP.' Below this is a 'Management Zone' toggle switch set to 'On'.
- VLAN Specifications**: A section with a note: 'Specify the zone's shut/no shut behaviour mtu and arp-aging-timeout(Only for catfish3 zones that are associated with a port)'. It contains two text fields: 'MTU' with the value '1500' and 'ARP aging timeout' with the value '3600'.
- Enable VLAN**: A toggle switch at the bottom set to 'On'.

14. Click **Submit**.

15. Repeat [Step 1](#) through [Step 14](#) to create additional trunk ports with different VLANs.



# Configuring BGP, OSPF, Static Routing, and Route Retraction on SteelHead SD

This topic describes how to configuring SteelHead SD Border Gateway Protocol (BGP), open shortest path first (OSPF) with an area border router (ABR), static routing, and route retraction. It includes these sections:

- [“Configuring BGP on SteelHead SD” on page 41](#)
- [“Configuring OSPF with ABR on SteelHead SD” on page 55](#)
- [“Defining static routes on SteelHead SD appliances” on page 66](#)
- [“Route retraction for SteelHead SD” on page 67](#)

---

**Important:** Before you begin configuring BGP and OSPF for SteelHead SD, we recommend you read the *SteelConnect Manager User Guide*. The procedures here provide the basic steps for configuring SteelHead SD appliances.

---

## Configuring BGP on SteelHead SD

This section describes how to configuring BGP on SteelHead SD. It includes these sections:

- [“BGP on SteelHead SD overview” on page 42](#)
- [“Enabling BGP and configuring BGP neighbors on SteelHead SD” on page 42](#)
- [“Configuring BGP routing policies” on page 44](#)
- [“Configuring BGP path selection” on page 45](#)
- [“Configuring BGP inbound and outbound prefixes” on page 46](#)
- [“Configuring BGP route redistribution” on page 47](#)
- [“Configuring conditional default-route originate routing” on page 48](#)
- [“Configuring the BGP origin-type attribute” on page 49](#)
- [“Enabling multi exit discriminator \(MED\) settings” on page 51](#)
- [“Configuring BGP route summarization” on page 52](#)
- [“Viewing BGP status” on page 55](#)

## BGP on SteelHead SD overview

SteelHead SD provides full BGP support for local autonomous system (AS) numbers and neighbor configurations (including router ID, password, keepalive time, and hold time) for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

SteelHead SD provides support for both exterior Border Gateway Protocol (eBGP) and interior Border Gateway Protocol (iBGP). SteelHead SD doesn't restrict BGP to the LAN or the WAN; it can communicate with its associated neighbors regardless of whether it is on the LAN or WAN.

You can configure BGP regardless of whether it is a zone or an uplink.

---

**Important:** Before you begin configuring BGP for SteelHead SD, we recommend you consult the *SteelConnect Manager User Guide*.

---

## Enabling BGP and configuring BGP neighbors on SteelHead SD

This section describes how to enable BGP and configure BGP neighbors on branch SteelHead SD appliances. By default, BGP is disabled.

**Note:** For SteelHead SD appliances, you can only add BGP neighbors under the Appliances > BGP tab. You can't add BGP neighbors from the Routing > BGP page.

### Branch community list

SteelConnect 2.12 enables you to specify a branch community for BGP configurations. Every site has a default branch community configured automatically. You can override the default branch community by attaching a community list created based on your requirements. You can create a community under Routing > Community List. For details, see ["Creating routing community lists" on page 73](#).

The prefixes reported from a site are tagged with the branch community of its own site and with the branch community of the site where the prefix is configured. When the branch community is updated all the prefixes reported are updated with the revised branch community. When a community in the branch-community configuration is removed, the branch community is updated with the default value.

### To enable BGP and configure a BGP neighbor

1. Choose Appliances and select the appliance to expand the pane.
2. Select the BGP tab.
3. Specify an AS number in Local AS to start a BGP session. The range is from 1 to 4294967295.
4. Click the search selector and select a branch community from the list. If no branch community is selected, the appliance receives a unique string.

- Under BGP neighbors, click **Add BGP Neighbor**.

Figure 7-1. Creating a BGP neighbor

**Add BGP Neighbor**

Name

IPv4 address

Remote AS

Password

Keep alive time

Hold time

Weight

Next hop self

Default route originate

**Inbound**

Prefix list

AS list

Route map

**Outbound**

Prefix list

AS list

Route map

- Specify a name for the BGP neighbor.
- Specify the IP address of the BGP neighbor.
- Specify the remote AS number that the BGP peer belongs to: for example, 200. The range is from 1 to 4294967295.
- The remainder of the BGP attributes are provided by default. They can be changed based on your administrator settings. Optionally, fill out these BGP neighbor attributes:
  - Password** - Optionally, type a password to enable MD5 authentication. You must use the same password on both BGP neighbors. If you do not require MD5 authentication, you can leave this field blank.
  - Click the eye icon to see the password as you type. The view persists until you click the eye icon again to hide the password.
  - Keep Alive Time** - Optionally, specify the amount of time, in seconds, that the eBGP neighbors exchange keepalive messages to determine whether a link has failed or is no longer available. The neighbors exchange keepalive messages often enough so that the hold time doesn't expire. The default setting is 60.
  - Hold Time** - Optionally, specify the amount of time, in seconds, that a gateway neighbor waits for an incoming keepalive, update, or notification message from a neighbor before it assumes its neighbor is down. If the gateway doesn't receive a keepalive, update, or notification message from its neighbor within the period specified, it closes the connection and routing through that neighbor becomes unavailable.

A 0 value means that no keepalive messages are sent and the connection will never close. The hold-time range is from 0 to 65535. The default setting is 180.

The hold-time value is three times the interval at which keepalive messages are sent. Using the default values for the keepalive time of 60 and the hold time of 180, the settings work together like this: after two neighbors establish an eBGP session, 60 seconds later they'll each send a keepalive message. When a gateway receives a keepalive message from its neighbor, that gateway's hold time for the session will have counted down from 180 to 120, but it's then reset to 180. This process continues every 60 seconds. However, should neighbor A lose power, then neighbor B won't receive any keepalives. So after 180 seconds, neighbor B determines that neighbor A is down and closes the session.

- **Weight** - Specify the BGP weight value to the routes received from the BGP neighbor. A route with a high weight value is preferred among multiple routes with the same destination. The default value is range is 2 to 65534. For details on how the weight metric is used in BGP path selection, see [“Configuring BGP path selection” on page 45](#).
- **Next hop self** - Click **On** to change the next hop attribute for received updates to its own IP address. Enable this option to change the next-hop attribute for external networks that will be advertised to branch route.

When routes from another AS are learned via the eBGP neighbor, the next hop for that route isn't changed when it is passed to its iBGP peers. As an iBGP peer may not be aware of next hop of the external route, that route becomes unreachable for the iBGP peer. If the iBGP neighbor is configured with the Next-hop self option, the next hop is changed to its own interface address which is reachable from the iBGP neighbor.

- **Default route originate** - Click **On** to distribute the default route (0.0.0.0/0) to the specified BGP neighbor. The default setting is **Off**.

**Route map** - Click the search selector and select the route use case. The routing policies defined by the selected route map are applied while accepting routes to the BGP neighbor.

10. Click **Submit**.

11. Repeat [Step 5](#) through [Step 10](#) if you have two MPLS providers that need to do BGP peering with the current appliance. You need to create a BGP configuration for each one.

12. Repeat this process for other SteelHead SDs behind other routers.

**Note:** BGP redistribution and summarization can only be configured after you have defined route maps and prefixes.

## Configuring BGP routing policies

Optionally, you can configure BGP routing policies by defining inbound and outbound prefixes, AS paths, and route maps for BGP neighbors. By specifying these options, you can define what inbound and outbound routes are allowed or denied for BGP neighbors.

We recommend you define route maps, AS lists, and prefix lists before you configure the inbound and outbound settings. For details on configuring routing policies, see [“Overview of routing policies on SteelHead SD” on page 69](#).

## Configuring BGP path selection

BGP path selection uses a defined set of criteria to determine the most efficient route through a network. The criteria is listed in the same order in which BGP uses them to select the optimal routes to be injected into the IP routing table.

1. **Highest weight** - You configure this value when you configure BGP neighbor (Appliances > BGP tab: Add BGP Neighbor). A route with a high weight value is preferred among multiple routes with the same destination. For details, see ["Enabling BGP and configuring BGP neighbors on SteelHead SD" on page 42](#).
2. **Highest local preference** - you configure this value when you create BGP routing policies (Routing > Route Maps: Add Route Map). For example, when you create a route map with the use case: Policies at the BGP neighbor level. The default value for the local preference is 100. If a route has no local preference specified it is treated as if it had a local preference of 100. If the iBGP speaker receives multiple routes to the same destination, then the route with the highest value is preferred. For details, see ["Configuring route maps" on page 76](#).
3. **Locally generated** - Prefer a route that is locally sourced. The best path selection algorithm uses this criteria to prefer paths that originate locally with a network statement, an aggregate statement or the redistribution of a route between local routing protocols. Aggregating network routes into one makes internet routing more efficient by saving network space. You don't need to configure this setting because the gateway is able to deduce the information it is generating itself locally rather than learning it from a nonlocal source. This data is never passed outside of the local route selection process and is purely internal to the local router.
4. **Shortest AS path** - You configure this value when you create BGP routing policies (Routing > Route Maps: Add Route Map). For example, when you create a route map with the use case: Default route origination in BGP for a neighbor. For details, see ["Creating routing AS path lists" on page 74](#) and ["Configuring route maps" on page 76](#).
5. **Origin type** - You configure this value when you create BGP routing policies (Routing > Route Maps: Add Route Map). For example, when you create a route map with the use case: Policies at the BGP neighbor level. The lowest origin type is the preferred path: IGP is lower than EGP, and EGP is lower than Incomplete. Only the routes with the lowest origin value are considered when multiple routes share the shortest AS path, then the algorithm continues by considering the multi exit discriminator (MED) settings. For details, see ["Configuring route maps" on page 76](#).
6. **Lowest MED** - You configure this value when you configure BGP (Appliances > BGP tab). MED is a BGP path attribute that can influence the route selection process. MED breaks the tie between the two routes when the weight, local preference, AS-Path, and origin type are same. ["Enabling multi exit discriminator \(MED\) settings" on page 51](#).
7. **eBGP over iBGP** - External BGP routes are preferred over internal BGP routes. iBGP or internal BGP runs within the same AS, whereas eBGP or external BGP operates between autonomous systems.
8. **IBP metric** - You configure this value when you create BGP routing policies (Routing > Route Maps: Add Route Map). For example, when you create a route map with the use case: Policies at the BGP neighbor level. If there is no external route selection path, the path with the lowest IGP value to the next hop is preferred. The IGP route is interior to the AS of origination. For details, see ["Configuring route maps" on page 76](#).
9. **Route age** - Routes with a longer age are preferred over "newer" routes or routes with a shorter age

10. **Router ID** - The path that originates from the BGP router with the lowest router ID is preferred. The router ID can be set manually and refers to the IP address with the highest router value. The router ID is the final tiebreaker in the BGP route selection process if there are multiple identical prefixes learned in the RIB. Typically, a tie break is found before the router ID but it is guaranteed to be different since two routers cannot have the same IP address within the same routing domain. SteelConnect doesn't support VRF so everything is in the same routing domain and the system doesn't overlap or duplicate addresses.

## Configuring BGP inbound and outbound prefixes

Outbound fields are disabled if a cluster site is selected as a transit hub for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances. For details on configuring transit hubs, see the *SteelConnect Manager User Guide*.

To configure inbound and outbound BGP route settings

1. Choose Appliances and select the appliance to expand the pane.
2. Select the BGP tab.

Figure 7-2. Configuring inbound and outbound settings

The screenshot shows a configuration window with two sections: 'Inbound' and 'Outbound'. Each section contains three dropdown menus: 'Prefix list', 'AS list', and 'Route map'. All dropdowns currently show '(Optional) Nothing selected'. At the bottom right of the window are 'Cancel' and 'Submit' buttons.

3. Under Inbound, fill out these attributes:
  - **Prefix list** - Specify the prefixes to be allowed or denied for route advertisements from the BGP neighbor to the appliance.
  - **AS list** - Specify the AS paths. The route from the neighbor is permitted if the AS path matches the regular expression in the AS path list.
  - **Routemap** - Specify route policy for the BGP neighbor. The routing policies defined by the selected route map are applied while accepting routes from the BGP neighbor.
4. Under outbound, fill out these attributes:
  - **Prefix list** - Specify the prefixes to be allowed or denied for route advertisements to the BGP neighbor from the appliance.
  - **AS list** - Specify the AS paths. The route to the neighbor is permitted if the AS path matches the regular expression in the AS path list.
  - **Routemap** - Specify the route policy for the BGP neighbor. The routing policies defined by the selected route map are applied while accepting routes to the BGP neighbor.

5. Click **Submit**.

**Note:** After the BGP neighbor is created, it appears in the BGP neighbors list. Click **Edit** to modify neighbor settings.

## Configuring BGP route redistribution

SteelHead SD includes BGP options to globally configure:

- redistribution of OSPF routes into BGP.
- redistribution of static routes into BGP.
- redistribution of overlay routes into BGP.
- redistribution of traffic using the route map with the use case for static and connected route injection in BGP.

---

**Important:** We recommend you define route policies, AS lists, and prefix lists before you configure BGP route redistribution. For details on configuring routing policies, see [“Creating routing IPv4 prefix lists” on page 72](#).

---

In SteelConnect 2.12, you can differentiate between static and overlay routes. Previously, there was no differentiation between overlay and static routes. To avoid this ambiguity, you can configure the Overlay to BGP option to distinguish overlay routes from static routes. The policies applied on redistribution of other routes are also applicable on overlay routes

### To configure BGP route redistribution

1. Choose Appliances and select the appliance to expand the pane.
2. Select the BGP tab.

Figure 7-3. Configuring BGP route redistribution

The screenshot shows the configuration page for [HA] 770-SD. The 'BGP' tab is selected in the top navigation bar. The 'Local AS' is set to 65510. The 'Branch Community' dropdown is set to 'If none of the strings are selected, the appliance will receive a unique string for the site'. Under 'Redistribute settings', the following options are visible:

- OSPF to BGP:** On (green button), Off (grey button)
- Route map:** (Optional) Nothing selected
- Static to BGP:** On (grey button), Off (red button)
- Overlay to BGP:** On (green button), Off (grey button)
- Route map:** (Optional) Nothing selected
- Sites:** Apply config to selected sites
- Connected to BGP:** On (green button), Off (grey button)
- Route map:** (Optional) Nothing selected

At the bottom right, there are 'Cancel' and 'Submit' buttons.

3. Specify an AS number in Local AS. The range is from 1 to 4294967295.
4. Click the button to list the branch community strings and select one for this site.

The Branch Community option is per site and takes a community list as an argument. Every site will have a default branch community configured. You can override the default branch community by attaching a community list. The prefixes reported from a site are tagged with the branch community of its own site and with the branch community of the site where the prefix is specified.

5. Specify your BGP redistribution settings:

- **OSPF to BGP** - Click **On** to enable redistribution of OSPF routes into BGP. By default, redistribution is disabled.

**Route Map** - Click the search selector to select the route map. This option only applies to route maps with the use cases: OSPF route injection in BGP or User defined route map. This option redistributes OSPF routes in BGP using a list of IPv4 prefixes.

- **Static to BGP** - Click **On** enable redistribution of static routes into BGP. By default, redistribution is disabled.

**Route Map** - Click the search selector to select the route map. This option only applies to the route maps with the use cases: Static and connected route injection in BGP or User defined route map. This option redistributes static and connected routes in BGP using a list of IPv4 prefixes.

- **Overlay to BGP** - Click **On** enable redistribution of overlay routes into BGP. By default, redistribution is disabled. Configuring overlay routes takes effect immediately.

**Route Map** - - Click the search selector to select the route map. This option only applies to the route maps with the use cases: Static and connected route injection in BGP or User defined route map. This option redistributes static and connected routes in BGP using a list of IPv4 prefixes.

- **Sites** - Click the search selector to select the site. Overlay routes can also be redistributed based on the sites they are reported from. If no site is chosen, the prefixes from all the sites are redistributed. Sites can be added or removed. Any update to the route-map or the sites takes effect in about 60 seconds.

- **Connected to BGP** - Click **On** or **Off** to enable redistribution of connected routes into BGP. By default, redistribution is disabled.

**Route Map** - - Click the search selector to select the route map. This option only applies to the route maps with the use cases: Static and connected route injection in BGP or User defined route map. This option redistributes static and connected routes in BGP using a list of IPv4 prefixes.

6. Click **Submit**.

For details on configuring route maps, see [“Configuring route maps” on page 76](#).

## Configuring conditional default-route originate routing

Typically, when the default-route originate attribute is configured, the default route is sent to the BGP neighbor without any conditions. To support a conditional default-originate route, a route-map is attached to the default route origination configuration and it is sent to the specified neighbor only when the route map matches at least one prefix in the IP routing table.



You configure the conditional default-route originate attribute when you create a BGP route-map with the use case: Default route origination in BGP for a neighbor.

For details on configuring route maps, see [“Configuring route maps” on page 76](#).

#### To configure conditional default-route originate

1. Create a non-empty prefix list. For details, see [“Creating routing IPv4 prefix lists” on page 72](#).
2. Create a route map with the use case: Default route origination in BGP for a neighbor. For details, see [“Configuring route maps” on page 76](#).
3. In the Route Maps list, select the route map you created.
4. Select the Match Criteria tab.
5. Under IP list, select created prefix list.
6. To define the match and set criteria, select the route map to expand the page.
7. Fill out the fields for the match and set criteria. The criteria differ according to the use case you have chosen. For details, see [“Configuring route maps” on page 76](#).
8. Choose Appliances and select the appliance to expand the pane.
9. Select the BGP tab.
10. Specify an AS number in Local AS to start a BGP session. The range is from 1 to 4294967295.
11. Click the search selector and select a branch community from the list. If no branch community is selected, the appliance receives a unique string.
12. Under BGP neighbors, click **Add BGP Neighbor**.
13. Fill out the BGP neighbor attributes. For details, see [“Enabling BGP and configuring BGP neighbors on SteelHead SD” on page 42](#).
14. Under Default route originate, click **On** to distribute the default route (0.0.0.0/0) to the specified BGP neighbor. The default setting is **Off**.
15. Under route map, click the search selector and select the route map you created for the use case: Default route origination in BGP for a neighbor and click **Submit**.

## Configuring the BGP origin-type attribute

When you configure BGP on SteelHead SD appliances, it receives multiple paths to the same destination.

The origin-type path attribute in a BGP update message that indicates the origin of the path. The origin-type attribute enables you to select the best path for the BGP route.

SteelHead SD supports these origin-types:

- **IGP** - The route is interior to the AS of origination. The routes received from BGP in this session are marked as IGP.
- **EBP** - Network layer reachability information (NLRI) is learned via EGP, as indicated by “e” in the BGP table.

- **Incomplete** - The routes that are redistributed into BGP from other protocols. The prefix originates from an aggregate statement or via redistribution of a static route.

The lowest origin type is the preferred path: IGP is lower than EGP, and EGP is lower than Incomplete. Only the routes with the lowest origin value are considered when multiple routes share the shortest AS path, then the algorithm continues by considering the multi exit discriminator (MED) settings. For details, see ["Enabling multi exit discriminator \(MED\) settings" on page 51](#) and ["Configuring BGP path selection" on page 45](#).

You set the origin type when you create a route-map that has the use case: Policies at the BGP neighbor level use case. Enabling the origin-type attribute in a BGP route map enables you to filter the routes or change the origin type of routes received from a BGP neighbor. For details, see ["Configuring BGP path selection" on page 45](#).

---

**Tip:** You can also set the origin-type attribute in use case: User defined route map. This use case enables you to define a route map using any of the match and set criteria that are available in all the route-map use cases. For details on route maps and use cases, see ["Configuring route maps" on page 76](#).

---

### To create a route map with the origin-type attribute

1. Choose Routing > Route Map.
2. Click **Add Route Map**.
3. Specify a name for the route map. Make sure you use a descriptive name to help you differentiate this route map.
4. Select the use case: Default route origination in BGP for a neighbor.
5. Click **Submit**.
6. Select the new policy to expand the page.

Figure 7-4. Configuring the origin-type attribute

The screenshot shows the 'policybgpneighbor' configuration page with the 'Match Criteria' tab selected. The page has a header with the title 'policybgpneighbor', an 'Actions' dropdown, and a close button. Below the header are three tabs: 'Info', 'Match Criteria' (active), and 'Set Criteria'. The 'Match Criteria' section contains several input fields:

- Origin type:** A dropdown menu with the placeholder text 'Select origin type'.
- Community:** A list box with one item: '(Optional) Nothing selected'.
- Next hop list:** A list box with one item: '(Optional) Nothing selected'.
- Metric:** A text input field with the placeholder text '(Optional) (0-4294967295)'.
- Tag:** A text input field with the placeholder text '(Optional) (0-4294967295)'.

At the bottom right of the form are 'Cancel' and 'Submit' buttons.

7. Select the origin type from the list:
  - **igp** - Set the prefix to originate from routing information learned from the interior gateway protocol (IGP) such as OSPF.
  - **egp** - Network layer reachability information (NLRI) is learned via EGP, as indicated by “e” in the BGP table.
  - **incomplete** - Set the prefix to originate from an aggregate statement or via redistribution of a static route.
8. Specify the remaining match criteria. For details, see [“Configuring route maps” on page 76](#).
9. Click **Submit**.

## Enabling multi exit discriminator (MED) settings

In BGP path selection, you configure MED attributes when there are multiple paths to a destination prefix that have the same local preference and the same AS path length. The purpose of the MED settings is to select the best path when there are multiple connections between two autonomous systems.

The MED attribute is applied to outbound routes, dictating the best inbound path into the AS (assuming multiple paths exist). When a BGP speaker learns a route from a peer, it can pass the route's MED to any iBGP peers, but not to eBGP peers. As a result, the MED has relevance only between neighboring autonomous systems.

MED is a BGP path attribute that can influence the route selection process. MED breaks the tie between the two routes when the weight, local preference, AS-Path, and origin type are same. For details, see [“Configuring BGP path selection” on page 45](#).

You can configure these MED types:

- **Deterministic MED** - Enabling this option ensures the comparison of the MED variable when choosing routes advertised by different peers in the same autonomous system.
- **Always-compare MED** - Enabling this option ensures the comparison of the MED for paths from neighbors in different autonomous systems.

### To enable multi-exit discriminator settings

1. Choose Appliances and select the appliance to expand the pane.

## 2. Select the BGP tab.

Figure 7-5. Configuring MED settings

770-SD

Actions X

Live IPs AutoVPN System dump Tools HA Routing **BGP** Services NetFlow

**Location**

Static to BGP *i*

Overlay to BGP *i*

Connected to BGP *i*

Route map *i* • (Optional) Nothing selected

**Multi exit discriminator settings**

Deterministic MED *i*

Always\_compare MED *i*

## 3. Under Multi exit discriminator, enable one of these MED settings:

- **Deterministic MED** - Click **On** to ensure the comparison of the MED variable when choosing routes advertised by different peers in the same AS. The default value is **Off**.
- **Always\_compare MED** - Click **On** to ensure the comparison of the MED for paths from neighbors in different autonomous systems. This setting useful when multiple service providers or enterprises agree on a uniform policy for setting MED. The default value is **Off**.

4. Click **Submit**.

## Configuring BGP route summarization

With route summarization, a new network prefix with a shorter prefix length is advertised into BGP. Summarizing prefixes conserves router resources and accelerates best path calculation by reducing the size of the BGP table. Summarization also provides increased stability by reducing routing loops.

You can configure BGP route summarization using one of these modes:

- **Manual** - Creates a static route and advertises the network via a network statement. The summary route will always be advertised even if the networks are not available.
- **Automatic** - Creates a network range. When viable routes that match the network range enter the BGP table, an aggregate route is created. On the originating router, the aggregated prefix sets the next hop to Null 0. The route to Null 0 is automatically created by BGP to prevent routing loops.

When configured, the routing policy advertises a summary address only and not the individual prefixes to a BGP neighbor.

**Note:** Routing policies only impact the underlay routing. They do not impact the overlay routing orchestrated by SCM.

### To configure BGP route summarization

1. Choose Appliances and select the appliance to expand the pane.
2. Select the BGP tab.
3. Under Summarization, click **Add Prefix**.

You can configure one or more summary addresses matching the individual addresses to advertise to a BGP neighbor. You can also advertise individual addresses. By default, only summary addresses are advertised.

Figure 7-6. Adding AS summarization prefixes

The system default is to calculate the prefix manually.

4. Click **Automatic** to have the system calculate the prefixes automatically, or click **Manual** to specify the prefix.
  - For automatic prefix calculation, specify a starting and an ending address, and SteelConnect provides the summarized prefix. For example, entering the starting address 160.0.1.0 and the ending address 160.0.2.0 results in the automatic prefix 160.0.0.0/22.
  - For manual prefix calculation, after Summarized Prefix, enter a static IP address with a netmask.
5. Specify the prefix starting and ending point.
6. Specify an IP address for the range of addresses including the prefix length in the Summarized Prefix text box.
7. Specify your summary and AS-set settings:
  - **Summary Only** - Click **On** to advertise both summary and individual prefix advertisements to an eBGP peer.
  - **AS-set** - Click **On** to provide an AS-set to use to detect and avoid routing loops. An AS-set summarizes the path attributes of all the BGP individual routes that the aggregate summarizes to help detect and avoid BGP routing loops.
8. Click **Submit**.

## Resetting BGP sessions

If a BGP routing policy changes due to a configuration change, the BGP neighbors must be reset. Configurable routing policies for a neighbor may impact inbound or outbound routing table updates. Whenever there is a change in the routing policy, the BGP session must be cleared or reset for the new policy to take effect.

Resetting BGP sessions can be done at two levels

- at the neighbor level
- at global level

### To configure BGP neighbor reset

1. Choose Appliances and select the appliance to expand the pane.
2. Select the BGP tab.

Figure 7-7. Resetting BGP sessions

The screenshot shows the configuration interface for a SteelHead SD appliance, specifically the BGP tab. The interface includes a top navigation bar with tabs for Live, IPs, AutoVPN, System dump, Tools, HA, Routing, BGP (selected), Services, and NetFlow. Below the navigation bar, there is a 'Location' section with a 'Route map' dropdown set to '(Optional) Nothing selected'. The 'Multi exit discriminator settings' section contains two toggle switches: 'Deterministic MED' and 'Always\_compare MED', both currently set to 'On'. The 'BGP neighbor reset' section includes a 'Reset type' dropdown set to 'Soft reset', a 'Reset options' dropdown set to 'Selected BGP neighbor', and a 'BGP neighbors' dropdown set to 'Nothing selected'. At the bottom right, there are 'Cancel' and 'Submit' buttons.

3. Under BGP neighbor reset, specify these settings to reset BGP neighbors:
  - **Reset Type** - Select one of these options:
    - **Soft reset** - A soft refreshes the route updates without tearing down existing peering sessions. A soft reset uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. A soft reset is recommended for reconfiguring the routing table.

- **Hard reset** - A hard reset tears down the connection between peers including the TCP connection and deletes routes coming from the specified peer. Session will reestablish from the start once hard reset is done. The prefixes in the BGP, IP, and Forwarding Information Base (FIB) tables provided by the neighbor are lost. A hard reset is not recommended. Clearing a BGP session using a hard reset invalidates the cache and results in a negative impact on the network performance when the information in the cache becomes unavailable. A hard reset is also disruptive because active BGP sessions are torn down.
  - **Soft inbound reset** - A soft inbound reset is the same as soft reset but refreshes only the inbound route table updates.
  - **Soft outbound reset** - A soft outbound reset is the same as soft reset but refreshes only the outbound route table updates.
4. Under Reset options, select:
    - Selected BGP neighbor to reset the BGP session at the neighbor level.
    - All BGP neighbors to reset the BGP session at a global level. Be advised that when you specify this option, the BGP tab disappears as it is applicable to all BGP neighbors.
  5. Click the search selector to select the BGP neighbor for which you want to reset the session.
  6. Click **Submit**.

## Viewing BGP status

SCM displays the advertised and learned network routes and peering session state information. To filter the list, type a search filter in the search box; for example, type IPv6 to narrow the search to all IPv6 networks.

### To view BGP neighbors

1. Choose Appliances and select the appliance you want to view.
2. Click the BGP tab to view the BGP neighbors state, received prefixes, remote AS, keep-alive value, hold time, and last error. You can edit BGP values as well.

### To view BGP routing tables

1. Choose Health Check > Routing Tables.
2. Select the BGP tab and select the appliance to display the BGP learned and advertised routes.

## Configuring OSPF with ABR on SteelHead SD

This section describes how to configure OSPF with ABR on SteelHead SD. It includes these sections:

- [“Introducing OSPF with ABR” on page 56](#)
- [“Creating an OSPF network” on page 56](#)
- [“Configuring OSPF interfaces” on page 59](#)
- [“Creating OSPF areas” on page 60](#)

- [“Configuring redistribution settings for OSPF” on page 62](#)
- [“Configuring OSPF route summarization” on page 64](#)
- [“Viewing OSPF status” on page 65](#)

## Introducing OSPF with ABR

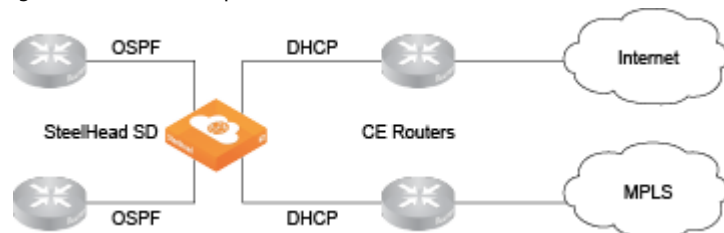
SteelHead SD provides single and multiple area OSPF with ABR and route redistribution between OSPF zone interfaces and ABRs on the LAN side of the network. You can configure OSPF regardless of whether it is a zone or an uplink.

SteelHead SD supports OSPF for a branch site with one or two MPLS providers, where each provider is connected to a customer edge (CE) router. A SteelConnect branch gateway is deployed in front of the CE routers. The provider edge (PE) routers on the MPLS WAN side are using BGP and the CE routers on the LAN side are using OSPF.

Figure 7-8. OSPF single area



Figure 7-9. OSPF multiple area




---

**Important:** Before you begin configuring OSPF for SteelHead SD, we recommend you consult the *SteelConnect Manager User Guide*.

---

## Creating an OSPF network

You create OSPF networks at the site level. Before configuring OSPF, make sure the appliance is registered in SCM and that OSPF is enabled on any routing device that will peer with the appliance. You create an OSPF network based on a site location that includes one area and then you attach one or more interfaces to the OSPF area.

### To create an OSPF network

1. Deploy the SteelHead SD and assign a zone and uplink to a port.



2. Choose Routing > OSPF.
3. Click **Add OSPF Network**.
4. Select the site for the new OSPF network.

After you select a site for an OSPF network, the system automatically populates all the remaining fields based on the default settings. You can simply click **Submit** to create a network using the default settings. You do not have to explicitly configure the settings.

Figure 7-10. Creating an OSPF network on the branch SteelHead SD

**+ Add OSPF Network** ✕

Site ?

Name

Default Area Name ?

Default Area ID ?

Inherit Org Defaults ? ☒ On ☐ Off

Password ?  👁

Hello Interval ?

Dead Interval

Priority

Cost

5. Manually fill out the network attributes that you do not want to inherit:
  - **Site** - Select the site where the OSPF network is located. Optionally, leave the site selection blank to select the first site in the list shown on the Network Designs > Sites page. Use this method to save time by quickly creating OSPF networks based on the order in which the sites appear in the site list. Creating another network and leaving the site selection blank again selects the second site in the list, and so on.
  - **Name** - Specify a network name.
  - **Default Area Name** - Specify a name for the area.
  - **Default Area ID** - Specify the area in which the zone resides. This ID will typically be one of the already existing areas in the branch. If not, either specify a 32-bit unsigned number from 0 to 4294967295 or an IPv4 address in dotted decimal notation (x.x.x.x). The default setting is the backbone area ID 0; however, you can change the value to your existing area ID. For small LANs, area 0 might be all you need, but as a network grows, you will need more than one area connecting to area 0.

For a routing device to become an OSPF neighbor with another device, both devices must belong to the same area ID and their passwords and authentication methods must match.

- **Inherit Org Defaults** - Click **On** to allow the OSPF network and area to automatically inherit the settings when an organization's default network settings are updated. This OSPF network's settings will change to match the new values.

Click **Off** to define unique settings for the network and to lock the network configuration so any changes do not overwrite the settings.

- **Password** - Specify a password. The authentication methods appear when typing a password. All OSPFv2 exchanges between routing devices can be authenticated using one of these methods:
  - **MD5** - Select this tab to use the Message Digest 5 algorithm as the authentication method. MD5 authentication enables routing devices to securely identify one another before they establish adjacency. MD5 is a cryptographic hash function with a 128-bit hash value derived from the contents of the OSPF packet and a key and key ID. This method doesn't send the password but instead calculates and includes an encoded MD5 checksum in the transmitted packet. The receiving routing device uses the key and key ID to verify the packet.

The MD5 key doesn't have to be the same within the area, but it must be exactly the same between two OSPF neighbors.

---

**Tip:** Click the eye icon to see the password as you type. The view persists until you click the eye icon again to hide the password.

---

- **Simple** - Select this tab to include an unencrypted plain text password with the packet. The receiving routing device uses the password to verify the packet. The simple password can be from one to eight characters and can include ASCII strings. If you include spaces, enclose the password in quotation marks. Use this authentication method when devices within an area do not support the more secure MD5 authentication, as Simple is the least secure setting.
- **MD5 Key ID** - (Appears when you select MD5.) Specify a value to associate with the MD5 key. The ID is used by the receiver of the OSPF packet to determine which key to use for authentication.

To change your MD5 key, specify a new key and key ID. When both OSPF neighbors have a new key and key ID, the old key is deleted and the current MD5 key and key ID become active.

- **Hello Interval** - Specify how often, in seconds, to send a hello packet. Initially the gateway sends a hello packet to all OSPF-enabled interfaces to form an adjacency as a neighbor. The routing devices become neighbors and exchange link-state advertisements. After the gateway learns the common network topology, it sends the hello to check if an OSPF neighbor is alive. The range is from 1 to 65535. The default is 10. The hello interval must be exactly the same between two OSPF neighbors.
- **Dead Interval** - Specify how many seconds to wait for a hello packet before declaring an OSPF neighbor out of service, triggering a refresh of the link-state database and routing information. The range is from 1 to 65535. The default is 40. The dead interval must be exactly the same between two OSPF neighbors.
- **Priority** - Specify the priority for becoming the network's designated routing device. The designated router originates network link advertisements on behalf of the network, and it establishes adjacencies with all routing devices on the network.

The routing device that has the highest priority value on the logical IP network or subnet is elected as the designated router. A priority value of 0 means that the routing device never becomes the designated router; it doesn't even participate in the election process. A value of 1 means that the routing device participates in the election process but has the least chance of becoming a designated router. A priority of 255 means the routing device is always the designated router.

To ensure that a routing device is elected as the designated routing device, configure the priority value to a higher value than any other interface on the Ethernet network. The range is from 0 to 255. The default value is 1.

- **Cost** - Specify a routing metric used in the link-state calculation. OSPF selects ideal routes by locating destination routes with the least cost. Routes with lower total path metrics are preferred to those with higher path metrics. This setting controls the cost calculation of OSPF network segments. The default formula to calculate the cost for the OSPF metric is dividing the reference bandwidth (100 Mbps by default) by the interface bandwidth. For example, in the case of Ethernet, it is  $100 \text{ Mbps} / 10 \text{ Mbps} = 10$ .

You can manipulate the cost by specifying a number within the range of 1 to 65535. 10 is the default setting.

The OSPF network needs a zone and, optionally, one or more uplinks to report OSPF learned routes to SCM.

---

**Tip:** If you modify the Default Area settings, keep in mind the impact the changes will have on new and existing OSPF networks. Changes to the Default Area Name, Default Area ID, and Inherit Org Defaults impact only new OSPF networks. Changes to the Password, Hello Interval, Dead Interval, Priority, and Cost impact new OSPF networks as well as existing OSPF networks with Inherit Org Defaults enabled. For details on editing OSPF networks, see the *SteelConnect Manager User Guide*.

---

6. Click **Submit**. The OSPF network appears with the available interfaces listed.

Figure 7-11. Created OSPF network



## Configuring OSPF interfaces

After you define your OSPF network, you must attach interfaces on which you want to run OSPF.

### To configure OSPF interfaces

1. Choose Routing and select the OSPF network for which you want to attach an interface.
2. Select the OSPF Interfaces tab.

### 3. Click **Attach Interface**.

Figure 7-12. Attaching an OSPF interface

### 4. Fill out these interface attributes:

- **OSPF Area** - Select the OSPF area associated with the interface from the drop-down list.
- **Inherit Area Values** - Click **On** to allow the interface to automatically inherit the area settings. When enabled and this interface area is updated, this interface settings will change to match the containing OSPF area.

Click **Off** to define unique settings for the area. This option locks the interface configuration so any changes to the area do not overwrite the interface parameters. For details on these unique settings, see [Step 5 on page 57](#).

### 5. Click **Submit**.

After you attach the interface to the OSPF area, the gateway configures the zone or zones to run OSPF and establishes OSPF neighbors with LAN routers in the same network segment.

## Creating OSPF areas

All of the networks learned from an OSPF zone interfaces are mapped to the OSPF area that the interface is connected to. For details on dynamic routing with OSPF, we recommend you consult the *SteelConnect Manager User Guide*.

A large OSPF domain is broken into separate areas to restrict the multiplication of routes and reduce the resources required by each router to maintain its link state database. Each area is connected to a central backbone, typically called area 0. OSPF uses different types of Link State Advertisements (LSAs) to communicate link state information between neighbors.

SteelHead SD supports these LSA types:

- **Standard** - Routers in this area accept default and autonomous system boundary router (ASBR) injected external routes. The backbone is considered a standard area.
- **Stub** - Routers in this area accept inter-area routes and the default route from their ABR. They do not accept ASBR injected external routes. A stub type can contain type 1, 2, and 3 LSAs.

- **Totally Stub** - This type of router is similar to a stub router. They accept inter-area routes and the default route from their ABR. They do not accept ASBR injected external routes. A totally stub type can only contain type 1 and 2 LSAs, and a single type 3 LSA. The type 3 LSA describes a default route, substituted for all external and inter-area routes.

### To create an OSPF area

1. Choose Routing > OSPF and select the OSPF network for which you want to create an area.
2. Select the Areas tab and click **New Area**.

Figure 7-13. Creating OSPF areas

The screenshot shows the 'New Area' configuration window. The 'Name' field is set to 'Branch10-area-1', 'Area ID' is '1', and 'Type' is 'Standard'. The 'Inherit OSPF Network Values' checkbox is checked, with 'On' and 'Off' buttons. Below this are sections for 'OSPF Zones' and 'OSPF Uplinks', both with a placeholder 'Please select zone interfaces for this area' and 'Please select WAN uplinks for this area' respectively. There are also sections for 'Inbound prefix' and 'Outbound prefix', both with a placeholder 'Nothing selected'. At the bottom, there are two large text areas for 'Area ranges advertised' and 'Area ranges not advertised'. The 'Submit' button is orange and the 'Cancel' button is white.

3. Fill out the attributes for the OSPF area:
  - **Name** - Specify a descriptive name for the OSPF area.
  - **Area ID** - Specify a valid area ID as either a 32-bit unsigned number from 0 to 4294967295 or an IPv4 address in dotted decimal notation (x.x.x.x). The default setting is the backbone area ID 0; however, you can change the value to your existing area ID. For small LANs, area 0 might be all you need, but as a network grows, you will need more than one area connecting to area 0.
  - **Type** - Specify the OSPF LSA type:
    - **Standard** - Routers in this area accept default and autonomous system boundary router (ASBR) injected external routes. The backbone is considered a standard area.
    - **Stub** - Routers in this area accept inter-area routes and the default route from their ABR. They do not accept ASBR injected external routes. A stub type can contain type 1, 2, and 3 LSAs.
    - **Totally Stub** - This type of router is similar to a stub router. They accept inter-area routes and the default route from their ABR. They do not accept ASBR injected external routes. A totally stub type can only contain type 1 and 2 LSAs, and a single type 3 LSA. The type 3 LSA describes a default route, substituted for all external and inter-area routes.

- **Inherit OSPF Network Values** - Click **On** to allow the OSPF network to inherit the OSPF network values previously configured, such as password, hello interval, dead interval, priority, and cost.  
Click **Off** to define unique settings for the network and to lock the network configuration so any changes do not overwrite the settings. This OSPF network's settings will change to match the new values.
- **OSPF Zone** - Select the zone from the list. These are the zones that are participating in OSPF for the area that is configured on this page. Only one zone interface per area is allowed.
- **OSPF Uplinks** - Select the uplinks from the list. These are the uplinks that will be participating in OSPF in the area that is configured on this page.
- **Inbound prefix** - Optionally, specify the inbound prefix. Any prefixes defined in this prefix list are used to filter networks sent to this area.
- **Outbound prefix** - Optionally, specify the outbound prefix. Any prefixes defined in this prefix list are used to filter networks advertised from this area.
- **Area ranges advertised** - Specify a set of advertised routes to be advertised. In order to aggregate routing information at area boundaries, area address ranges can be employed. Each address range is specified by an [address, mask] pair.
- **Area ranges not advertised** - Specify the set routes that will not be advertised. In order to aggregate routing information at area boundaries, area address ranges can be employed. Each address range is specified by an [address, mask] pair. In this case, Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.
- Click **Submit**.

## Configuring redistribution settings for OSPF

The LAN/WAN routing interworking solution bridges eBGP and OSPF to redistribute underlay routing information between the protocols on a gateway.

In 2.12, you can differentiate between static and overlay routes. Previously there was no differentiation between overlay and static routes. To avoid this ambiguity, you can configure the Overlay to OSPF option to distinguish overlay routes from static routes. The policies applied on redistribution of other routes are also applicable on overlay routes.

For details on how redistribution works, see the *SteelConnect Manager User Guide*.

### To redistribute OSPF settings

1. Choose Routing and select the OSPF network.

2. Select the Redistribute Settings tab.

Figure 7-14. Redistributing OSPF settings

The screenshot shows the 'catfish-2-lan-ospf' configuration window with the 'Redistribute Settings' tab selected. The window contains the following fields and controls:

- Default Metric:** A text input field with the placeholder '(Optional) (1-16777214)'.
- Default Route Origination:** A toggle switch with 'On' (green) and 'Off' (red) buttons.
- Always:** A toggle switch with 'On' (green) and 'Off' (red) buttons.
- Metric:** A text input field with the placeholder '(Optional) (0-16777214)'.
- Metric Type:** A dropdown menu currently set to 'None'.
- Route map:** A dropdown menu currently set to '(Optional) Nothing selected'.
- Redistribute settings section:**
  - BGP to OSPF:** Toggle switch with 'On' (green) and 'Off' (red) buttons.
  - Static to OSPF:** Toggle switch with 'On' (green) and 'Off' (red) buttons.
  - Overlay to OSPF:** Toggle switch with 'On' (green) and 'Off' (red) buttons.
  - Connected to OSPF:** Toggle switch with 'On' (green) and 'Off' (red) buttons.
- Buttons:** 'Cancel' and 'Submit' buttons are located at the bottom right of the main settings area and below the 'Redistribute settings' section.

3. Optionally, specify the default metric with a range of 1 to 16777214. The ABR generates a default route with a specified metric into the stub area. The default route matches any destination that is not explicitly reachable from within the area. Routing protocols use default metrics to calculate the best path to a specified destination. The routes that are redistributed carry the specific value.
4. To specify whether you want the default route (0.0.0.0/0) injected in OSPF:
  - **Default Route Origination** - Click **On** to enable default route origination. Enabling this option injects a default route into the participating areas in OSPF.
  - **Always** - Click **On** to advertise the default route (0.0.0.0/0) regardless of the default route entry in the routing table.
  - **Metric** - Optionally, specify the metric with a range of 1 to 16777214. Routing protocols use metrics to calculate the best route. When a metric value in a route matches this value, the route qualifies for distribution by the router.
  - **Metric type** - The type of external route that you want the routes to be injected as. When the type matches the value specified, then that route is qualified to be distributed:
    - **Type 1 (E1)** - This type includes the external cost to the destination as well as the cost (metric) to reach the AS boundary router.
    - **Type 2 (E2)** - This type uses only the external cost to the destination and ignores the cost (metric) to reach the AS boundary router.
  - **Tag** - Optionally, enter a value 32 bit value from 0 to 4294967295 that will be attached to the routes. When a tag in route matches this value, the route qualifies for distribution by the router.

- **Route map** - Click the search selector and select the route map. This option applies a routing policy based on which routes will be redistributed into OSPF.
5. Under Redistribute settings, specify your OSPF redistribution settings:
    - **BGP to OSPF** - Click **On** to redistribute the routes learned from BGP into the OSPF protocol.
    - **Static to OSPF** - Click **On** to redistribute static routes to OSPF.
    - **Overlay to OSPF** - Click **On** to redistribute overlay routes to OSPF. Optionally, the overlay routes are redistributed based on the sites from which they were reported. If no site is chosen, the prefixes from all the sites are redistributed. Sites can be added or removed.
    - **Connected to OSPF** - Click **On** to redistribute connected routes into OSPF.
  6. Optionally, specify these settings if any of the above OSPF redistribution settings is enabled:
    - **Metric** - Optionally, enter the cost metric that you want the route to be injected with into OSPF. The range is 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.
    - **Metric type** - The type of external route that you want the routes to be injected as. When the type matches the value specified, then that route is qualified to be distributed:
      - **Type 1 (E1)** - This type includes the external cost to the destination as well as the cost (metric) to reach the AS boundary router.
      - **Type 2 (E2)** - This type uses only the external cost to the destination and ignores the cost (metric) to reach the AS boundary router.
    - **Tag** - Optionally, enter a value 32 bit value from 0 to 4294967295 that will be attached to the routes. When a tag in route matches this value, the route qualifies for distribution by the router.
    - **Route map** - Click the search selector and select the route map. This option applies a routing policy based on which routes will be redistributed into OSPF.
    - **Sites** - For Overlay to OSPF routes only. Optionally, specify the site to which this redistribution policy applies. The overlay routes are redistributed based on the sites from which they were reported. Only the prefixes from configured sites will be redistributed. When no site is configured, prefixes reported from all the sites will be redistributed into the intended protocol.
  7. Click **Submit**.

## Configuring OSPF route summarization

For an OSPF area, you can filter intra-area prefixes. All routes that match the specified area range are filtered.

### To add summarization for OSPF

1. Choose Routing > OSPF.
2. Select the OSPF network.
3. Select the OSPF Summarization tab.
4. Click **Add Prefix** to add prefixes.



You can configure one or more summary addresses matching the individual addresses to advertise to a OSPF peer. You can also advertise individual addresses. By default, only summary addresses are advertised.

Figure 7-15. Summarizing routes for OSPF

5. Click **Automatic** to have SCM calculate the prefixes automatically, or click **Manual** to specify the summarized prefix.

For automatic prefix calculation, specify a starting and an ending IP address. The system provides the summarized prefix. For example, entering the starting address 160.0.1.0 and the ending address 160.0.2.0 results in the automatic prefix 160.0.0.0/22.

6. Fill out the these attributes for automatic or manual:
  - **Summarized Prefix** - Specify the IP prefix designated for the range of addresses, including the prefix length.
  - **Advertise** - Click **On** to advertise the summary prefix. Click **Off** to stop advertisements of the summary address.
  - **Tag** - Specify a 32-bit value attached to the summary route. The specified value will be tagged to the advertised summary routes.
7. Click **Submit**.

## Viewing OSPF status

There are multiple places where SCM provides visibility to OSPF and the state of routes.

### To view OSPF routing tables

1. Choose Health Check > Routing Tables.
2. Select the OSPF tab and select the appliance to display the OSPF neighbors and learned routes.

### To view the Forward Information Base (FIB) routing table

1. Choose Health Check > Routing Tables.
2. Select the FIB tab and select the appliance to display the FIB information, including destination, next hop, metric value, route type, and subroute type. This table is very useful and should be the first step in debugging if the expected routes are learned by the appliance.

## Defining static routes on SteelHead SD appliances

SteelHead SD provides static routing at the appliance level where it essentially acts as a router. The static route is not tied to a particular zone. Static routes:

- support IPv4 destination networks.
- support the distance metric setting that prioritizes the routing protocol when two routes have the same route destination.

### To define static routes

1. Choose Routing > Static Routes.
2. Click **Add Static Route**.

Figure 7-16. Adding a static route

The screenshot shows a web-based dialog titled "Add Static Route". It contains the following fields and controls:

- Appliance:** A dropdown menu showing "Champaign" and "SDI-VGW".
- Destination network:** A text input field containing "10.1.1.0/24".
- Gateway:** A text input field containing "1.1.1.1".
- Distance metric:** A text input field containing "2".
- Notes:** A large text area for additional information.
- Buttons:** "Cancel" and "Submit" buttons at the bottom right.

3. Select the appliance to which you want to add the static route.
4. Specify the IPv4 destination mask address.
5. Specify the IPv4 address for the gateway.
6. Specify the distance metric to prioritize the routing protocol where two routes provide the same route destination. The preferred route has the least distance metric. The default value is 2, giving the static route precedence over routes discovered by dynamic routing protocols but not over directly connected routes. The range is from 2 to 253.

This table shows the default values per route source.

Route source	Default distance
Connected interface	0
Static route	1
EIGRP summary route	5
BGP external (eBGP)	20
EIGRP internal	90

Route source	Default distance
OSPF	110
IS-IS	115
RIP	120
EIGRP external	170
BGP internal (iBGP)	200
Unknown	255

7. Optionally, include any notes that will help identify this static route.

8. Click **Submit**.

SCM sends the static route configuration to the gateway. The static route appears in the Static Routes page and adds the event to the Event Log.

**Note:** If a static route is configured on a gateway that is a partner in a high availability pair, SCM sends the static route information to the partner as well as sending the configuration to the gateway.

## Route retraction for SteelHead SD

SteelHead SD advertises available routes and doesn't advertise unavailable routes. If a route becomes unavailable, route retraction withdraws this route and ensures it is no longer advertised.

**Note:** The behavior of route attraction and retraction is the same across all SteelConnect appliances.

To benefit from route retraction on a SteelHead SD, you need to meet the following requirements:

- You need to redistribute the overlay network into the internet gateway protocol on the LAN.
- For SteelHead SD appliances deployed in HA mode, you need to redistribute the overlay network and connected routes into iBGP.

**Note:** In SteelConnect 2.12, you might not want to redistribute overlay networks into iBGP because both HA appliances will be aware of overlay routes, but you should still redistribute connected routes.

### To redistribute the overlay into the internet gateway protocol on the LAN

1. In SCM, choose Routing > OSPF.
2. Select your OSPF network to edit the settings.
3. In the Redistribute settings tab, click **On** for Overlay to OSPF, and click **On** for Connected to OSPF.
4. Click **Submit**.

### To redistribute the overlay and connected routes into iBGP

1. In SCM, choose Appliances > Overview.
2. Select the site.
3. Open the BGP tab and click **On** for Overlay to BGP and click **On** for Connected to BGP.

4. Click **Submit**.

# Configuring BGP and OSPF Routing Policies on SteelHead SD

This topic describes how to configure autonomous system boundary routers (ASBR) and route policies. It includes these sections:

- [“Overview of routing policies on SteelHead SD” on page 69](#)
- [“What are routing policies?” on page 70](#)
- [“Creating routing IPv4 prefix lists” on page 72](#)
- [“Creating routing community lists” on page 73](#)
- [“Creating routing AS path lists” on page 74](#)
- [“Configuring route maps” on page 76](#)

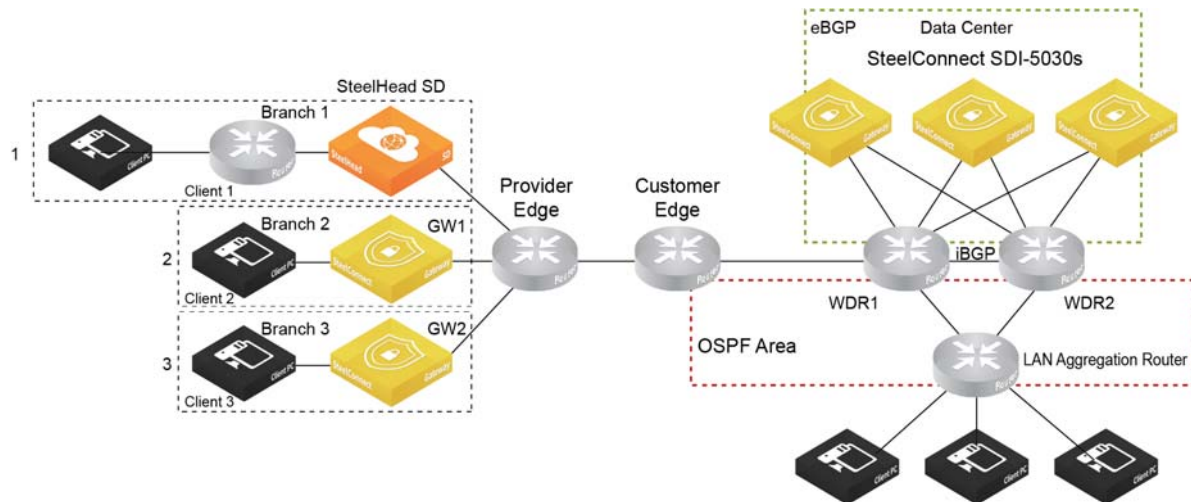
## Overview of routing policies on SteelHead SD

SteelHead SD appliances act as a full ASBR when they are located at the branch. ASBR-full routing policies are supported on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. ASBR-full support is not available on SteelConnect SDI-130/330/1030 and virtual gateways.

An ASBR is a router that is connected to several autonomous systems (ASs) using multiple protocols. Typically, ASBRs are connected via an exterior routing protocol (for example, BGP). An ASBR can also connect LAN routers through an interior gateway protocol (IGP), such as OSPF within its own AS. Basically, with an ASBR you are distributing routes from BGP to OSPF and from OSPF to BGP. An ASBR can also distribute static and connected routes into these protocols.

For example, if you have a SteelHead SD on Branch-1 with eBGP configured on the WAN uplink and OSPF configured on the LAN zones. The SteelHead SD can distribute LAN routes to the WAN and WAN routes to the LAN. This method of redistributing routes received via one routing protocol through another protocol is called *route redistribution* or *route injection*.

Figure 8-1. ASBR deployment in branch 1



SteelHead SD provides:

- **BGP redistribution** - Support includes static and connected route redistribution, OSPF route redistribution, and default route redistribution to BGP neighbors.
- **OSPF redistribution** - Support includes static and connected route redistribution, OSPF route redistribution, and default route redistribution.
- **Extended ASN capability** - Extended autonomous system number (ASN) capability is set as the default when the first AS number is configured. Normal ASN ranges from 1 to 65535, but with the extended ASN capability the range 65536 to 4294967295 is also supported.

---

**Important:** ASBR routing policies are available only on underlay branch networks.

---

## What are routing policies?

Routing policies are rules that are applied when routes are distributed between the routers. Creating routing policies enables you to redistribute BGP, OSPF, static, and connected routes.

**Note:** ASBR routing policies are not policy-based routing where routing decisions are made while directing the traffic.

Creating routing policies enables you to apply certain rules and route attributes while redistributing BGP, OSPF, static and connected routes. You can create route-maps for the following purposes:

- Route injection in OSPF.
- Default route origination in OSPF.

- Static and connected route injection BGP.
- OSPF route injection in BGP.
- Policies at the BGP neighbor level.
- Default route origination in BGP for a neighbor.

Each route map clause has two types of values:

- A match value selects routes to which the clause should be applied.
- A set value modifies information that will be redistributed into the target protocol.

For each route that is being redistributed, the router evaluates the match criteria of a clause in the route map. If the match criteria succeed, then the route is redistributed and some of the attributes may be modified by the set clause. If the route doesn't match any clause in a route map, then the route redistribution is denied.

Once configured, the route-maps can be applied to satisfy the needs of these use-cases:

- **Route Injection in OSPF** - OSPF redistributes static, connected, and BGP routes. This route-map category contains only a match criteria. The route map depends on the following objects:
  - IP prefix lists
  - Interface (all zones/uplinks associated with SteelHead SD appliances in the given organization)
- **Default Route Origination in OSPF** - Redistributes the default route in OSPF. This category of route-map contains both match and set criteria. This is the simplest route-map category that is not dependent on other objects.
- **Static and Connected Route Injection in BGP** - Redistributes static and connected routes in BGP using a list of IPv4 prefixes. This route-map category contains both match and set criteria. Also dependent on the following objects:
  - IPv4 prefix lists
  - Interface
- **OSPF Route Injection in BGP** - Redistributes OSPF routes in BGP using a list of IPv4 prefixes. This category of route map contains both match and set criteria.
- **Policies at the BGP Neighbor Level** - Redistributes routes for BGP neighbors using a community list and list of IP next-hop prefixes. You can set the origin-type attribute in this use case to influence path selection based on the origin of a prefix. This route-map category contains both match and set criteria. The match criteria in this use case is dependent on:
  - Community list
  - Prefix list
- **Default Route Origination in BGP for a Neighbor** -Redistributes the route in BGP. This route-map category contains both match and set criteria. There are not any dependent objects for this type of route map.
- **User Defined Route Map** - Enables you to create route map that includes all the match and set criteria available.

## Basic steps

Perform these basic steps to configure routing policies.

1. If you have a SteelConnect SDI-2030 gateway, configure a dynamic routing policy. For details, see the *SteelConnect Manager User Guide*.

**Note:** You can't create dynamic routing policies for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances located at the branch.

2. Configure IPv4 prefix lists. For details, see ["Creating routing IPv4 prefix lists" on page 72](#).
3. Configure community lists. For details, see ["Creating routing community lists" on page 73](#).
4. Configure AS prefix lists. For details, see ["Creating routing AS path lists" on page 74](#).
5. Configure route maps by specifying the available use cases. For example, create a route map for a routing policy to establish BGP neighbors. For details, see ["Configuring BGP route redistribution" on page 47](#).
6. Configure inbound and outbound route maps and prefixes for BGP neighbors using the configured route maps. For details on configuring BGP neighbors, see ["Enabling BGP and configuring BGP neighbors on SteelHead SD" on page 42](#).
7. Configure BGP redistribution and BGP summarization settings using the configured route maps. For details, see ["Configuring BGP route redistribution" on page 47](#) and ["Configuring BGP route summarization" on page 52](#).

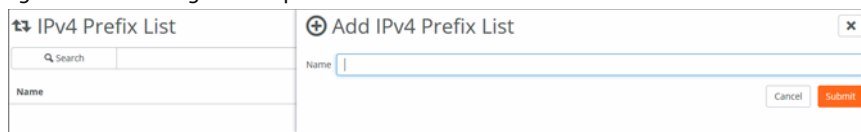
## Creating routing IPv4 prefix lists

An IPv4 prefix list contains a list of IPv4 prefixes and a name that is associated for each list. For details on how prefix lists is used in BGP routing, see ["Configuring conditional default-route originate routing" on page 48](#).

### To create a IPv4 prefix list

1. Choose Routing > IPv4 Prefix Lists.
2. Click **Add IPv4 Prefix List**.

Figure 8-2. Creating an IPv4 prefix list



The screenshot shows a web-based dialog box titled "IPv4 Prefix List" with a subtitle "Add IPv4 Prefix List". Inside the dialog, there is a "Name" label followed by a text input field. At the bottom right of the dialog, there are two buttons: "Cancel" and "Submit".

3. Specify the name of the IPV4 prefix list.
4. Click **Submit**.



- To define the prefixes for the list, select the list in the IPv4 Prefix List page.

Figure 8-3. Defining IPv4 prefixes list

The screenshot shows the 'IPv4 Prefix List' configuration interface. On the left, a table lists the prefix list 'test'. On the right, the configuration for the 'test' list is shown, including an 'Action' dropdown set to 'Allow' and an 'Add Prefix' button.

- Click **Allow** to distribute only the specified prefixes and deny the rest. Click **Deny** to stop distribution of the prefixes specified and allow the rest.

- Click **Add Prefix**.

Figure 8-4. Adding a prefix

The screenshot shows the 'Add Prefix' dialog box. It has a text input field for the 'IPv4 Prefix' and 'Cancel' and 'Submit' buttons.

- Enter the IP prefix designated for the range of addresses to distribute. Use the format: xxx.xxx.xxx.xxx/xx

- Click **Submit**.

---

**Tip:** Click **Actions** to delete a list.

---

## Creating routing community lists

A BGP community is a group of routes to which a BGP router applies the same policies. You specify the name of the community list and a string that contains values only from a predefined set of keywords and numbers. For details on how community lists is used in BGP path selection, see ["Configuring BGP path selection" on page 45](#).

### To create a community list

- Choose Routing > Community Lists.
- Click **Add Community List**.

Figure 8-5. Creating a community list

The screenshot shows the 'Add Community List' dialog box. It has a 'Name' field and a 'Community' dropdown menu with options like 'internet', 'local-AS', 'no-export', and 'no-advertise'.

- Enter a descriptive name for the community list.

4. Click the search selector for community list options. In addition to the keywords below, you can also configure numbers in the range from 1 to 65535 and numbers in AA:NN format where the range for AA and NN is 1 to 65535.
  - **internet** - Advertises this route to the internet community; by default, all prefixes are members of the internet community.
  - **local-AS** - Doesn't advertise the route to any external peers.
  - **no-export** - Instructs routers not to export a prefix to eBGP neighbors. For instance, subnets of a larger block can be advertised to influence external AS best-path selection, and those not required for this traffic engineering purpose may be tagged NO-EXPORT to prevent them from being leaked to the internet (and thus contributing to unnecessary global routing table growth).
  - **no-advertise** - Instructs a BGP router not to advertise the tagged prefix to any other neighbor, including other iBGP or eBGP routers.
5. Click **Submit**.
6. To edit a community list, select the list in the Community List page, edit the expressions, and click **Submit**.

Figure 8-6. Editing an AS path list

The screenshot shows the 'Community List' configuration interface. On the left, there's a table with one entry named 'test'. On the right, the 'Community' section has a dropdown menu open, displaying three options: 'local-AS', 'no-export', and 'no-advertise'. The 'internet' option is currently selected and shown in a separate box. At the bottom right, there are 'Cancel' and 'Submit' buttons.

---

**Tip:** Click **Actions** to delete a list.

---

## Creating routing AS path lists

You specify the name of the AS path list and define a regular expression that defines the attributes of the AS path. For details on how AS path lists are used in BGP path selection, see [“Configuring BGP path selection” on page 45](#).

---

**Important:** You must be familiar with creating regular expressions (that is, regex) to create AS path lists. If you are not familiar with regex, we recommend that you do not configure this feature.

---

The AS path list can be used while applying route policies at the BGP neighbor level.

### To create an AS path list

1. Choose Routing > AS Path List.

2. Click **Add AS Path List** to expand the page.

Figure 8-7. Creating an AS path list

The screenshot shows the 'Add AS Path List' dialog box. On the left, there is a table with a search bar and a 'Name' column. The main area of the dialog has a 'Name' input field and an 'AS path' dropdown menu. The dropdown menu is open, displaying a list of options: 'Anything', 'Learned from AS', 'Locally originated routes', 'Originated in AS', 'Any instance of AS', and 'Directly connected ASes'. To the right of the dropdown is a text area with the placeholder 'Select AS paths to create a list.' At the bottom right, there are 'Cancel' and 'Submit' buttons.

3. Enter a descriptive name for the AS path list.
4. Click the search selector for a list of AS list options. Enter one or more AS numbers from 1 to 4294967295. Separate multiple numbers with a space.
  - **Anything** - Specifies the BGP expression `".*"`, which matches anything. The `".*"` matches any single character (`"."`), and then finds zero or more instances of that single character (`"*"`).
  - **Learned from AS** - Enter one or more AS numbers from 1 to 4294967295 and click **Submit**. Separate multiple numbers with a space.
  - **Locally originated routes** - Specifies the BGP expression: `"^$"`, which matches locally originated routes. `"^$"` means that the string is null. Within the scope of BGP, the only time that the AS path is null is when you are looking at a route within your own AS that you or one of your iBGP peers has originated.
  - **Originated in AS** - Enter one or more AS numbers from 1 to 4294967295. Separate multiple numbers with a space and click **Submit**.
  - **Any instance of AS** - Enter one or more AS numbers from 1 to 4294967295. Separate multiple numbers with a space and click **Submit**.
  - **Directly connected to AS** - Specifies the BGP expression `"^[0-9]+$"`, which matches all routes originated in any directly connected single AS. These are the routes directly originated by the peers of your AS.
5. Click **Submit**.
6. To edit an AS path list, select the list in the AS Path page, edit the expressions, and click **Submit**.

Figure 8-8. Editing an AS path list

The screenshot shows the 'AS Path List' page. On the left, there is a table with a search bar and a 'Name' column. The table contains one entry with the name 'test'. The main area of the page has a title 'test' and an 'AS path' dropdown menu. The dropdown menu is open, displaying the same list of options as in Figure 8-7. To the right of the dropdown is a text area with the placeholder 'Select AS paths to create a list.' At the bottom right, there are 'Cancel' and 'Submit' buttons.

**Tip:** Click **Actions** to delete a list.

## Configuring route maps

After you configure AS lists, community lists, and IPv4 lists, you configure route maps. A route map defines the routes from the specified routing protocol that are redistributed into the target routing process. You define each route map with match and set conditions for each use case.

For details on how route maps is used in BGP path selection, see [“Configuring BGP path selection” on page 45](#).

### To create use case route maps

1. Choose Routing > Route Maps.
2. Click **Add Route Map**.

Figure 8-9. Creating route maps

3. Specify the name of the route map.
4. Select a use case from the drop-down list:
  - **Route injection in OSPF** - Allows the creation of match clauses that can be applied during BGP, static, and connected route injection in OSPF.
  - **Default route origination in OSPF** - Allows the creation of match and set clauses that can be used during the default route origination in OSPF.
  - **Static and connected route injection in BGP** - Allows the configuration of match and set clauses that can be applied while redistributing static and connected routes in BGP.
  - **OSPF route injection in BGP** - Allows the creation of match and set clauses that can be applied while redistributing OSPF routes in BGP.
  - **Policies at a BGP neighbor level** - Allows the configuration of match and set clauses that can be applied while establishing a BGP neighbor. For details on how route map criteria are used in BGP path selection, see [“Configuring BGP path selection” on page 45](#).
  - **Default route origination in BGP for a neighbor** - Allows the configuration of match and set clauses that can be applied while advertising a default route to a BGP neighbor.
  - **User defined route map** - Allows the configuration of match and set clauses that can be applied while applying all the route use cases. For details on how route map criteria are used in BGP path selection, see [“Configuring BGP path selection” on page 45](#).
5. Click **Submit**. The route map is displayed on the Route Map page.

---

**Tip:** Click **Deny** on the Route Map page to stop distribution of the route map.

---

6. To define the match and set criteria, select the route map to expand the page. The Match Criteria and Set Criteria tabs are displayed depending on the match and set requirements for each use case.

Figure 8-10. Match Criteria and Set Criteria tabs

7. Fill out the fields for the Match Criteria and Set Criteria using this table. The criteria differ according to the use case you have chosen.

Use case	Match criteria	Set criteria
Route injection in OSPF	<ul style="list-style-type: none"> <li><b>Interface</b>- Optionally, select the interface. When the interface matches the next-hop interface of the route, the route qualifies for redistribution by the router.</li> <li><b>IP list</b> - Optionally, select an IP list. When a routes prefix address matches a prefix in the list, then that route is qualified for distribution.</li> <li><b>Next hop list</b> - Optionally, select the next-hop prefix. When the next-hop address matches the selected address, the route qualifies for distribution by the router.</li> <li><b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li><b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> </ul>	No set criteria required.
Default route origination in OSPF	<ul style="list-style-type: none"> <li><b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li><b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> </ul>	<ul style="list-style-type: none"> <li><b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> </ul>

Use case	Match criteria	Set criteria
Static and connected route injection in BGP	<ul style="list-style-type: none"> <li>• <b>Interface</b> - Optionally, click the search selector and select the interface. When the interface matches the next-hop interface of the route, the route qualifies for redistribution by the router.</li> <li>• <b>IP list</b> - Optionally, select the IPv4 prefix list.</li> <li>• <b>Next hop list</b> - Optionally, select the next-hop prefix. When the next-hop address matches the selected address, the route qualifies for distribution by the router.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>AS path</b> - Click <b>On</b> to set the AS path for the route. Specify the AS string as space separated list from 1 to 4294967295. For details, see <a href="#">“Configuring BGP path selection” on page 45</a>.</li> <li>• <b>Tag</b> - If <b>On</b>, then the value is prepended with the AS path of the BGP route.</li> <li>• <b>IP next hop</b> - If <b>On</b>, then updates the IP next-hop address of the routes. Enter the IP address to be used as the next hop.</li> <li>• <b>Self address</b> - If <b>On</b>, under Self address, click <b>On</b> to use the self address as the next-hop address.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Community</b> - In addition to the keywords below, you can also configure numbers in the range from 1 to 65535 and numbers in AA:NN format where the range for AA and NN is 1 to 65535. For details, see <a href="#">“Configuring BGP path selection” on page 45</a>. <ul style="list-style-type: none"> <li>– internet</li> <li>– local-AS</li> <li>– no-export</li> <li>– no-advertise</li> </ul> </li> <li>• <b>Additive</b> - The specified community string is added to the route’s community string.</li> </ul>

Use case	Match criteria	Set criteria
OSPF route injection in BGP	<ul style="list-style-type: none"> <li>• <b>Interface</b> - Optionally, select the interface. When the interface matches the next-hop interface of the route, the route qualifies for redistribution by the router.</li> <li>• <b>IP list</b> - Optionally, select the IPv4 prefix list.</li> <li>• <b>Next hop list</b> - Optionally, select the next-hop prefix. When the next-hop address matches the selected address, the route qualifies for distribution by the router.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Metric type</b> - When the type matches the value specified, then that route is qualified to be distributed: <ul style="list-style-type: none"> <li>– <b>Type 1</b> - This type includes the external cost to the destination as well as the cost (metric) to reach the AS boundary router.</li> <li>– <b>Type 2</b> - This type uses only the external cost to the destination and ignores the cost (metric) to reach the AS boundary router.</li> </ul> </li> <li>• <b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>AS path</b> - Click <b>On</b> to set the AS path for the route. Specify the AS string as space separated list from 1 to 4294967295. For details, see <a href="#">“Configuring BGP path selection” on page 45</a>.</li> <li>• <b>Tag</b> - If <b>On</b>, then the value is prepended with the AS path of the BGP route.</li> <li>• <b>IP next hop</b> - If <b>On</b>, then updates the IP next-hop address of the routes. Enter the IP address to be used as the next hop.</li> <li>• <b>Self address</b> - If <b>On</b>, under Self address, click <b>On</b> to use the self address as the next-hop address.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Community</b> - In addition to the keywords below, you can also configure numbers in the range from 1 to 65535 and numbers in AA:NN format where the range for AA and NN is 1 to 65535. For details, see <a href="#">“Configuring BGP path selection” on page 45</a>. <ul style="list-style-type: none"> <li>– internet</li> <li>– local-AS</li> <li>– no-export</li> <li>– no-advertise</li> </ul> </li> <li>• <b>Additive</b> - The specified community string is added to the route’s community string.</li> </ul>

Use case	Match criteria	Set criteria
Policies at the BGP neighbor level	<ul style="list-style-type: none"> <li>• <b>Origin type</b> - The path attribute in the BGP update message that indicates the origin of the route. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. Select the origin type from the list: <ul style="list-style-type: none"> <li>– <b>igp</b> - The route is interior gateway protocol (IGP) (such as OSPF) to the AS of origination. The routes received from BGP are marked with the "i".</li> <li>– <b>egp</b> -Route is received from BGP via Exterior Gateway Protocol (EGP), as indicated by "e" in the BGP table.</li> <li>– <b>incomplete</b> - The routes that are redistributed into BGP using the redistribution command. These routes are marked with "?" in the BGP routing table.</li> </ul> </li> <li>• <b>Community</b> - Optionally, select the community list. A BGP route is permitted if it belongs to the specified community string. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>.</li> <li>• <b>Next hop list</b> - Optionally, select the next-hop prefix. When the next-hop address matches the selected address, the route qualifies for distribution by the router.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Origin type</b> - The path attribute in the BGP update message that indicates the origin of the route. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. Select the origin type from the list: <ul style="list-style-type: none"> <li>– <b>igp</b> - The route is interior gateway protocol (IGP) (such as OSPF) to the AS of origination. The routes received from BGP are marked with the "i".</li> <li>– <b>egp</b> -Route is received from BGP via Exterior Gateway Protocol (EGP), as indicated by "e" in the BGP table.</li> <li>– <b>incomplete</b> - The routes that are redistributed into BGP using the redistribution command. These routes are marked with "?" in the BGP routing table.</li> </ul> </li> <li>• <b>AS path</b> - Click <b>On</b> to set the AS path for the route. Specify the AS string as space separated list from 1 to 4294967295. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>.</li> <li>• <b>Tag</b> - If <b>On</b>, then the value is prepended with the AS path of the BGP route.</li> <li>• <b>IP next hop</b> - If <b>On</b>, then updates the IP next-hop address of the routes. Enter the IP address to be used as the next hop.</li> <li>• <b>Self address</b> - If <b>On</b>, under Self address, click <b>On</b> to use the self address as the next-hop address.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Local-preference</b> - Optionally, enter the value from 0 to 4294967295 to set the value to the received routes. The default value for the local preference is 100. If a route has no local preference specified it is treated as if it had a local preference of 100. If the iBGP speaker receives multiple routes to the same destination, then the route with the highest value is preferred. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>.</li> </ul>



Use case	Match criteria	Set criteria
Policies at the BGP neighbor level cont.		<ul style="list-style-type: none"> <li>• <b>Tag</b> - Optionally, enter value to be attached to all routes. The range is from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Community</b> - In addition to the keywords below, you can also configure numbers in the range from 1 to 65535 and numbers in AA:NN format where the range for AA and NN is 1 to 65535. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. <ul style="list-style-type: none"> <li>– internet</li> <li>– local-AS</li> <li>– no-export</li> <li>– no-advertise</li> </ul> </li> <li>• <b>Additive</b> - The specified community string is added to the route's community string.</li> </ul>
Default route origination in BGP for a neighbor	<ul style="list-style-type: none"> <li>• <b>IP list</b> - Select a route prefix that can be allowed or denied.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Tag</b> - Optionally, enter a value from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Prefix list</b> - Select the prefix list. The injected default route will be advertised only if the prefix is present in the FIB. If at least one prefix in the route-map is matched in the local routing table, a default will be originated. For details, see <a href="#">"Creating routing IPv4 prefix lists" on page 72</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>AS path</b> - Click <b>On</b> to set the AS path for the route. Specify the AS string as space separated list from 1 to 4294967295. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>.</li> <li>• <b>Tag</b> - If <b>On</b>, then the value is prepended with the AS path of the BGP route.</li> <li>• <b>IP next hop</b> - If <b>On</b>, then updates the IP next-hop address of the routes. Enter the IP address to be used as the next hop.</li> <li>• <b>Self address</b> - If <b>On</b>, under Self address, click <b>On</b> to use the self address as the next-hop address.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> </ul>

Use case	Match criteria	Set criteria
Default route origination in BGP for a neighbor cont.		<ul style="list-style-type: none"> <li>• <b>Tag</b> - Optionally, enter value to be attached to all routes. The range is from 0 to 4294967295. When a tag in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Community</b> - In addition to the keywords below, you can also configure numbers in the range from 1 to 65535 and numbers in AA:NN format where the range for AA and NN is 1 to 65535. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. <ul style="list-style-type: none"> <li>– internet</li> <li>– local-AS</li> <li>– no-export</li> <li>– no-advertise</li> </ul> </li> <li>• <b>Additive</b> - The specified community string is added to the route's community string.</li> </ul>

Use case	Match criteria	Set criteria
User defined route map	<ul style="list-style-type: none"> <li>• <b>Interface</b>- Optionally, select the interface. When the interface matches the next-hop interface of the route, the route qualifies for redistribution by the router.</li> <li>• <b>Origin type</b> - The path attribute in the BGP update message that indicates the origin of the route. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. Select the origin type from the list: <ul style="list-style-type: none"> <li>– <b>igp</b> - The route is interior gateway protocol (IGP) (such as OSPF) to the AS of origination. The routes received from BGP are marked with the "i".</li> <li>– <b>egp</b> -Route is received from BGP via Exterior Gateway Protocol (EGP), as indicated by "e" in the BGP table.</li> <li>– <b>incomplete</b> - The routes that are redistributed into BGP using the redistribution command. These routes are marked with "?" in the BGP routing table.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Origin type</b> - The path attribute in the BGP update message that indicates the origin of the route. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. Select the origin type from the list: <ul style="list-style-type: none"> <li>– <b>igp</b> - The route is interior gateway protocol (IGP) (such as OSPF) to the AS of origination. The routes received from BGP are marked with the "i".</li> <li>– <b>egp</b> -Route is received from BGP via Exterior Gateway Protocol (EGP), as indicated by "e" in the BGP table.</li> <li>– <b>incomplete</b> - The routes that are redistributed into BGP using the redistribution command. These routes are marked with "?" in the BGP routing table.</li> </ul> </li> </ul>

Use case	Match criteria	Set criteria
User defined route map cont.	<ul style="list-style-type: none"> <li>• <b>Community</b> - Optionally, select the community list. A BGP route is permitted if it belongs to the specified community string. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>.</li> <li>• <b>IP list</b> - Optionally, select an IP list. When a routes prefix address matches a prefix in the list, then that route is qualified for distribution.</li> <li>• <b>Next hop list</b> - Optionally, select the next-hop prefix. When the next-hop address matches the selected address, the route qualifies for distribution by the router.</li> <li>• <b>Metric</b> - Optionally, enter a value from 0 to 4294967295. When a metric value in a route matches this value, the route qualifies for distribution by the router.</li> <li>• <b>Metric type</b> - When the type matches the value specified, then that route is qualified to be distributed: <ul style="list-style-type: none"> <li>– <b>Type 1</b> - This type includes the external cost to the destination as well as the cost (metric) to reach the AS boundary router.</li> <li>– <b>Type 2</b> - This type uses only the external cost to the destination and ignores the cost (metric) to reach the AS boundary router.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>AS path</b> - Click <b>On</b> to set the AS path for the route. Specify the AS string as space separated list from 1 to 4294967295. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>.</li> <li>• <b>Tag</b> - If <b>On</b>, then the value is prepended with the AS path of the BGP route.</li> <li>• <b>Community</b> - In addition to the keywords below, you can also configure numbers in the range from 1 to 65535 and numbers in AA:NN format where the range for AA and NN is 1 to 65535. For details, see <a href="#">"Configuring BGP path selection" on page 45</a>. <ul style="list-style-type: none"> <li>– internet</li> <li>– local-AS</li> <li>– no-export</li> </ul> </li> <li>• no-advertise <ul style="list-style-type: none"> <li>– internet</li> <li>– local-AS</li> <li>– no-export</li> <li>– no-advertise</li> </ul> </li> <li>• <b>Additive</b> - The specified community string is added to the route's community string.</li> </ul>

8. Click **Submit**.

# Configuring LAN-Side Internet Breakout on SteelHead SD

This topic describes how to configure LAN-side internet breakout on SteelHead SD appliances. It includes these topics:

- [“Overview of LAN-side internet breakout on SteelHead SD” on page 85](#)
- [“Configuring LAN-side internet breakout” on page 86](#)
- [“Troubleshooting” on page 89](#)

These procedures describe LAN-side internet breakout for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway at the branch. For additional information, see the *SteelConnect Manager User Guide*.

## Overview of LAN-side internet breakout on SteelHead SD

With LAN-side internet breakout, you are able to forward internet-bound traffic on the LAN-side of the network and avoid backhauling internet traffic. For details on internet breakout, see the *SteelConnect Manager User Guide*.

Prior to SteelConnect 2.12, internet breakout was only supported on the WAN-side of the network. Internet breakout on the WAN-side of the network can occur in one of the following ways:

- Sending the packet to Zscaler or Cloudi-Fi over tunnels to the Zen nodes that break out from the cloud firewalls.
- Locally using a direct-to-internet uplink or any other internet-capable uplink.
- Overlay the packet to the data center (DC) remote site and it breaks out from the DC site.

You configure LAN-side internet breakout by enabling the Underlay option for internet bound traffic as a breakout preference. The Underlay option is available at the organization, site, and zone level. Alternatively, you can also configure the Underlay option as a preferred path in a traffic rule.

**Note:** Specific routes are given higher preference than the default route so if the internet-bound traffic has a specific route available on the appliance, the appliance honors that specific route irrespective of the configured internet breakout preference.

When the Underlay option is the preferred breakout option, make sure that a default route is available on the appliance so that the internet traffic is routed on the interface from where the default route (0.0.0.0/0) is learned. You can configure underlay internet breakout on any interface, not just the LAN interface.

**Note:** The default route may not be learned from the LAN-side. The traffic is applied to the interface on which the default route is learned. If a default route is learned from a WAN uplink and the internet breakout preference is underlay, the traffic would be put on that uplink. If the default route is learned from a LAN-side, the traffic is put on the LAN interface.

## Configuring LAN-side internet breakout

This section describes how to configure LAN-side internet breakout at the organization, site, and zone level. You can also configure the Underlay option under Traffic Rules.

### To configure LAN-side internet breakout at the organization level

1. Choose Organization.
2. Select the Networking Defaults tab.

Figure 9-1. Configuring internet breakout at the organization level

The screenshot shows the RVBD configuration interface. The top navigation bar includes tabs for Name / Location, Networking Defaults (selected), Transit, Social Media, Wi-Fi Manager, Numbering Pools, Maintenance, Data Retention, SNMP, Logging, System Dump, NetFlow, SSH, Legal Disclaimer, and Appliance Threshold. Below the navigation bar, there are links for Appliance Login and Global Subnet Discovery. The main section is titled "Internet breakout preference". It contains a text box with a search prompt "Type to search" and a dropdown menu showing "RouteVPN" and "Underlay". To the right of the dropdown are "Cancel" and "Submit" buttons. Below this is the "WAN usage preference" section, which includes a table with two rows: "1" with "RouteVPN" and "2" with "MPLS". At the bottom is the "Fall back to all available uplinks" section, which includes a text box and a toggle switch for "Traffic fall back" set to "On".

3. Click the search selector and select Underlay.
4. Click **Submit**.

### To configure LAN-side internet breakout at the site level

1. Choose Network Design > Sites.
2. Select the site to expand the page.

3. Select the WAN/AutoVPN tab.

Figure 9-2. Configuring intent breakout at the site level

**branch-site-1** Actions X

Info Zones xLAN DNS **WAN/AutoVPN** RADIUS Size Cloudi-Fi Zscaler Location

Local Subnet Discovery

**Internet breakout preference**

This setting overrides the organization default for the internet breakout preference. When set, it is valid for all zones in this site. Note: You can also override this setting per zone.

When sending traffic to the internet, the default behavior is to use direct internet uplinks (local breakout). You can also use RouteVPN, WANs, or underlay routing as alternative breakouts. Some of these options require that you specify the default site that will handle the breakout. Note: Underlay routing is only available as an internet breakout preference for sites with SDI-2030 gateways or SteelHead SD appliances.

Type to search Use organization default

- Internet
- RouteVPN
- Underlay**

Cancel Submit

When active, traffic exiting this site will not be NATed. Enable this setting if an upstream gateway is handling NAT or if the network uses public IP addresses.

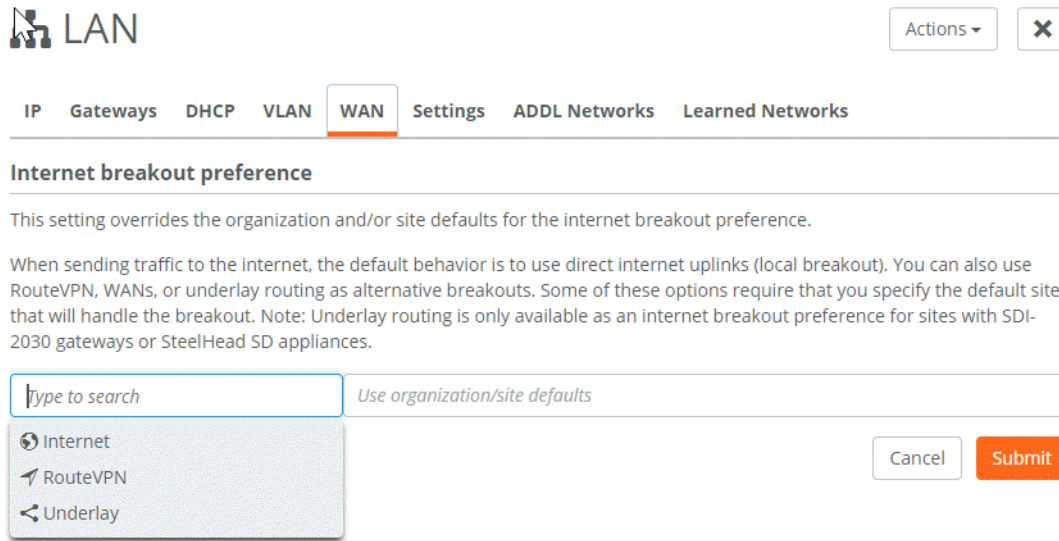
4. Click the search selector and select Underlay.
5. Click **Submit**.

#### To configure LAN-side internet breakout at the zone level

1. Choose Network Design > Zones.
2. Select the site to expand the page.

### 3. Select the WAN tab.

Figure 9-3. Configuring internet breakout at the zone level



The screenshot shows a configuration interface for a LAN. At the top, there's a header with a LAN icon and the word "LAN". To the right are "Actions" and a close button. Below this is a navigation bar with tabs: IP, Gateways, DHCP, VLAN, **WAN** (selected), Settings, ADDL Networks, and Learned Networks. The main section is titled "Internet breakout preference". Below the title is a descriptive text: "This setting overrides the organization and/or site defaults for the internet breakout preference." and a longer paragraph explaining the default behavior and alternative breakouts (RouteVPN, WANs, underlay routing). At the bottom, there's a search selector with a text input "Type to search" and a dropdown menu showing "Internet", "RouteVPN", and "Underlay". To the right of the search input is a text field "Use organization/site defaults". At the bottom right are "Cancel" and "Submit" buttons.

### 4. Click the search selector and select Underlay.

When sending traffic to the internet, the default behavior is to use direct internet uplinks (local breakout). You can also use RouteVPN, WANs, or underlay routing as alternative breakouts. Some of these options require that you specify the default site that will handle the breakout rule.

### 5. Click **Submit**.

## To configure LAN-side internet breakout in a traffic rule

1. Choose Rules > Traffic Rules.
2. Select the site to expand the page.
3. Click **New Traffic Rule**.



- Specify the traffic rule options. For details, see the *SteelConnect Manager User Guide*.

Figure 9-4. Configuring internet breakout in a traffic rule

**Create Traffic Rule**

Position: >> Top <<

Name: Traffic\_rule

Site scope: Apply rule in all sites

Users / Source: All (excluding guests)

Applications / Target: Any

Path Quality profile: None

Path preference: type to search (Nothing selected)

Rule fall through: Internet, MPLS, RouteVPN, Underlay

QoS priority:

Cancel Submit

- Click the search selector in the Path preference field and select Underlay.
- Click **Submit**.

## Troubleshooting

Enter the **show connections** CLI command to verify that the TX path is underlay. The Outgoing Interface will show the LAN interface, which means the default route was learned from the LAN interface. for example:

```
show connections
```

Enter the **tcpdump** command to run a packet trace on the LAN interface, for example:

```
tcpdump -i lan0_0 port 5005 -nn
```

For details on the SteelHead SD CLI, see the *SteelConnect Manager User Guide*.



# Configuring High Availability on SteelHead SD

This topic describes how to configure high availability (HA) on SteelHead SD 2.0. It includes these sections:

- [“Overview of HA on SteelHead SD” on page 91](#)
- [“Prerequisites” on page 94](#)
- [“Configuring a SteelHead SD HA pair” on page 94](#)
- [“Monitoring a high-availability pair” on page 101](#)
- [“Troubleshooting” on page 103](#)

**Note:** Previous versions of SteelHead SD supported an active-passive HA scheme. You can’t upgrade your SteelHead SD 1.0 (SCM 2.10) HA seamlessly to SteelHead SD 2.12 HA. You must first manually unpair your master and backup appliances in SCM, upgrade from SteelHead SD 1.0 (SCM 2.10) to SteelConnect 2.12, and reconfigure HA in SCM.

## Overview of HA on SteelHead SD

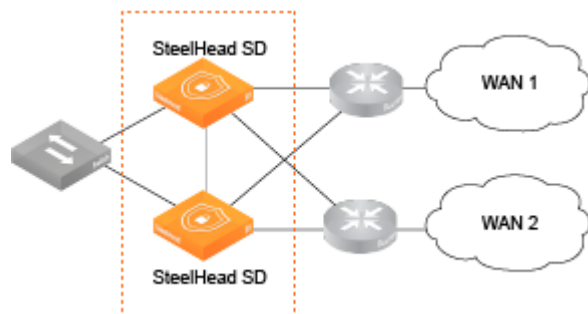
SteelHead SD provides active-active HA for 570-SD, 770-SD, and 3070-SD appliances.

**Note:** SteelConnect 2.12 provides active-active HA for SteelConnect SDI-2030 appliances located at the data center.

With active-active HA support, when a fault is detected, traffic is immediately routed to the peer appliance so that both appliances function in tandem. Traffic can be sent over any uplink regardless of the role assigned to the SteelHead SD appliance (that is, master or backup appliance). Active-active HA simplifies the configuration of uplinks for the HA pair of appliances.

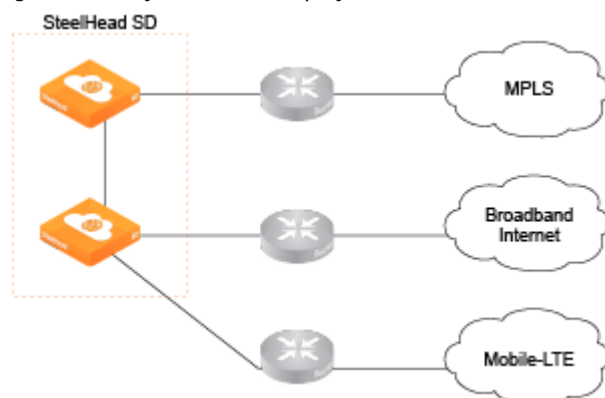
[Figure 10-1](#) shows an example of a symmetric deployment where the SteelHead SD HA pair are both connected to WAN 1 and WAN 2 via four uplinks.

Figure 10-1. Active-active HA deployment at the branch



SteelHead SD also supports asymmetric HA deployments.

Figure 10-2. Asymmetric HA deployment



SteelHead SD includes these HA features:

- Symmetric and asymmetric connectivity.
- Layer 2 (L2) and Layer 3 (L3) LAN topologies.
- OSPF and BGP where SteelHead SD can peer with a router.
- Backup standby HA link for LAN port if the AUX port is unreachable.
- Master role under Appliances > Appliances Overview: HA tab.
- Mixed-mode HA, where one SteelHead SD appliance is licensed for SD-WAN-only mode and the peer SteelHead SD appliance is licensed for SD-WAN and WAN optimization modes.
- Dedicated HA link for the SteelHead SD HA pair so that the peer appliances operate as a single logical unit.
- Autoconfiguration of the HA partner for bootstrapping when SCM connectivity with a peer is not accessible.
- Integration with SCM health check for visibility and troubleshooting.
- Zscaler support for HA deployments.

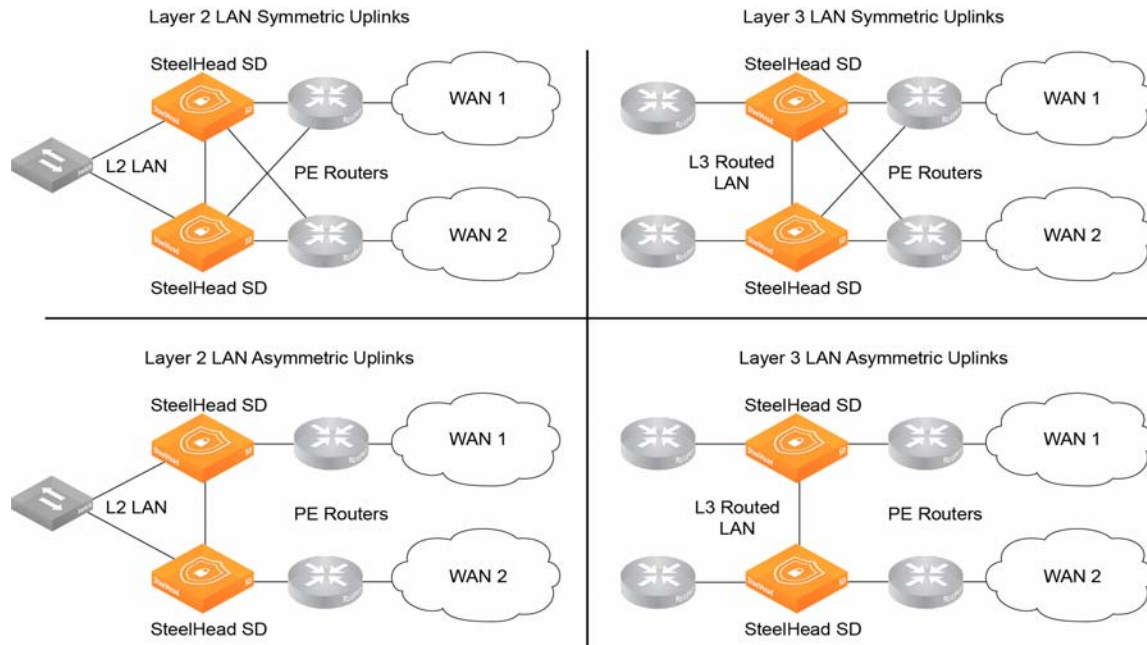
## Symmetric and asymmetric uplink connectivity

SteelHead SD provides symmetric and asymmetric uplink connectivity:

- **Symmetric** - In symmetric mode, each peer appliance is connected to all uplinks so that they essentially act as a single appliance. For example, you can have the 2 WAN uplinks connected to the peer appliances with four uplinks. Each uplink operates as a separate tunnel with separate IP addresses assigned to each uplink. If there is an uplink failure, the tunnel on that uplink goes down and the traffic is moved to the backup appliance. The 3070-SD supports up to 6 uplinks, where you can have 1 internet and 2 MPLS WAN uplinks for a total of 6 uplinks.

- **Asymmetric** - In asymmetric mode, different WANs are connected to the peer appliances. If there is an appliance failure or a LAN-side fail over, the master appliance becomes to peer appliance.

Figure 10-3. Symmetric and asymmetric HA deployment examples at the branch



## Layer 2 and Layer 3 support at the branch

With SteelHead SD 2.0, you can configure BGP and OSPF on the LAN branch.

You can configure iBGP between SteelHead SD HA peers if you want your overlay network to be advertised between the two appliances so that their routing tables are kept in synchronization. Also, you can have a combination of L2 and L3 zones so that if you have more than one LAN port configured, they can be a mix of L2 and L3. SteelHead SD uses iBGP between the peers to redistribute the overlay and connected routes.

LAN connectivity can be through either L2 switch domain or L3. In the case of a L3 LAN, connectivity is established through dynamic routing. SteelHead SD supports:

- **L3 LAN** - You can redistribute static, connected, overlay, and WAN routes on both appliances in the HA pair. Your client traffic can go to either appliance in the HA pair. Using route convergence, the master processes the traffic and sends it on the overlay network.
- **L2 LAN** - With L2, you can have a switch on the LAN-side connected to SteelHead SDs that have the same LAN zone with different IP address for each appliance. The system assigns a single virtual IP address (VIP) on the zone that is owned by the master appliance. All traffic goes to the master appliance where it sends it on the overlay network. If there is a failure, the VIP moves to the backup appliance where it becomes the new master.

Multigroup VIP and Virtual Router Redundancy Protocol (VRRP) with a third-party router are not supported at this time.

## Failure conditions

SteelHead SD supports appliance, uplink, LAN, and dedicated port failure conditions. This list describes some typical use cases:

- **Appliance failure** - For failures due to power, hardware, or VM failures, the master role is moved to the peer appliance. The VIP is moved to the new master appliance and L3 advertisements are stopped from the previous master appliance.
- **LAN failure** - For an L2 LAN failure, the VIP moves to the backup appliance and MPLS connectivity is withdrawn. Traffic is sent through the backup appliance. For an L3 LAN failure, routing converges to send traffic to the backup appliance. Traffic is moved between appliances through the AUX port depending on which uplink the traffic needs to exit the HA pair.
- **AUX port failure** - For an AUX port failure, you can configure a LAN-side HA standby link to avoid a split-brain scenarios if the AUX link goes down. The standby LAN HA link also provides connectivity via the LAN to SCM when a SteelHead SD appliance does not have an internet uplink. With a backup LAN HA link configured, when the AUX link fails, the HA traffic is switched to the LAN-side link. The AUX port is still the primary HA link, so that when the AUX link comes back up, traffic is switched back to the AUX link.

## Prerequisites

Before configuring high availability, check these requirements and recommendations:

- Both appliances must be running the same software version.
- Both appliances must be cabled directly on the LAN branch using the AUX port.
- In an L2 deployment, peer appliances must be located in the same zone of the branch network.
- In an L3 deployment, two zones must be created, one for each appliance.
- If you enable a standby LAN link for an AUX link failure, the standby HA LAN link must be part of a switched domain and a loopback IP address must be configured that is unique across all organizations.
- If you have two high-availability (HA) appliances that have the same public IP, tunnels with the two HA appliances can't be established, as they would appear identical. You must override the AutoVPN port to ensure tunnels between the two HA sites are established. For details, see ["Overview of AutoVPN on SteelHead SD" on page 33](#)

## Configuring a SteelHead SD HA pair

These tasks assume that you have installed, registered, and performed the initial configuration of the SteelHead SD HA pair. You should create your branch site where the HA pair will be located, along with the associated zone and uplinks. For details, see the *SteelConnect Manager User Guide*. This section contains these topics:

- ["Configuring the AUX port on the HA pair" on page 95](#)
- ["Configuring the LAN zone for the SteelHead SD HA pair" on page 95](#)
- ["Assigning the LAN zone to the SteelHead SD HA pair" on page 96](#)

- “Configuring the appliances in an HA pair” on page 97
- “Configuring a standby LAN HA link” on page 98

## Configuring the AUX port on the HA pair

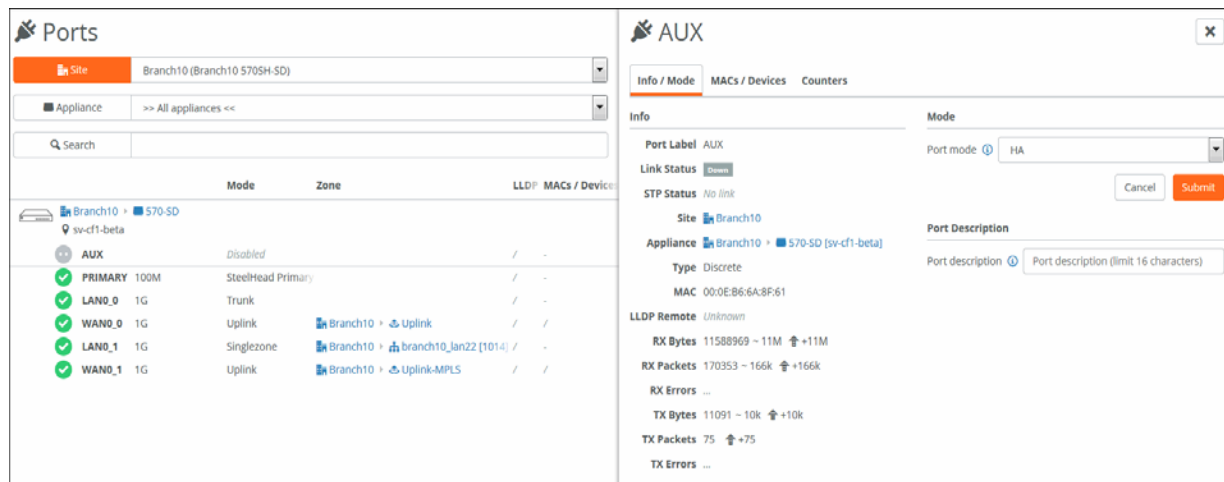
The first task is to configure the AUX port on the SteelHead SD HA pair. You will select the HA or Cluster mode for the port.

**Note:** If you have two SteelHead SD appliances in HA mode, then the AUX port must be used for the interconnection so it will not be available as an additional WAN uplink.

### To configure the AUX port on the master and backup SteelHead SD appliances

1. On the first appliance in the pair, choose Appliances > Ports and select the site from the Site drop-down list.
2. Under Appliances, select the appliance. The ports for the appliance are displayed.
3. Select the AUX port to expand the page.
4. Under Mode, select HA from the Port mode drop-down menu.

Figure 10-4. Configuring the AUX port on the HA pair



5. Click **Submit**.
6. Repeat [Step 1](#) through [Step 5](#) for the peer appliance in the HA pair.

**Note:** After you have specified HA for the port mode, SCM displays this alert: HA Port active: This port has been configured to serve as a dedicated port for HA.

## Configuring the LAN zone for the SteelHead SD HA pair

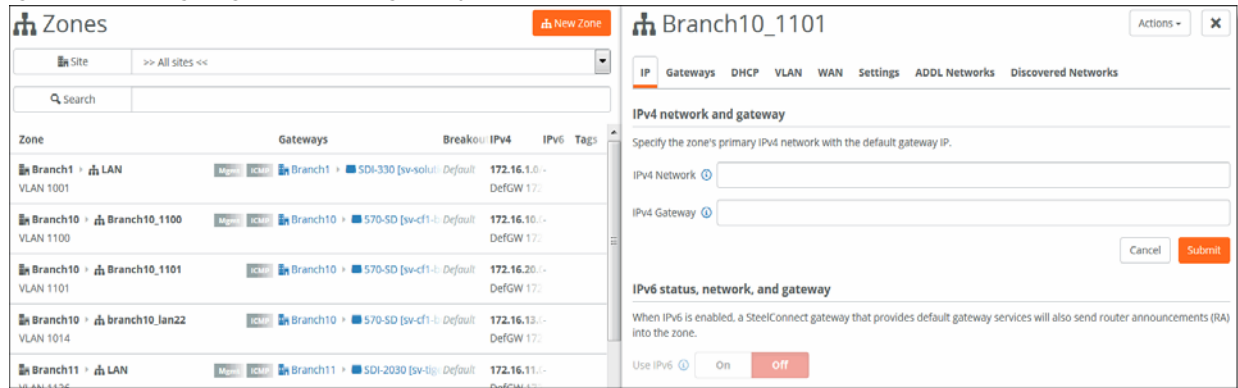
The next task is to configure the LAN zone for the SteelHead SD HA pair.

### To configure the LAN zone

1. Choose Network Design > Zones.

2. Select the Zone for the appliance to expand the page.
3. Under IPv4 Network and IPv4 Gateway, specify the gateway IP address.

Figure 10-5. Configuring the LAN zone gateway



4. Click Submit.
5. For L3 LAN topologies, repeat [Step 1](#) through [Step 4](#) to create an additional zone.

## Assigning the LAN zone to the SteelHead SD HA pair

After you configure the LAN zones, you must assign the LAN ports to the zones:

- If the LAN-side network is L2, the same zone must be attached to the LAN port on both appliances.
- If the LAN-side network is L3, a different zone must be attached to the LAN port for each of the appliances.

### To assign the LAN port to the zone

1. To assign the appliance port to the zone, choose Appliances > Ports.
2. Select the site from the Site list.
3. Select the LAN port to expand the pane.

Figure 10-6. Configuring the LAN port





- Under Port Mode, select Singlezone or Multizone. If you select Singlezone, select the zone from the drop-down list.
- Click **Submit**.
- Repeat [Step 1](#) through [Step 5](#) for each appliance port that needs to be assigned to a zone.

## Configuring the appliances in an HA pair

To configure the appliances into an HA pair

- Choose Appliances and select the appliance.
- Select the HA tab.

Figure 10-7. HA tab

The screenshot shows the configuration page for appliance [HA] 770-SD, with the HA Master tab selected. The page is divided into three main sections:

- High availability settings:**
  - High availability partner appliance: dropdown menu showing "branch-site-4 -> [HA] 770-SD [XN1342EE139F1E83]"
  - Preferred HA Master: toggle switch set to "On" (with "Off" button visible)
- Zone HA Configurations:**
  - Configure zone level HA (Required only for L2 deployments)
  - Buttons: + Configure Zone, Edit, Delete

Zone	Zone IP	IP	Partner IP
branch-site-4 -> LAN	172.16.7.1	172.16.7.10	172.16.7.11
branch-site-4 -> LAN	172.16.7.1	172.16.7.10	172.16.7.11
- Standby HA link configuration:**
  - Select the standby link for active-active HA. Available for SteelHead SD appliances and the SteelConnect SDI-2030 gateway.
  - HA standby link: dropdown menu showing "branch-site-4 -> LAN [1006]"
  - Buttons: Cancel, Submit

- Under High availability partner appliance, select the appliance that is in the branch.
- Under Preferred HA Master, click **On** if you want this appliance to be the HA master.
- Click **Submit**.

Once the two appliances are paired, you can see them negotiate their roles in the Appliances Overview page. The master and backup roles are assigned and appear for the paired appliances.

- If you have a L2 zone in your network, click **Configure Zone** to configure the LAN interface IP addresses.

Figure 10-8. Configuring the LAN interfaces for L2 zones

- Select the zone for the HA pair.
- Enter the HA IP address for the current appliance.
- Enter the HA IP address for the partner appliance.
- Click **Submit**.

## Configuring a standby LAN HA link

SteelConnect 2.12 supports one additional HA standby link. You can configure the LAN link as a backup HA link in case the AUX port is disconnected. If the AUX link goes down, you can use LAN-side connectivity to run the HA heartbeat, configure replication, and perform additional synchronization functions to avoid a *split-brain* HA condition.

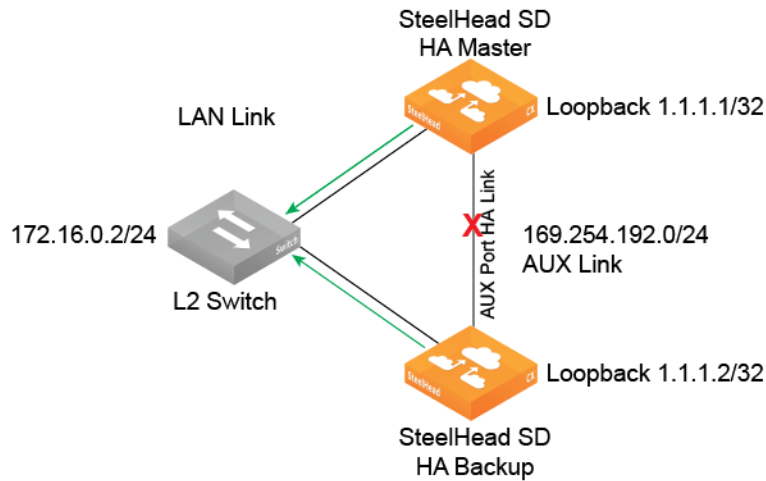
With a standby LAN HA link configured, when the AUX link fails, the HA traffic is switched to the LAN-side. The AUX port is still the primary HA link, so that when the AUX link comes back up, traffic is switched back to the AUX link. The standby LAN HA link also provides connectivity via the LAN to SCM when a SteelHead SD appliance does not have an internet uplink.

The standby HA LAN link:

- Must be part of a switched domain (that is, the master and backup HA appliances must be connected via a switch over the LAN).
- A loopback IP address must be configured on the master and backup HA appliances. The loopback IP address must be unique across the organization.

- The loopback IP address must contain the zones belonging to the current site. It must be a /32 address and should not have a physical port attached to it.

Figure 10-9. Standby LAN HA link



When the AUX link is offline, all the HA traffic is switched to the LAN link. When the master wants to use the backup appliance uplinks, Generic Routing Encapsulation (GRE) tunnels the packet via the LAN link. When the backup appliance has a packet to send to the master appliance, it uses the LAN link for GRE encapsulated packets. When the AUX link comes back up, any further HA traffic uses the AUX link.

**Note:** If a standby HA link is configured, a firmware download may fail if the AUX port or primary HA link goes down.

## Configuring the loopback IP address

Configuring a standby LAN HA link requires that you configure a loopback IP address.

### To configure a loopback IP address

1. Create a /32 zone belonging to the site. Do not attach any physical port to it. The /32 zone will appear under the Routing Loopback zone drop-down list.) For details on creating zones for sites, see the *SteelConnect Manager User Guide*.
2. Choose Appliances and select the appliance.

3. Select the Routing tab.

Figure 10-10. Configuring loopback IP

The screenshot shows the configuration window for a SteelHead SD appliance, titled "770-SD". The "Routing" tab is selected in the top navigation bar. Below the navigation bar, the "Routing" section is visible. Under "Routing", the "Router ID" is set to "200.200.1.28". The "Routing loopback IP" section is expanded, showing a "Loopback zone" dropdown menu with the text "Please select ::" and a "Loopback IP" text input field with the placeholder "Loopback interface IP Address.". At the bottom right of the form, there are "Cancel" and "Submit" buttons.

4. Select the loopback zone from the drop-down list. All the zones associated with the appliance are listed.
5. Specify the loopback IP address for the specified zone. The loopback IP address should not be same as the zone IP address.
6. Click **Submit**.

## Configuring the standby LAN HA link

After you have configured the loopback IP address, you must specify a LAN link.

### To configure the standby LAN HA link

1. Choose Appliances and select the appliance.

2. Select the HA tab.

Figure 10-11. Configuring the standby LAN HA link

The screenshot shows the configuration page for a SteelHead SD appliance, specifically the High Availability (HA) settings. The page title is "[HA] 770-SD" with a sub-label "HA Master". The navigation bar includes tabs for Live, IPs, AutoVPN, System dump, Tools, HA (selected), Routing, BGP, Services, NetFlow, and Location. The main content area is divided into three sections:

- High availability settings:** Includes a dropdown for "High availability partner appliance" set to "branch-site-4 -> [HA] 770-SD [XN1342EE139F1E83]" and a "Preferred HA Master" toggle set to "On".
- Zone HA Configurations:** A section for configuring zone level HA (required only for L2 deployments). It contains a table with two rows, each representing a zone configuration. Each row has "Edit" and "Delete" buttons, a zone name, a zone IP, an IP, and a partner IP.
- Standby HA link configuration:** A section for selecting the standby link for active-active HA. It includes a dropdown for "HA standby link" set to "branch-site-4 -> LAN [1006]" and "Cancel" and "Submit" buttons.

		Zone	Zone IP	IP	Partner IP
Edit	Delete	branch-site-4 -> LAN	172.16.7.1	172.16.7.10	172.16.7.11
Edit	Delete	branch-site-4 -> LAN	172.16.7.1	172.16.7.10	172.16.7.11

3. Under Standby HA link configuration, select the standby LAN link from the drop-down list.
4. Click **Submit**.

After you submit your request, it is cascaded to the other HA appliance.

## Monitoring a high-availability pair

SCM displays all appliances belonging to a high-availability pair with a blue HA icon in all views. After the appliance reports its HA state to SCM, the icon indicates whether it is the master or the backup.

When an HA appliance pair loses connectivity, Appliances and Health Check display both the master and backup appliance as HA Master. For SteelHead SD appliances, SCM will not display Offline for an appliance unless the appliance actually goes offline.

**Note:** Uplink tracking and LAN port tracking is not available on SteelHead SD.

SCM manages both appliances in a pair as one. For example, under Appliances > Ports, if you view the ports for an HA pair, they appear together.

Figure 10-12. HA pair ports

Appliance	Mode	Zone	LLDP	MACs / Devices
[HA] 570-SD [SV-Desk-2]	AUX 1G	HA Control Port	/	-
[HA] 570-SD [SV-Desk-2]	PRIMARY	SteelHead Primary	/	-
[HA] 570-SD [SV-Desk-2]	LAN0_0	Disabled	/	-
[HA] 570-SD [SV-Desk-2]	WAN0_0 1G	Uplink	/	/
[HA] 570-SD [SV-Desk-2]	LAN0_1	Singlezone	/	/
[HA] 570-SD [SV-Desk-2]	WAN0_1	Disabled	/	-
[HA] 570-SD [SV-Desk-1]	AUX 1G	HA Control Port	/	-
[HA] 570-SD [SV-Desk-1]	PRIMARY	SteelHead Primary	/	-
[HA] 570-SD [SV-Desk-1]	LAN0_0	Disabled	/	-
[HA] 570-SD [SV-Desk-1]	WAN0_0 1G	Uplink	/	/
[HA] 570-SD [SV-Desk-1]	LAN0_1	Disabled	/	-
[HA] 570-SD [SV-Desk-1]	WAN0_1	Disabled	/	-

To view appliance health of an HA pair

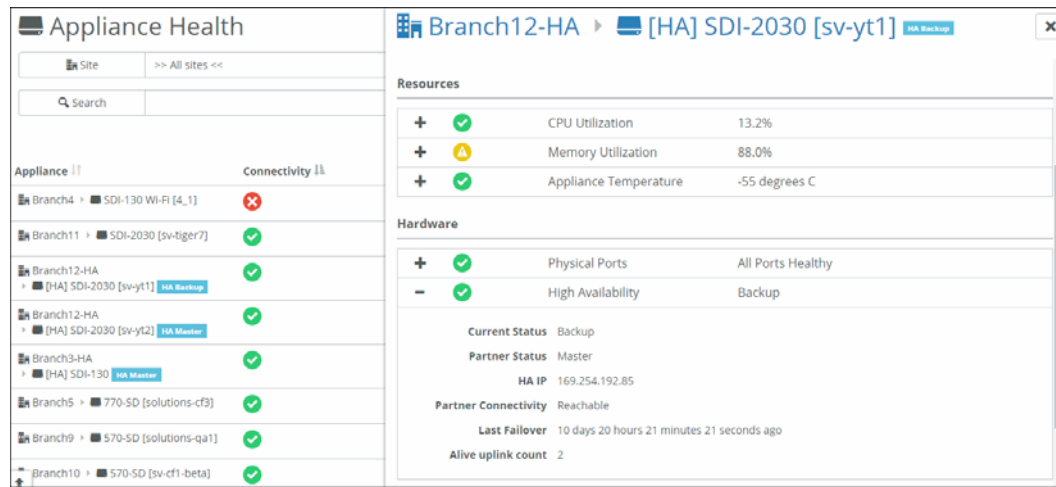
1. Choose Health Check > Appliance Health.

Figure 10-13. Appliance health in an HA pair

Appliance	Connectivity	Config	Version	Management Interfaces	Hardware	Resources
Branch1 - SDI-330 [sv-solutions-gw1]	✓	✓	✓	✓	✓	✓
Branch8 - [HA] 570-SD [SV-Desk-1] HA Master	✓	✓	✓	✓	✓	✓
Branch6 - [HA] SDI-330 [6, 1] HA Master	✓	✓	✓	✓	✓	✓
Branch8 - [HA] 570-SD [SV-Desk-2] HA Backup	✓	✓	✓	✓	✓	✓
Branch12 - [HA] SDI-2030 [sv-yt2] HA Master	✓	✓	✓	✓	✓	✓
Branch10 - 570-SD [sv-cf1-beta]	✓	✓	✓	✓	✓	✓
Branch12 - [HA] SDI-2030 [sv-yt1] HA Backup	✓	✓	✓	✓	✓	✓

2. Select the appliance to expand the page.

Figure 10-14. Viewing HA pair health details



3. Under Hardware, click the plus sign to the left of High Availability to view:
  - current status
  - partner status
  - HA IP address
  - partner connectivity status
  - time since last failover
  - alive uplink count

## Troubleshooting

- Make sure the roles are displayed correctly on the appliances in the Appliances > Overview page.
- All the tunnels must be up and should be using the uplinks for both the HA appliances.
- If the appliance HA role is *Unknown* or if the appliance pair is listed as Master/Master, make sure the AUX port (that is, the dedicated HA port) is enabled and it is configured as HA mode. If the AUX port is configured and enabled, then collect a system dump from the appliances and contact Riverbed Support at <https://support.riverbed.com>.
- The HA role is established with a daemon named **keepalived**. Search the logs for “keepalived” to debug HA issues.
- Some useful CLI commands to analyze are:

```
show keepalived_resources
show ha_info
```

For details on the SteelHead SD CLI, see the *SteelConnect Manager User Guide*.





# Configuring QoS Shaping on SteelHead SD

This topic describes how to configure QoS shaping. It includes these sections:

- [“QoS shaping on SteelHead SD” on page 105](#)
- [“If you set the QoS priority in a traffic rule” on page 106](#)
- [“Configuring QoS shaping on SteelHead SD” on page 107](#)

These procedures describe QoS shaping for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

## QoS shaping on SteelHead SD

SteelHead SD supports QoS shaping to allocate bandwidth and prioritize traffic. With SteelHead SD QoS there are no classes to configure: you simply set the bandwidth with a fixed value to provide QoS shaping on inbound and outbound traffic. QoS shaping is supported on site uplinks of a given WAN.

You configure QoS as a policy on a WAN uplink to ensure that your uplink doesn't exceed a set bandwidth. For example, if you know your uplink can't handle more than 100 Mbps, you set your limit at something lower than 100 Mbps to ensure that you have a minimal level of service for that uplink. If traffic exceeds the configured bandwidth, it is buffered and shaped. If traffic exceeds the buffer capacity, it is dropped. The QoS shaper throttles and limits traffic to your configured bandwidth.

QoS prioritizes traffic flowing on:

- **Outbound QoS** - Outbound QoS prioritizes and shapes outbound traffic on a WAN uplink. Egress traffic on a WAN uplink is provisioned with an outbound QoS policy.
- **Inbound QoS** - Inbound QoS prioritizes and shapes inbound traffic on a WAN uplink, ingress traffic on a WAN uplink is provisioned with an inbound QoS policy.

**Note:** QoS marking is currently supported on SteelConnect when you define a traffic rule to match on a specified site or application to apply an outbound DSCP mark. For additional information on QoS marking, see the *SteelConnect Manager User Guide*.

## SteelHead SD QoS shaper

SteelHead SD QoS uses a class-based queuing implementation that assigns packets with a DSCP mark to one of the four dedicated service class queues and distributes bandwidth between them using a deficit weighted round robin (DWRR) scheme. Traffic scheduling and shaping uses a basic single rate and bucket algorithm to regulate the data transmission rate and drain the queues. QoS shaping:

- classifies traffic based on the DSCP mark and shapes it according to a fixed bandwidth allocation designated for each traffic class to ensure that their aggregate bandwidth doesn't exceed the configured rate.
- is per packet; it is not flow based.
- applies only on WAN interfaces, not LAN interfaces. It is not site aware.

PQ class ID	QoS class (bandwidth)	Example of traffic type	DSCP values
Urgent (3)	Latency Sensitive - 40%	VoIP	Class Selector CS7(56), CS6(48), EF(46), VA(44), CS5(40), CS4(32)
High (2)	Streaming Media - 30%	Video	AF4x(34,36,38), AF3x(26,28,30), CS3(24), AF2x(18,20,22), TOS4(4), CS2(16), TOS1(1)
Normal (1)	Best Effort - 20%	MAPI	CS0, AF1x, TOS2, and if the DSCP value is not specified
Low (0)	Background Traffic - 10%	YouTube	CS1

**Note:** The DSCP standards for QoS have been specified and respecified many times. For the latest standards, see DSCP RFC 2474, RFC 3168, RFC 3260, and RFC 5865.

If all queues have equal size packets, and all queues are full, they are not handled equally. Urgent receives 40% of the bandwidth, High receives 30%, Normal receives 20%, and Low receives 10%. This bandwidth distribution occurs when you have different traffic classes shared on the same WAN uplink and under congestion conditions they are competing for the same bandwidth rate. If all your traffic is in the Low traffic class, then it's not competing with the other queue classes, so it receives 100% of the bandwidth.

Traffic scheduling and shaping uses a basic single rate to regulate the data transmission rate and drain the queues. Each round turn traverses only traffic class queues that are in the active bitmap and always in the order from higher to lower priority queues. The token bucket shaper then throttles the rate at which packets are transmitted by determining when a packet selected by the DWRR can be sent.

To ensure that each class-based queue doesn't overflow, when the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough room to accept incoming traffic.

To view the TOS/DSCP and QoS traffic classes table, see [Appendix B, "TOS, DSCP, QoS Traffic Class Table."](#)

## If you set the QoS priority in a traffic rule

You can also configure custom DSCP marks in the SCM when you configure the QoS priority in traffic rules (Rules > Traffic Rules > New Traffic Rule). Traffic rules allow you to mark traffic to specific DSCP value. Only DSCP marked traffic is placed in the QoS priority queues. Traffic must have a DSCP marking value for QoS traffic to be classified. For details, see the *SteelConnect Manager User Guide*.

If the QoS priority is configured in a traffic rule, then:

- inbound QoS shaping is done before the QoS mark is applied.
- outbound QoS shaping is done after the QoS mark is applied.

Setting the QoS priority in the traffic rule marks the traffic with the configured DSCP value upon egress, which executes independently of QoS shaping.

For example, if the original DSCP mark on the traffic is NORMAL priority and matches the traffic rule with the QoS priority set to URGENT, then QoS shaping will be influenced as follows:

- Inbound QoS shaping queues and processes the traffic as NORMAL priority, before the traffic rule changes the DSCP mark.
- Outbound QoS shaping queues and processes the traffic as URGENT priority, after the traffic rule changes the DSCP mark.

## Configuring QoS shaping on SteelHead SD

To configure QoS shaping

1. choose Network Design > Uplinks and select the appliance.
2. Select the QoS tab.

Figure 11-1. Configuring inbound and outbound QoS

catfish-ha-2-appliance1...

Actions X

Info Settings AutoVPN **QoS** L2 Settings

### Outbound Quality of Service (QoS)

Outbound QoS will ensure optimal use of outgoing (upstream) bandwidth on this uplink. Please specify the outgoing bandwidth capacity of your uplink in megabits. For best results, it is recommended to use a slightly lower value than what is advertised by your service provider.

Outbound Quality of Service (QoS) **On** Off

Bandwidth 100

Units Mbits/sec

Cancel Submit

### Inbound Quality of Service (QoS)

Inbound QoS will limit incoming (downstream) bandwidth on this uplink to prevent remote queue buildup. Please specify the incoming bandwidth capacity of your uplink in megabits. For best results, it is recommended to use a slightly lower value than what is advertised by your service provider.

Inbound Quality of Service (QoS) **On** Off

Bandwidth 100

Units Mbits/sec

Cancel Submit

3. Specify the percentage of bandwidth for the outbound traffic. If you set the bandwidth to 99%, it will ensure there is overhead free in case there is total saturation of the scheduler.

If your egress throughput traffic rate on the Wan1\_Uplink is 5 Mbps and you want to constrain it to not exceed 3 Mbps. Set the Outbound QoS Bandwidth to 3Mbps to ensure that the aggregate throughput upon the egress of the Wan1\_Uplink doesn't exceed your configured bandwidth.

Different traffic classes (Urgent, High, Normal, Low) sent on the same WAN uplink will share the bandwidth at a ratio of (4:3:2:1) respectively. Their combined bandwidth will not exceed the configured rate.

If you configure an inbound policy as well as an outbound policy, it is rate limited independent of the outbound policy.

4. Select the units for the bandwidth from the list.
5. Click **Submit**.
6. Specify the percentage of bandwidth for the inbound traffic. (If you set the bandwidth to 99%, it will ensure there is overhead free in case there is total saturation of the scheduler.)
7. Select the units for the bandwidth from the list.
8. Click **Submit**.
9. To check if the policy has been applied, choose Appliances > Overview. The Config column changes change from Pending to Shipped.

## Health Check and Reporting on SteelHead SD

This topic describes the health-check and reporting features. It includes these sections:

- [“Checking SteelHead SD connectivity to SCM” on page 109](#)
- [“Viewing the SteelHead SD HA status” on page 110](#)
- [“Displaying underlay ARP tables” on page 110](#)
- [“Displaying FIB tables” on page 111](#)
- [“Displaying BGP peer tables” on page 112](#)
- [“Displaying OSPF neighbors and routes” on page 112](#)
- [“Displaying NTP server status” on page 113](#)
- [“Enabling SNMP reporting and logging” on page 114](#)
- [“Exporting syslog messages to an external syslog server” on page 114](#)
- [“Exporting Netflow data” on page 115](#)

These procedures describe health-check and reporting tools for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. For details on health check and visibility in SCM, see the *SteelConnect Manager User Guide*.

For details on troubleshooting in SCM, see the *SteelConnect Manager User Guide*.

### Checking SteelHead SD connectivity to SCM

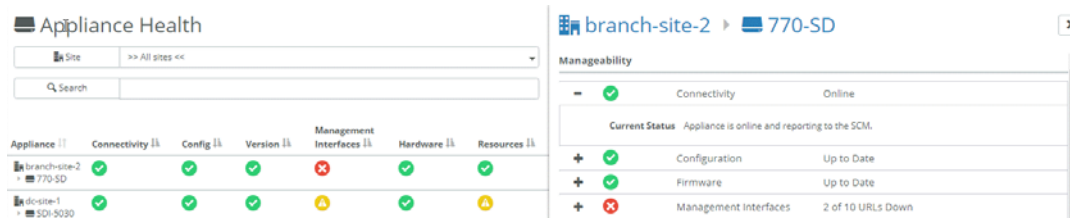
You can check SteelHead SD connectivity to SCM in the Health Check > Appliance Health page.

#### To view SteelHead SD connectivity to SCM

1. Choose Health Check > Appliance Health.
2. Select the SteelHead SD appliance to expand the page.

- Under Manageability: Connectivity, click the plus sign (+) next to the Connectivity and the Management Interfaces sections. The current status for the appliance and management interfaces is displayed.

Figure 12-1. Viewing if SteelHead SD is connected to SCM



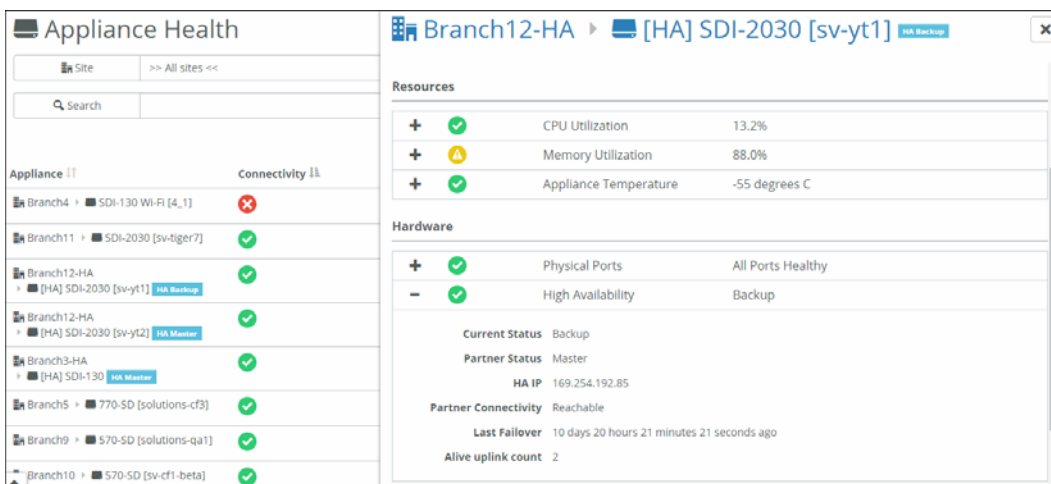
## Viewing the SteelHead SD HA status

You can view the SteelHead SD high availability (HA) status of the appliance in the Health Check > Appliance Health page.

To view the SteelHead SD HA IP address and status

- Choose Health Check > Appliance Health.
- Select the SteelHead SD appliance to expand the page.
- Under Manageability: Hardware, click the plus sign (+) next to High Availability. The current HA status for the appliance is displayed.

Figure 12-2. Viewing the SteelHead SD HA status



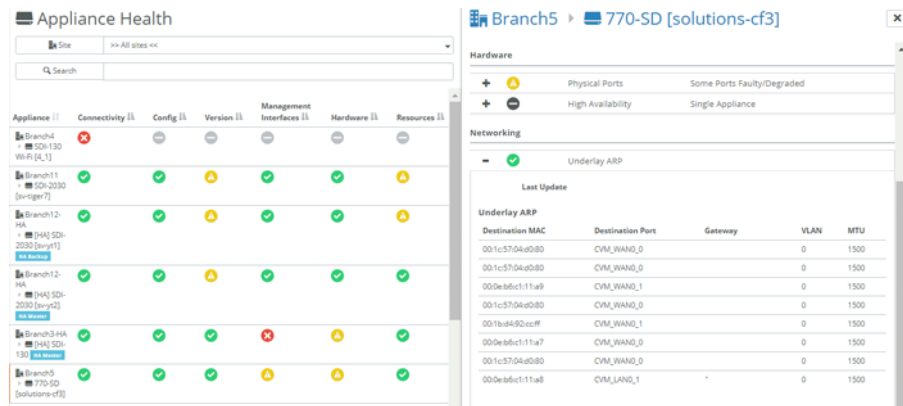
## Displaying underlay ARP tables

SCM displays the underlay Forward Information (FIB) and Address Resolution Protocol (ARP) tables for SteelHead SD 570-SD, 770-SD, 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

## To display the underlay ARP tables

1. Choose Health Check > Appliance Health.
2. Select the SteelHead SD appliance to expand the page.
3. Under Networking, click Underlay ARP to display the FIB table.

Figure 12-3. Displaying underlay ARP table



## Displaying FIB tables

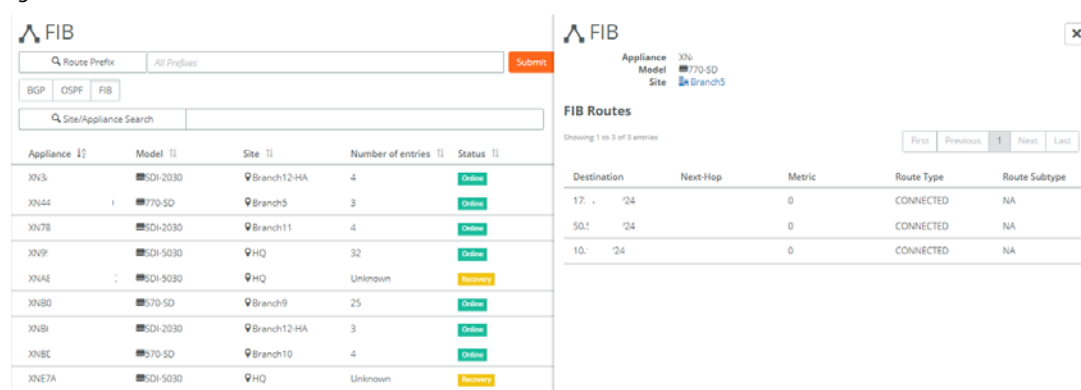
SCM displays the Forward Information (FIB) tables for SteelHead SD 570-SD, 770-SD, 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

You can search also search by site or appliance serial number.

## To display FIB tables

1. Choose Health Check > Routing Tables.
2. Select the FIB Tables tab to display the FIB tables for all the appliances in the organization. You can search for an appliance by serial number or search for appliances by site name.
3. Optionally, search for the table by specifying the site or the appliance serial number. Partial searches are supported.

Figure 12-4. FIB tables



The Route Type specifies whether the route is directly connected. It can be connected either by OSPF or BGP.

You can navigate using the page buttons.

## Displaying BGP peer tables

SCM displays the BGP peer and routing tables for SteelHead SD 570-SD, 770-SD, 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

You can search also search by site or appliance serial number.

### To display a BGP peer table

1. Choose Health Check > Routing Tables.
2. Select the BGP tab.
3. To display the BGP tables for all the appliances in the organization, select the BGP Tables tab. All the BGP learned and advertised routes are displayed. You can search for an appliance by serial number or search for appliances by site name.
4. Optionally, search for the table by specifying the site or the appliance serial number. Partial searches are supported.
5. Select the appliance to expand the page.

Figure 12-5. Viewing BGP learned and advertised routes

**BGP**

Route Prefix: All Prefixes

BGP OSPF RIB

Size/Appliance Search

Appliance	Model	Site	Local AS	Peer	Peer IP	Remote AS	Status	Peer State
XN03 9700	770-SD	branch-site-4	65510	MPLS-router	100.110.140.1	65502	Online	Established
XN1 1688	770-SD	branch-site-4	65510	MPLS-router	100.110.150.1	65502	Online	Established
XN18 EF79	SDI-5030	dc-site-1	65507	cluster-1panther3_wdr2	10.150.53.1	65504	Online	Established
XN EF79	SDI-5030	dc-site-1	65507	cluster-1panther3_wdr1	10.150.50.1	65504	Online	Established
XN52 DCE7	770-SD	branch-site-2	65508	MPLS-router	100.110.120.1	65502	Online	Established
XN58 9889	SDI-5030	dc-site-1	65506	cluster-1panther2_wdr1	10.150.49.1	65504	Recovery	Unknown
XN58 9889	SDI-5030	dc-site-1	65506	cluster-1panther2_wdr2	10.150.52.1	65504	Recovery	Unknown

**BGP**

Appliance: XN1 1688  
Model: 770-SD  
Site: branch-site-4  
BGP Neighbor IP: 100.110.140.1

**BGP Learned Routes**

Showing 1 to 5 of 23 entries

Destination	Next-Hop	AS Path	Metric	Weight
172.1 /24	100.	65502 65510	0	0
17. /24	100.	65502 65509	0	0
172. /24	100.1	65502 65508	0	0
172. /24	100.	65502 65508	0	0
172. /24	100.1	65502 65508	0	0

**BGP Advertised Routes**

Showing 1 to 3 of 3 entries

Network	Mask
172.	24
100.	24

You can navigate using the page buttons. The lower half of the page displays the BGP Advertised Routes table (if any).

## Displaying OSPF neighbors and routes

SCM displays the OSPF neighbors and routing tables for SteelHead SD 570-SD, 770-SD, 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

You can search also search by site or appliance serial number.



### To display OSPF nodes and routes

1. Choose Health Check > Routing Tables.
2. Select the OSPF Tables tab to display all the appliances in the organization with OSPF. You can search for an appliance by serial number or search for appliances by site name.
3. Optionally, search for the table by specifying the site or the appliance serial number. Partial searches are supported.
4. Select an OSPF appliance to display the OSPF nodes and routes for the appliance.

Figure 12-6. OSPF appliance neighbors and learned routes

The screenshot shows the OSPF configuration page. On the left, there's a search bar for 'Route Prefix' and 'All Prefixes', and a 'Subnet' button. Below that are tabs for 'BGP', 'OSPF', and 'RIP'. A search bar for 'Site/Appliance Search' is also present. The main table lists OSPF appliances with columns: Appliance ID, Model, Site, Neighbors, Routes learnt, and Status. The selected appliance is 770-SD at branch-site-2, with 2 neighbors and 2 routes learnt, and a status of 'Online'.

The right pane shows the detailed view for the selected appliance (770-SD). It has tabs for 'Appliance', 'Model', and 'Site'. The 'OSPF Neighbors' section shows a table with columns: Neighbor ID, Neighbor IP, Area, Local Interface, and State. The table has two entries: 200.21 with IP 172.1.1.1 and Area 9.9.9.9, and 20 with IP 172.1.1.2 and Area 9.9.9.9. Both are in 'Full' state.

The 'OSPF Learned Routes' section shows a table with columns: Destination, Next-Hop, Cost, and Type. The table has two entries: 172.1.1/24 with Next-Hop 172.1.1.2 and Cost 20, and 172.1.2/24 with Next-Hop 172.1.1.2 and Cost 20. Both are of type 'OSPF'.

You can navigate using the page buttons. The lower half of the page displays the OSPF learned routes (if any).

## Displaying NTP server status

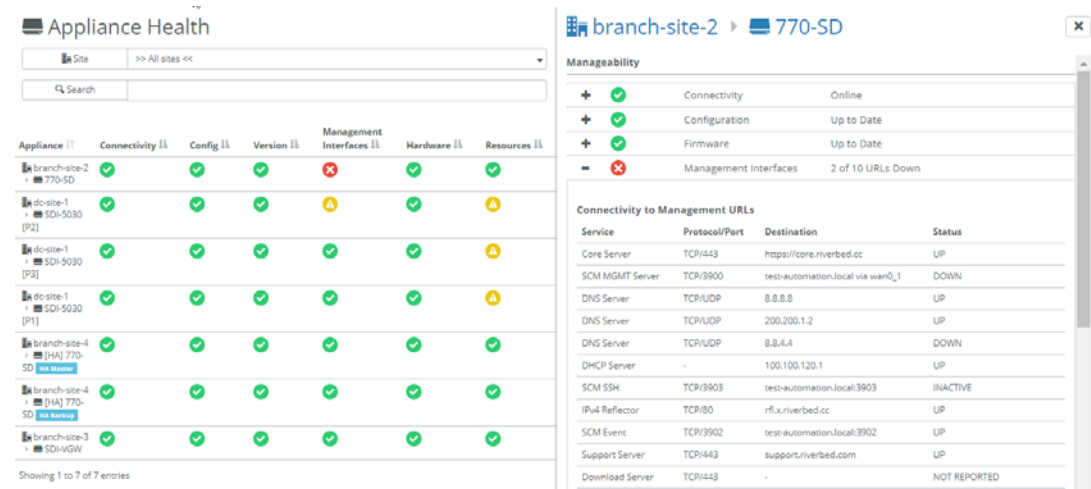
SCM displays NTP server status for SteelHead SD 570-SD, 770-SD, 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch.

### To display NTP server status

1. Choose Health Check > Appliance Health.
2. Select the SteelHead SD to expand the pane.

### 3. Under Manageability, select Management Interfaces.

Figure 12-7. Displaying NTP server status



## Enabling SNMP reporting and logging

SNMP reporting is supported on SteelHead SD SD-570, SD-770, SD-3070 and 2030-SDI appliances located at the branch.

When direct SNMP reporting is enabled, your network management system (NMS) initiates the SNMP poll to all individual appliances in a realm. The appliances send SNMP data directly to the NMS. You can override this setting to limit the SNMP data to all gateways within an organization.

To enable SNMP operations (such as SNMP GET and SNMP WALK or asynchronous traps from a SteelHead SD appliance), you need to provide the NMS interface IP address through which the appliance is reachable. The IP address of the appliance is required:

- For a 2030-SDI located at the data center, use the management IP address. To view the management IP, choose Appliances > IPs tab.
- For the SD-570, SD-770, SD-3070, and 2030-SDI at the branch, use the zone IP address for the appliance. To view the zone IP address, choose Appliances. Select the appliance and click the IPs tab. Scroll down to Under Zone gateway assignment (internal) IPs, to view the zone IP address.

The port number to query the SteelHead SDs is the standard SNMP port 161. You need to specify this port if the NMS doesn't use it by default.

For details on SNMP supported versions and how to configure SNMP, see the *SteelConnect Manager User Guide*.

## Exporting syslog messages to an external syslog server

You can export syslogs to an external server using SCM for SteelHead SD SD-570, SD-770, SD-3070, and 2030-SDI appliances located at the branch.

For syslog reporting, the appliance must be able to reach the remote syslog server. A subset of the syslogs that are useful are exported to the remote syslog server. All logs are stored in a central location.

For details on sending syslog data to a remote server, see the *SteelConnect Manager User Guide*.

## Exporting Netflow data

Exporting NetFlow data is supported on the SDI-2030 on the SDI-130, SDI-330, SDI-1030, virtual gateways, SDI-2030, SDI-5030, and SteelHead SD appliances. NetFlow export is disabled by default.

Appliances running SteelConnect 2.12 can be enabled as flow exporters to export network flow information to a flow collector. In the flow exporter role, the appliances aggregate packet information into flows, and then export the flow records to one or more flow collectors using the IPFIX (IP Flow Information Export) protocol. For IPFIX details, see RFC5101.

The flow collector receives, stores, and preprocesses the flow data from the exporter.

NetFlow monitors all traffic flows that enter and exit the appliances, including flows on the underlay, overlay, and local flows. These flow records provide a central monitor with the SteelConnect view of the network.

For details on configuring NetFlow export support, see the *SteelConnect Manager User Guide*.



# Port Mapping for SteelHead SD

This appendix summarizes the port mapping for SteelHead SD appliances. It includes these sections:

- [“SteelHead SD 570-SD and 770-SD appliances” on page 117](#)
- [“SteelHead SD 3070-SD appliance” on page 119](#)

## SteelHead SD 570-SD and 770-SD appliances

### Physical ports

The SteelHead SD 570-SD and 770-SD appliances have these ports:

- AUX, PRI, LAN0\_0, WAN0\_0, LAN0\_1, WAN0\_1

### CVM ports

The CVM has these ports:

- knet2, knet3, knet4, knet5, knet6, knet7

### Physical port to flows port mapping

Physical port	AUX	Primary	LAN0_0	WAN0_0	LAN0_1	WAN0_1
Flows port	8	9	10	11	12	13

### Service chain virtual machines

Virtual machine (VM)	Pod name	Function
Service virtual machine (SVM)	catfish_secure_node0	Overlay tunnels, QoS, NAT, etc.
Routing virtual machine (RVM)	routing_pod0	Routing protocols, DNS service
Virtual SteelHead (vSH)	vsh_node0	WAN optimization

SteelHead SD dynamically allocates vSwitch ports based on service chain configuration and the WAN optimization toggle.

## vSwitch mapped VM ports

The vSwitch port mapping state can be fetched at runtime using this command on the CVM:

```
XXXXXXD8XXA9FF9-CVM:>orchestrator-agent --get_port_interface_mapping
```

Node name	Interface name	Port
cvm	knet2	AUX
cvm	knet3	PRI
cvm	knet4	LAN0_0
cvm	knet5	WAN0_0
cvm	knet6	LAN0_1
cvm	knet7	WAN0_1
catfish_secure_node0	knet22	WAN0_1
catfish_secure_node0	knet23	WAN0_0
catfish_secure_node0	knet24.1101	LAN0_0
catfish_secure_node0	knet24.1100	LAN0_0
catfish_secure_node0	knet25	LAN0_1
catfish_secure_node0	knet26	— (binds to vSHLAN0_0)
catfish_secure_node0	knet27	— (binds to vSH WAN0_0)
routing_pod0	knet18	LAN0_1
routing_pod0	knet19.1101	LAN0_0
routing_pod0	knet19.1100	LAN0_0
routing_pod0	knet20	WAN0_1
routing_pod0	knet21	WAN0_0
vsh_node0	knet14	PRI
vsh_node0	knet15	AUX
vsh_node0	knet16	LAN0_0
vsh_node0	knet17	WAN0_0

## Bridged VM ports for internal communication

Source	Port name	IP address	Protocol	Remote end	Purpose
CVM	port1	169.254.0.2	Static	Hypervisor mgmt_br bridge	Connects to hypervisor
	port2	169.254.169.254	Static	Hypervisor linklocal_br bridge	Connects to service chain VMs
SVM	port1	—*	Static*	Hypervisor linklocal_br bridge	Connects to CVM
RVM	port1	—*	Static*	Hypervisor linklocal_br bridge	Connects to CVM
vSH	hpn	—*	DHCP	Hypervisor linklocal_br bridge	Connects to CVM

\* Allocated at runtime.

## SteelHead SD 3070-SD appliance

### Physical ports

The SteelHead SD 3070-SD appliance has these physical ports:

- AUX, PRI, LAN3\_0, LAN3\_1, WAN3\_0, WAN3\_1

These ports are present only if you have installed an add-on NIC:

- LAN2\_0, WAN2\_0, LAN2\_1, WAN2\_1

### CVM ports

The CVM has these ports:

- knet2, knet3, knet4, knet5, knet6, knet7

These ports are present only if you have installed an add-on NIC:

- knet8, knet9, knet10, knet11

### Physical port to flows port mapping

Physical port	AUX	Primary	LAN3_0	WAN3_0	LAN3_1	WAN3_1
Flows port	8	9	10	11	12	13

**Note:** The 3070-SD appliance supports add-on NICs. The presence of an add-on NIC can change the total NIC count on the appliance and can also result in different flows port mapping accordingly. Each add-on NIC can carry either two or four NICs. For details on add-on NICs, see [“NIC support” on page 12](#).

### SVM ports

There are four more virtual NICs in SVM for each physical add-on NIC.

## RVM ports

There are four more virtual NICs in RVM for each physical add-on NIC.

## vSH ports

The vSH has these ports:

- hpn, PRI, AUX, LAN0\_0, WAN0\_0, inpath0\_0

vSH has only one LAN-WAN pair and will not change with the addition of any physical add-on NIC.



## TOS, DSCP, QoS Traffic Class Table

This appendix contains the TOS, DSCP, and QoS traffic Classes table. For details on configuring QoS shaping for SteelHead SD appliances, see [“Configuring QoS shaping on SteelHead SD” on page 107](#).

### TOS, DSCP, and QoS Traffic Classes Table

TOS Value	DSCP Value	Traffic Class ID	Traffic Class Priority
0	0	1	Normal
4	1	2	High
8	2	1	Normal
12	3	1	Normal
16	4	2	High
20	5	1	Normal
24	6	1	Normal
28	7	1	Normal
32	8	0	Low
36	9	1	Normal
40	10	1	Normal
44	11	1	Normal
48	12	1	Normal
52	13	1	Normal
56	14	1	Normal
60	15	1	Normal
64	16	2	High
68	17	1	Normal
72	18	2	High
76	19	1	Normal
80	20	2	High
84	21	1	Normal

TOS Value	DSCP Value	Traffic Class ID	Traffic Class Priority
88	22	2	High
92	23	1	Normal
96	24	2	High
100	25	1	Normal
104	26	2	High
108	27	1	Normal
112	28	2	High
116	29	1	Normal
120	30	2	High
124	31	1	Normal
128	32	3	Urgent
132	33	1	Normal
136	34	2	High
140	35	1	Normal
144	36	2	High
148	37	1	Normal
152	38	2	High
156	39	1	Normal
160	40	3	Urgent
164	41	1	Normal
168	42	1	Normal
172	43	1	Normal
176	44	3	Urgent
180	45	1	Normal
184	46	3	Urgent
188	47	1	Normal
192	48	3	Urgent
196	49	1	Normal
200	50	1	Normal
204	51	1	Normal
208	52	1	Normal
212	53	1	Normal
216	54	1	Normal
220	55	1	Normal

TOS Value	DSCP Value	Traffic Class ID	Traffic Class Priority
224	56	3	Urgent
228	57	1	Normal
232	58	1	Normal
236	59	1	Normal
240	60	1	Normal
244	61	1	Normal
248	62	1	Normal
252	63	1	Normal

