riverbed®

SteelHead™ SD Installation Guide

Models 570-SD, 770-SD, 3070-SD, SDI-2030

Version SteelHead SD 2.0, SteelConnect 2.11

August 2018

riverbed®

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107
www.riverbed.com

Part Number
712-00301-02

Contents

Welcome

About this guide

Welcome to the *SteelHead SD Installation Guide*. This guide describes how to install the Riverbed SteelHead SD 570-SD, 770-SD, and 3070-SD appliances when used in conjunction with SteelConnect SDI-2030 and SDI-5030 gateways.

This guide is written for storage and network administrators who are familiar with administering and managing SD-WAN networks.

Document conventions

This guide uses the following standard set of typographical conventions.

Convention	Meaning
italics	Within text, new terms and emphasized words appear in *italic* typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in **bold** typeface.

Courier	Code examples appear in Courier font:
	`amnesiac > enable`
	`amnesiac # configure terminal`

< >	Values that you specify appear in angle brackets: **interface <ip-address>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]**
{ }	Elements that are part of a required choice appear in braces: **{<interface-name> | ascii <string> | hex <string>}**
|	The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: **{delete <filename> | upload <filename>}**

Safety guidelines

Follow the safety precautions outlined in the *Safety and Compliance Guide* when installing and setting up your equipment.

Important: Failure to follow these safety guidelines can result in injury or damage to the equipment. Mishandling of the equipment voids all warranties. Read and follow safety guidelines and installation instructions carefully.

Many countries require the safety information to be presented in their national languages. If this requirement applies to your country, consult the *Safety and Compliance Guide*. Before you install, operate, or service the Riverbed products, you must be familiar with the safety information. Refer to the *Safety and Compliance Guide* if you don't clearly understand the safety information provided in the product documentation.

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 or go to http://www.riverbed.com/services/index.htm.
- **Documentation** - Have suggestions about Riverbed's online documentation or printed materials? Send comments to techpubs@riverbed.com.

1

SteelHead SD Overview

This chapter provides an overview of the SteelHead SD architecture, new features, hardware and software requirements, licensing, upgrading from SteelHead SD 1.0 to 2.0. It includes these sections:

This guide describes how to install a manufactured SteelHead SD appliance. It doesn't describe how to upgrade an existing SteelHead CX570, CX770, or CX3070 appliance to a SteelHead SD appliance. For details on upgrading SteelHead to SteelHead SD, see the *SteelHead SD In-Field Upgrade Guide*.

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

Introducing SteelHead SD

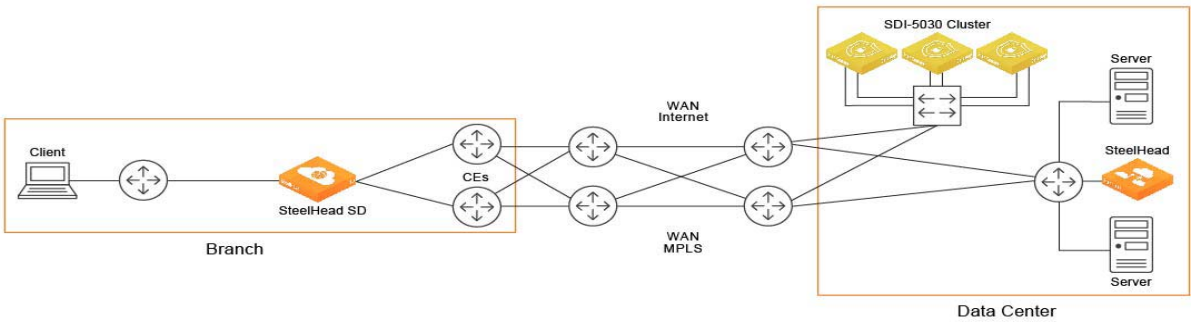
SteelHead SD combines SD-WAN and cloud networking capabilities (powered by SteelConnect) with Riverbed WAN optimization (powered by RiOS) into a single appliance. SteelHead SD seamlessly integrates advanced SD-WAN functionality with industry-leading WAN optimization, security, and visibility services 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 2.0 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 configurations:

- **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 about 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 isn't 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 about configuring SD-WAN features, see the *SteelConnect Manager User Guide* and the *SteelHead SD User Guide*.

SteelHead SD software architecture

SteelHead SD is based on the SteelOS infrastructure. It separates the control and data planes with internal virtual machine (VM) chaining, which provides management-plane autorecovery.

Figure 1-2. SteelHead SD platform architecture

SteelHead SD provides a flexible service platform, consisting of:

- **Routing virtual machine (RVM)** - The RVM is the control plane for all the underlay routing. All configuration from SCM (protocol, interface route maps, and policies) form the Routing Information Base (RIB) and the Forwarding Information Base (FIB), which is sent to the RVM. After the final FIB is formed, it is sent to the service core in the service virtual machine (SVM). SteelHead SD provides a clear separation between the data plane and the control plane.
- **Service virtual machine (SVM)** - The SVM is the core data plane of the appliance, which provides service chained network functions. These VMs include services such as QoS shaping, QoS marking, traffic filtering, path selection, encryption, application identification, and so forth. This architecture allows for extensible plug-and-play services that can be enabled, disabled, or reused in the packet flow chain, which in turn provides faster recovery and minimal disruption. For SteelHead SD, each packet goes through its own set of service functions (LAN ingress, LAN egress, WAN ingress, WAN egress).
- **Virtual SteelHead (VSH)** - The VSH manages WAN optimization services. WAN optimization is service chained into the data path and requires subscription-based licensing. Only one in-path interface is defined on SCM. This single in-path interface represents the VSH that is service chained into the SVM. It doesn't matter what zone you put the VSH in; any packets coming into any zone are sent to the VSH. Because the VSH is separated from the routing plane, it provides WAN optimization functionality for VLANs.
- **Controller virtual machine (CVM)** - The CVM controls and orchestrates the entire system. It's basically the control plane for SD-WAN and routing functions. It obtains all the configuration information from the SVM and RVM. The CVM manages appliance start up, licenses, initial configuration, and interface addressing. For details on CVM recovery from failures, see the *SteelConnect Manager User Guide*.

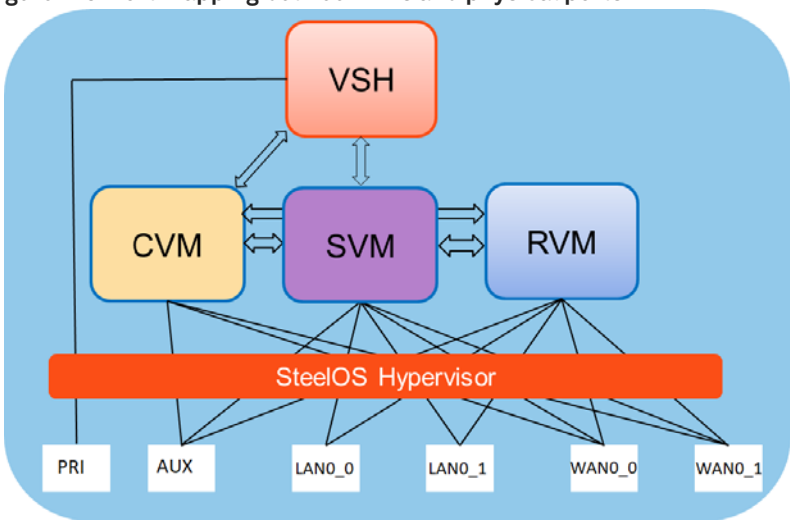
SteelHead SD port mapping between the VMs and physical ports

The SVM and RVM connect to all ports on the SteelHead SD appliance except for the primary port. The primary port (PRI) is connected directly to the VSH. The CVM is connected to the auxiliary (AUX) port and the WAN uplinks only. All the data and control packets are handled by the SVM and RVM.

The SteelHead SD AUX, LAN (LAN0_0, LAN0_1 or on the CX3070 LAN3_0, LAN3_1), and WAN (WAN0_0, WAN0_1 or on the CX3070 WAN3_0, WAN3_1) ports are connected to the SVM and RVM. Basically, there is a Layer 3 edge router on all of these ports.

The AUX and WAN ports are configured as uplinks on SCM. The AUX port can be used as an additional WAN uplink. The AUX port is also the dedicated port for SteelHead SD high-availability deployments.

Figure 1-3. Port mapping between VMs and physical ports



New features in SteelHead SD 2.0

SteelHead SD 2.0 features are supported on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. SteelHead SD 2.0 provides these features:

- **OSPF/ABR enterprise-class routing** - Open Shortest Path First (OSPF) is one of the most popular dynamic routing protocols used as an interior gateway protocol (IGP) in enterprise environments. SteelHead SD 2.0 and the SteelConnect SDI-2030 gateway support single and multi-area OSPF capabilities. Area border router (ABR) is also supported for route distribution and advertisements across a multiarea OSPF network. These advanced OSPF capabilities enable quick and seamless integration with OSPF on the LAN side of enterprise networks.
- **eBGP and iBGP support** - SteelHead SD 2.0 supports External Border Gateway Protocol (eBGP) and Internal Border Gateway Protocol (eBGP). eBGP is typically used in MPLS environments as an exterior gateway protocol (EGP) dynamic routing protocol. With eBGP support on SteelHead SD appliances and the SteelConnect SDI-2030 gateway, the system is able to learn and advertise routes onto the MPLS underlay network. This feature enables easy integration into the service provider's MPLS networks without the need for complex and tedious static route configurations. SteelHead SD 2.0 also supports iBGP for interior routing within the branch office or the data center.
- **ASBR support** - Autonomous system boundary router (ASBR) support enables distribution of routes between different autonomous systems (AS). With full ASBR support, SteelHead SD 2.0 can distribute routes between OSPF on the LAN-side and BGP on WAN-side of your network. As part of this capability, SteelHead SD 2.0 supports route filtering and policy maps that enable you to control which routes can or cannot be distributed. The eBGP and ASBR features enable you to replace customer edge (CE) routers in branch offices.

- **Topology discovery for LAN subnets** - This feature enables distribution of routes from the LAN side of the network into the overlay network. Thus the SD-WAN fabric is aware of all dynamically learned routes on the LAN side of the remote sites. The topology discovery for the LAN subnets feature renders an intelligent overlay fabric for your network, avoiding tedious route configurations.
- **LAN-side VLAN 802.1q support** - Multiple VLANs are very common in Layer 2 (L2) network environments on the LAN side. With this feature, multiple VLANs are supported 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.
- **1:1 active-active mode HA** - With 1:1 active-active HA you can deploy a pair of SteelHead SD appliances or SteelConnect SDI-2030 gateways with failover protection against LAN failures, appliance software and hardware failures, and WAN uplink failures. A key feature in active-active mode is both WAN uplinks are active, which improves overall HA failover performance. Enterprise networks have stringent network reliability requirements and 1:1 HA is a mandatory requirement for ensuring 24/7 business continuity.
- **Troubleshooting and visibility: Health Check, Insights, Syslog, and SNMP** - Health Check is the existing device and network health monitoring tool in SCM. Insights is a flow-based monitoring tool that provides insight into end-to-end deployments with visibility into users, applications, sites, uplinks, and networks. SteelHead SD appliances and SteelConnect SDI-2030 gateways can be monitored using Health Check and are integrated into the Insights reporting tool. They also provide SNMP-based management for easy integration into external operations support systems (OSS) and network management systems (NMS). Syslog support provides advanced logging capabilities to external servers for advanced troubleshooting and visibility.
- **Advanced deployment support: split data center, direct alternate path for mesh environments** - These deployments were introduced in the SteelConnect 2.10 release. With SteelHead SD 2.0/ SteelConnect 2.11, these features are available on SteelHead SD 570-SD, 770-SD, 3070-SD appliances and the SteelConnect SDI-2030 gateway. Collectively these advanced deployment features increase ease of operational integration and network management.
- **Zscaler security support** - The Zscaler cloud security solution is supported on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances and the SteelConnect SDI-2030 gateway located at the branch. SteelHead SD appliances and SteelConnect SDI-2030 gateways also provide Zscaler support for HA deployments.

Feature changes from SteelHead SD 1.0 to SteelHead SD 2.0

This table summarizes the feature changes for SteelHead SD 2.0.

SteelHead SD 1.0 feature	Feature after upgrading to SteelHead SD 2.0
SteelHead-side configuration settings are not preserved when you upgrade to SteelHead SD 2.0/SteelConnect 2.11.	Use the SteelCentral Controller for SteelHead (SCC) backup and restore functions to save and reapply SteelHead-side configuration settings. For details, see the Knowledge Base article, S32688.
Multiple in-path interfaces for WAN optimization are not supported on SteelHead SD 2.0.	SteelHead SD 2.0 does not support multiple in-path interfaces. SteelHead SD 2.0 supports a single in-path interface for WAN optimization. SteelHead SD is a Layer 3 gateway and multiple LAN ports are mapped to a single in-path interface. Multiple in-path interfaces are unnecessary on SteelHead SD appliances. To simplify in-path configuration and for ease-of-use, after upgrading to SteelHead SD 2.0 you will see only a single in-path interface in the SteelHead Management Console or the SCC. If you have multiple in-path interfaces configured for WAN optimization, you must make in-path configuration changes to account for this change.
The gateway bypass feature is not supported with SteelHead SD 2.0.	The SteelConnect gateway bypass feature is no longer supported on SteelHead SD 2.0. If at any point the status of the virtual SteelHead instance shows a failure condition, for example a reboot or a crash, the system stops sending traffic that was destined for the virtual SteelHead. Instead, it bypasses the SteelHead thereby ensuring the traffic is not black-holed. You can compare this behavior with a physical SteelHead entering bypass mode. A remote-site network redesign might be required. Consult with your Riverbed sales engineer or Riverbed Professional Services at http://www.riverbed.com/services/index.html.
Active-passive high availability (HA) is not supported.	Previous versions of SteelHead SD supported an active-passive HA scheme. Because SteelHead SD 2.0 supports active-active HA, you can't upgrade your SteelHead SD 1.0 HA seamlessly to SteelHead SD 2.0 HA. You must first manually unpair your master and backup appliances in SCM, upgrade to SteelConnect 2.11, and reconfigure HA in SCM. For details on configuring HA in SCM, see the *SteelHead SD User Guide* and *SteelConnect Manager User Guide*.

SD-WAN feature restrictions for SteelHead SD 2.0

This table summarizes the SDWAN feature restrictions for SteelHead SD 2.0.

SD-WAN feature	Description
Static uplinks on the WAN	If you have static uplinks on the WAN, a default static route is not added automatically in SteelConnect. On SCM, you must manually add static routes to reach networks that aren't present on the SteelConnect overlay network in order to send packets on those WANs. For details, see the Knowledge Base article, S32693.
WAN AutoVPN memberships	WAN AutoVPN memberships for zones are not supported on SteelHead SD 2.0 and SteelConnect 2.11 appliances.

SD-WAN feature	Description
Redirection of UDP traffic through the virtual SteelHead	Redirection of UDP traffic through the virtual SteelHead is not supported in SteelHead SD 2.0. You will not be able to optimize UDP traffic using the SteelHead IP blade.
Classic VPN	Classic VPN is not supported on SteelHead SD 2.0 and SteelConnect 2.11 appliances.
Flow distribution	Flow distribution for internet traffic across similar uplinks is not supported on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances
General SD-WAN features	The following general SD-WAN features are not supported on SteelHead SD 570-SD, 770-SD, 3070-SD, and SDI-2030 appliances: ▪ PPPoE ▪ LTE uplinks ▪ USB port for tethering (initial ZTP/SCM via USB tethering) ▪ Cloudifi ▪ Agents tab under Sites
LAN-side settings	The following LAN-side settings are not supported on SteelHead SD 570-SD, 770-SD, 3070-SD, and SDI-2030 appliances: ▪ Multiple physical ports in a single zone. ▪ Spanning tree on LAN side. ▪ Multiple physical ports in a zone. ▪ Native VLANs. ▪ zones Import configuration at the Site level. ▪ xLAN option under Site configuration.
Path preference/path selection restrictions	When WAN optimization is enabled and the application target of a traffic rule is set to SSL, SteelConnect does not correctly classify SSL traffic and the traffic will not travel across the SteelHead optimized path. For details, see the Knowledge Base article, S32180.
Traffic path rule restrictions	When the SteelHead is located out-of-path, application-based path preference rules are not honored for deployments using WAN optimization with fixed target in-path rule to the SteelHead. You have these configuration options: ▪ Convert your deployment to an in-path or virtual in-path and adjust SteelHead SD WAN optimization in-path rules to remove the fixed target setting. ▪ Adjust the SteelHead SD WAN optimization in-path rules to pass-through and disable WAN optimization for application types you want to have follow the path preference rules.
Static uplinks on the WAN	If you have static uplinks on the WAN, a default static route is not added automatically in SteelConnect. On SCM, you must manually add static routes to reach networks that aren't present on the SteelConnect overlay network in order to send packets on those WANs. For details, see the Knowledge Base article, S32693.

SD-WAN feature	Description
Source NAT on underlay traffic	Source NAT on underlay traffic is not supported on SteelHead SD 570-SD, 770-SD, 3070-SD, and SDI-203 appliances. SteelHead SD appliances do not perform source NATing on underlay traffic exiting via the Internet uplink if it is destined for a private address, regardless of the configured outbound NAT setting. This is a change from the previous behavior for SteelHead SD 1.0 appliances, if NAT was enabled for an uplink, NAT was performed for all traffic exiting via the Internet uplink. For details on configuring NAT, see the *SteelConnect Manager User Guide*.
RADIUS/Authentication server under Sites configuration in SCM	RADIUS/Authentication server under Sites configuration in SCM is not supported on SteelHead SD 570-SD, 770-SD, 3070-SD, and SDI-2030 appliances. Consult with your Riverbed sales engineer or Riverbed Professional Services at http://www.riverbed.com/services/index.html.

SteelHead SD and SteelConnect feature compatibility by model

Feature	SteelHead SD 570-SD, 770-SD, 3070-SD	SDI-2030	SDI-130	SDI-330	SDI-1030	SDI-5030	Virtual GW	Cloud GW
eBGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
iBGP	Yes	Yes	No	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)	No
Route retraction	Yes	Yes	No	No	No	Yes	No	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	No
Overlay route injection in LAN	Yes	Yes	No	No	No	Yes	No	No
Local subnet discovery	Yes	Yes	No	No	No	Yes	No	No
Static routes	Yes	Yes (LAN and WAN)	Yes (3rd-party routes)	Yes (3rd-party routes)	Yes (3rd-party routes)	Yes	Yes (3rd-party routes)	Yes (3rd-party routes)
VLAN support (LAN side)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—
1:1 Active-Active High Availability	Yes	Yes	No (Active-Passive HA)	No (Active-Passive HA)	No (Active-Passive HA)	No (HA cluster)	No (Active-Passive HA)	No (Active-Passive HA AWS)

Feature	SteelHead SD 570-SD, 770-SD, 3070-SD	SDI-2030	SDI-130	SDI-330	SDI-1030	SDI-5030	Virtual GW	Cloud GW
Brownfield transit for internet-only branch	Yes (As an edge device only)	Yes	Yes (As an edge device only)	Yes (As an edge device only)	Yes	Yes	Yes (As an edge device only)	Yes (As an edge device only)
Native VLAN support	No	No	Yes	Yes	No	No	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	The SteelHead SD 570-SD and 770-SD appliances are desktop models. The SteelHead SD 3070-SD appliance requires a 19-inch (483 mm) four-post rack. For details, see the *Rack Installation Guide*.
SteelHead SD Management Console	The Management Console has been tested with all versions of Chrome, Mozilla Firefox Extended Support Release version 38, and Microsoft Internet Explorer 11. JavaScript and cookies must be enabled in your web browser.
SteelConnect and SteelConnect Manager (SCM)	SteelHead SD requires SteelConnect 2.11or later. 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.
SteelCentral Controller for SteelHead (SCC)	We recommend you have SCC 9.7.1 installed.

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 *SteelConnect 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 Appendix , "SteelConnect Connection Ports."

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 SD-WAN service supports proprietary MIBs accessible through SNMPv2 and SNMPv3. For detailed information about the SD-WAN service MIB, see the *SteelConnect Manager User Guide*.

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

For detailed information on SteelConnect SNMP support, see the *SteelConnect Manager User Guide* and the *SteelHead SD User Guide*.

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 aren't 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*.

Licensing

SteelHead SD 2.0 requires a WAN optimization subscription license if you want to use the WAN service. The WAN optimization subscription license is an optional purchase. (Existing SteelHead SD 1.0 customers are not required to purchase a WAN optimization subscription license.)

SteelConnect SD-WAN service licensing

The SteelConnect SD-WAN service requires a gateway management subscription license that is managed by SCM. You must obtain this license before you begin the installation process.

After purchasing SteelHead SD, you will receive these emails:

- An email with the license token and SteelConnect serial number. You redeem the token in SCM where all hardware nodes and license keys are added to your organization. Each token is redeemable only once.
- An email that contains the URL for connecting to SCM and the default login and password: **admin** and **pppp**. This email is requested by the sales team and sent by the Riverbed Cloud Operations team.

If you don't receive these emails, contact your sales representative or Riverbed Support at https://support.riverbed.com.

To redeem the SD-WAN service token

1. Open the email you received from Riverbed and copy the token.
2. Connect to SCM.
3. Choose Organization > Licenses.
4. Click **Redeem Token** and paste the token into the text box.
5. Click **Submit**.

If automatic licensing fails, go to the Riverbed Licensing Portal at https://licensing.riverbed.com/ and follow the instructions for retrieving your licenses. The licensing portal requires a unique product ID such as a serial number, a license request key (activation code), or a token, depending on the product. Online instructions guide you through the process.

SteelHead WAN optimization service licensing

The SteelHead WAN optimization service requires an MSPEC license. Once you connect SteelHead SD to the network, the system automatically contacts the Riverbed Licensing Portal to retrieve and install license keys for the WAN optimization service.

If automatic licensing fails, go to the Riverbed Licensing Portal at https://licensing.riverbed.com/ and follow the instructions for retrieving your licenses. The licensing portal requires a unique product ID such as a serial number, a license request key (activation code), or a token, depending on the product. Online instructions guide you through the process.

Upgrading from SteelHead SD 1.0 to 2.0

All SteelHead SD 1.0 customers will be automatically upgraded to SteelHead SD 2.0 and SteelConnect 2.11. SteelConnect automatically upgrades to 2.11 according to the schedule and restrictions you have set in SteelConnect Manager (SCM). For details on scheduling updates in SCM, see the *SteelConnect Manager User Guide*.

Before proceeding with the SteelHead SD 2.0 upgrade process:

- Previous versions of SteelHead SD supported an active-passive HA scheme. Because SteelHead SD 2.0 supports active-active HA, you can't upgrade your SteelHead SD 1.0 HA seamlessly to SteelHead SD 2.0 HA. You must first manually unpair your master and backup appliances in SCM, upgrade to SteelConnect 2.11, and reconfigure HA in SCM. For details, see the *SteelHead SD User Guide*.
- You must back up your SteelHead WAN optimization configuration prior to upgrading to SteelHead SD 2.0. Secure vault contents (that is, certificates and keys) are not saved during the upgrade process; you must reinstall any SSL or proxy certificates. You can use the backup and restore functions on the SCC or the SteelHead Management Console to save and reapply the SteelHead configuration settings.
  - To back up your system and SteelHead appliances from the SCC, choose Manage > Operations: Backup/Restore to back up your configuration. For details, see the *SteelCentral Controller for SteelHead User Guide*.
  - To save your SteelHead configurations from the SteelHead Management Console, choose Administration > System Settings to save and copy your configuration to a local machine. For details, see "Managing configuration files," in the *SteelHead User Guide*.
- To upgrade to SteelHead SD 2.0, you must have internet connectivity for the SteelHead and the SteelConnect virtual gateway. With internet connectivity, both SteelHead perpetual and SteelConnect virtual gateway subscription licenses will be applied as part of the SteelHead SD 2.0 upgrade process.
- SteelHead SD 2.0 supports a single in-path interface for WAN optimization. SteelHead SD is a Layer 3 (L3) gateway, and multiple LAN ports are mapped to a single in-path interface—multiple in-path interfaces are unnecessary on SteelHead SD appliances. To simplify in-path configuration and for ease-of-use, after upgrading to SteelHead SD 2.0 you will see only a single in-path interface in the SteelHead Management Console or the SCC. If you have multiple in-path interfaces configured for WAN optimization, you must make in-path configuration changes to account for this change.
- The SteelConnect gateway bypass feature supported on SteelHead SD 1.0 is no longer supported on SteelHead SD 2.0. If at any point the status of the virtual SteelHead instance shows a failure condition, for example a reboot or a crash, the system stops sending traffic that was destined for the virtual SteelHead. Instead, it bypasses the SteelHead thereby ensuring the traffic is not black-holed. You can compare this behavior with a physical SteelHead entering bypass mode.

- You might need to recable SteelHead SD appliances in HA deployments when you upgrade to SteelHead SD 2.0. The AUX port is mandatory for back-to-back connectivity for SteelHead SD 2.0 HA deployments.

To upgrade SteelHead appliances using the SCC

1. Choose Manage > Upgrades: Upgrade Appliances to display the Upgrade Appliances page.
2. Click **Launch a new upgrade job** to display the Welcome page.
3. Click **Select your appliances** to display the Select your appliances to upgrade page.
4. Complete the configuration as described in this table.

Setting	Description
Choose product type	Select the product type from the drop-down list.
Choose target version	Select the target version from the drop-down list.
View ineligible appliances	Click to view the ineligible appliances for the upgrade job.
Filter	Select Show All from the drop-down list to view all appliances eligible for upgrade. You can filter appliances by current version, group, hostname, IP address, model, and serial number. ▪ **Show Selected Appliances** - Select an appliance to view and select this option from the drop-down list to view appliance details. Click Return to Eligible Appliances to return to the list.
Select/Unselect all	Select the check box to either select or unselect all the appliances.

5. Click **Configure Settings** to display the Settings page and complete the configuration as described in this table.

Setting	Description
Notes for this upgrade job	Optionally, specify any notes for the new upgrade job.
Upgrade Time	▪ **Upgrade Now** - Select this option to start the upgrade now. ▪ **Schedule the upgrade** - Select this option to schedule the upgrade. ▪ **UTC time** - Specify the UTC date and time in this format: yyyy/mm/dd hh:mm:ss ▪ **Local time** - Specify the local date and time in this format: yyyy/mm/dd hh:mm:ss
Reboot Options	▪ **Reboot immediately after installing the image** - Select this option to reboot the appliance immediately after installing the image. ▪ **Schedule the reboot after installing the image** - Select this option to schedule the reboot. ▪ **UTC time** -Specify the UTC date and time in this format: yyyy/mm/dd hh:mm:ss ▪ **Local time** - Specify the local date and time in this format: yyyy/mm/dd hh:mm:ss ▪ **Don't reboot** - Select this option to not reboot the appliance.

6. Click **Summary** to display the Summary page that lists your upgrade settings.
7. Click **Upgrade** to launch the software upgrade.

For detailed procedures, see the *SteelCentral Controller for SteelHead User Guide*.

To upgrade the software using the SteelHead Management Console.

1. Connect to the SteelHead Management Console.
2. Choose Administration > Maintenance: Software Upgrade.
3. Enter the SteelHead SD upgrade image URL in the From URL field.
4. Click **Install**.

Important: The software image is downloaded and installed on the other partition with RiOS still running on the appliance. You can stop the upgrade process at this step and retain your original SteelHead image and configuration settings. The new software is only installed once you reboot the appliance.

---

5. Choose Administration > Maintenance > Reboot/Shutdown.
6. Click **Reboot**. The appliance will reboot into SteelHead SD installer to install the product image. The installation takes approximately twenty minutes.

For detailed procedures, see the *SteelHead User Guide*.

Preparing your site for installation

Before you begin, make sure your shipment contains all the items listed on the packing slip. If it doesn't, contact your sales representative.

Your site must meet these requirements:

- It is a standard electronic environment where the ambient temperature doesn't exceed 104°F (40°C) and the relative humidity doesn't exceed 80% (noncondensing).
- Ethernet connections are available within the standard Ethernet limit.
- There is space on a standard four-post 19-inch Telco-type rack. For details about installing the SteelHead in a rack, see the *Rack Installation Guide* or the printed instructions that were shipped with the system. (If your rack requires special mounting screws, contact your rack manufacturer.)
- A clean power source is available, dedicated to computer devices and other electronic equipment.

The appliance is completely assembled, with all the equipment parts in place and securely fastened. The appliance is ready for installation with no further assembly required.

Before you begin

- Any interim firewalls must be configured to allow traffic on ports 80 and 443 so that the software installation and SCM operations aren't blocked. (Also any additional firewall configurations must allow traffic to and from the SteelHead appliance that is being upgraded.)
- We highly recommend that your network provides a DHCP service so the appliance can establish a connection automatically.

2

Installing SteelHead SD

This chapter describes how to install and perform the initial configuration of the SteelHead SD appliance. It includes these sections:

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

Overview

You use SteelConnect Manager (SCM) to install, configure, and manage the SteelHead SD appliances in your SD-WAN network. SteelConnect uses a zero-touch provisioning (ZTP) to install and manage your appliances, enabling you to configure and visualize the appliances in your network before you install and connect the hardware.

Defining an organization

SCM uses these terms to describe the network:

- **Organization** - A company representing an end customer. You can assign administrative rights to individual administrator accounts per organization. You can also manage appliances and licensing per organization.
- **Site** - A physical location of one or more office buildings, a hosting center, or a cloud location that make up the organization. A site houses a SteelConnect gateway and uses a permanent DNS alias. Every site requires a local network zone and at least one internet uplink. The zone is automatically created when you create a site.
- **Zone** - Zones are at the center of an SD-WAN network. A zone is equivalent to a Layer 2 IP segment within a site. Zones define subnets and VLANs on gateways. Every site has at least one zone and can have multiple zones. When you create a site, SteelConnect automatically adds a default zone.

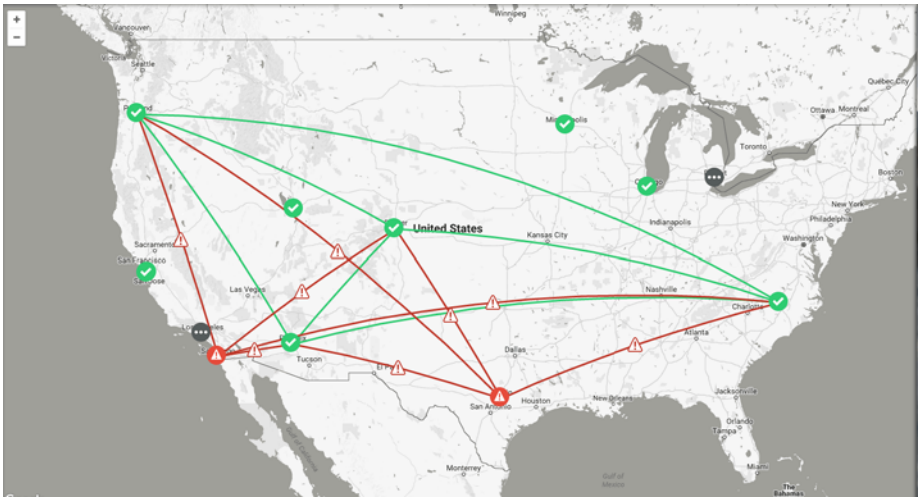
SCM is delivered with a default organization and site. You add your company name and basic information for your organization or change and customize this information later. For details about defining an organization, network, sites, zones, and uplinks, see the *SteelConnect Manager User Guide*.

To log in to SCM

- Using the SCM URL emailed to you, log in to SCM using the default username (**admin**) and the default password (**pppp**).

  After a successful log in, you're greeted by the dashboard.

Figure 2-1. SCM dashboard



The dashboard map updates dynamically to keep an accurate visual overview of your network. You can always refer to the dashboard map as you define your topology to make sure the deployment is accurate.

To change the default name and location of the organization

1. Choose Organization to display the default organization settings.
2. Change the organization name.
3. Click **Submit**.
4. Under location, type the company headquarters physical address.

5. Click **Submit**.

Adding sites

The next task is to create one or more sites. If you have a lot of sites you can also do a bulk import. For detailed information creating sites and bulk imports, see “Creating Sites” in the *SteelConnect Manager User Guide*.

All internet connections, or uplinks, are automatically created when you set up your sites. By default, all uplinks use DHCP; however, SteelConnect also supports static IPs and PPPoE with authentication. For details, see “Creating uplinks” in the *SteelConnect Manager User Guide*.

To add sites

1. Choose Network Design > Sites.
2. Click **New Site** to expand the page.
3. Add a site tag: for example, headquarters.
4. Add the site’s location: for example, San Francisco.
5. Type the site’s address, country, and time zone.
6. Click **Submit**.
7. Repeat the steps for the remaining sites in your network topology.

A zone is automatically created when you create a site. You can modify a zone now or wait until you have completed the installation process. For details, see the *SteelConnect Manager User Guide*.

Changing the default zone in a site

Zones are at the center of an SD-WAN network. A zone is equivalent to a Layer 2 IP segment within a site. Zones define subnets and VLANs on gateways.

Every site has at least one zone and can have multiple zones. When you create a site, SteelConnect automatically adds a default zone.

Zones can cross sites. For example, for a business application that involves a call center that requires peer-to-peer networking, you can stretch a single zone across multiple sites, providing users all over the globe with one universal security policy applied to the same IP zone.

You can add zones to any sites or any organization. A zone belongs to a site, but it can also belong to multiple sites. A site is a location like an office building, a hosting center, or a cloud location. Every site has at least one internet uplink and one local network zone.

To change the default zone

1. Choose Network Design > Zones.

2. Select a zone, click **Settings**, and update the zone name.
3. Select the IP tab, and change the IP address to match your LAN subnet on the SteelHead.
4. Click **Submit**.

By default, all sites are configured with an internet uplink and a AutoVPN uplink which automatically creates secure tunnels over internet links to create a secure overlay network.

You can add additional zones to a site, if necessary. For details on configuring zones, see "Designing a Network," in the *SteelConnect Manager User Guide*.

Adding shadow appliances

SCM stores all configurations, including your existing and future network plans. This means you can either add an appliance when you physically have it or you can preplan and configure an appliance by adding a *shadow appliance* and later drop the physical appliance into the topology with no further configuration.

To add shadow appliances

1. Choose Appliances > Overview.
2. Click **Add appliances** and select Create Shadow Appliance.
3. Select 570-SD, 770-SD, or 3070-SD from the model drop-down list.
4. Select the site where you want to deploy the shadow appliance from the site drop-down list.
5. Click **Submit**.
6. Repeat these steps for each of your appliances.

   After adding the virtual gateways, SCM automatically connects them using AutoVPN to create secure VPN tunnels. Later, you'll register the gateways to transform them from shadow appliances to physical appliances.
7. Choose Network Design > Uplinks to see that SCM has automatically assigned uplinks to the new gateways.

Before deploying the hardware, you can configure other SteelConnect features now or wait until later. For details about configuring SteelConnect features, see the *SteelConnect Manager User Guide*.

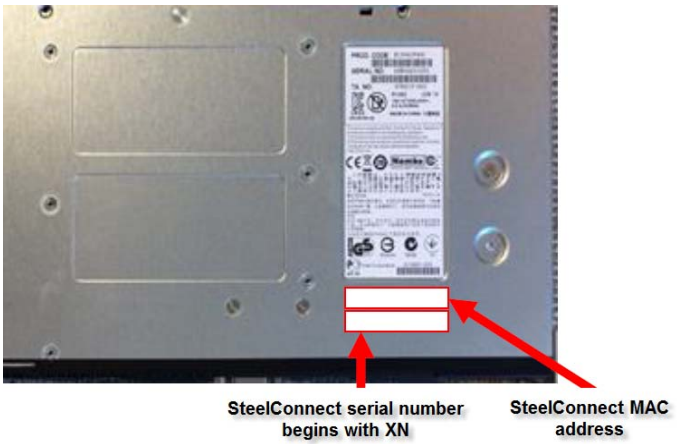
Next, you register the physical appliances to transform them from shadow appliances into physical appliances using the SteelConnect gateway serial number.

Registering appliances

The SteelConnect serial number is in the email from Riverbed that you received when your sales order was confirmed. It is also available on the appliance label. The SteelConnect gateway serial number always begins with the prefix XN. Find that serial number and MAC address on the appliance and write them down.

The SteelHead SD 3070-SD label is located on top of the appliance. The SteelHead SD 570-SD, 770-SD labels are located on the side of the appliance.

Figure 2-2. SteelConnect serial number and MAC address



Important: Make sure you register your appliances using the SteelConnect serial number starting with XN. If you don't, SCM won't autodetect the appliances when you register them.

To register a hardware appliance

1. Choose Appliances > Overview to view the shadow appliances you just created.

Figure 2-3. Example of a shadow appliance

2. Select the shadow appliance to expand the page.
3. Choose Actions > Register hardware.

Figure 2-4. Registering appliances

4. Type the SteelConnect serial number. Make sure you use the SteelConnect gateway serial number that begins with XN.
5. Click **Submit**.
6. Repeat the steps to register the remaining appliances.

The provisioning server hands off the appliance when it connects into the particular organization and site. It gives the appliance its configuration, brings it online, performs all firmware upgrades, and realizes your design on the appliance in the real world.

Configuring the primary and LAN ports in SCM

The next task is to configure the ports for the SteelHead SD appliance.

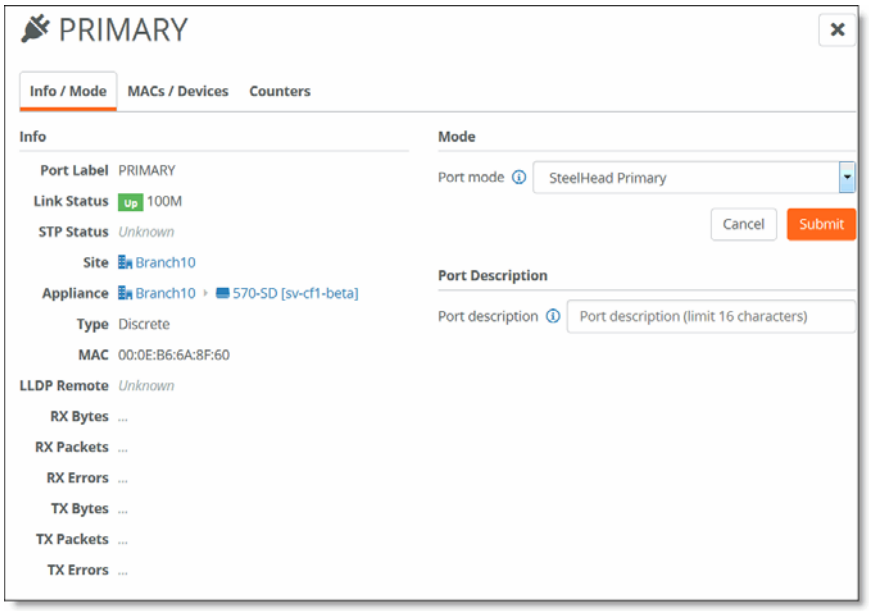
You set the LAN port mode to single-zone uplink for the SteelHead WAN optimization service. By default, the LAN port is disabled on SteelHead SD appliances unless it is explicitly enabled. If you don't enable the LAN port, SteelConnect won't see either the SteelHead WAN optimization service or the clients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

You set the primary port mode to SteelHead Primary for the SteelHead SD appliance.

To configure the primary and LAN ports

1. Choose Appliances > Ports.
2. Select the site with the SteelHead SD appliance from the drop-down list. The ports for the appliance are displayed.
3. Select the primary port to expand the page.

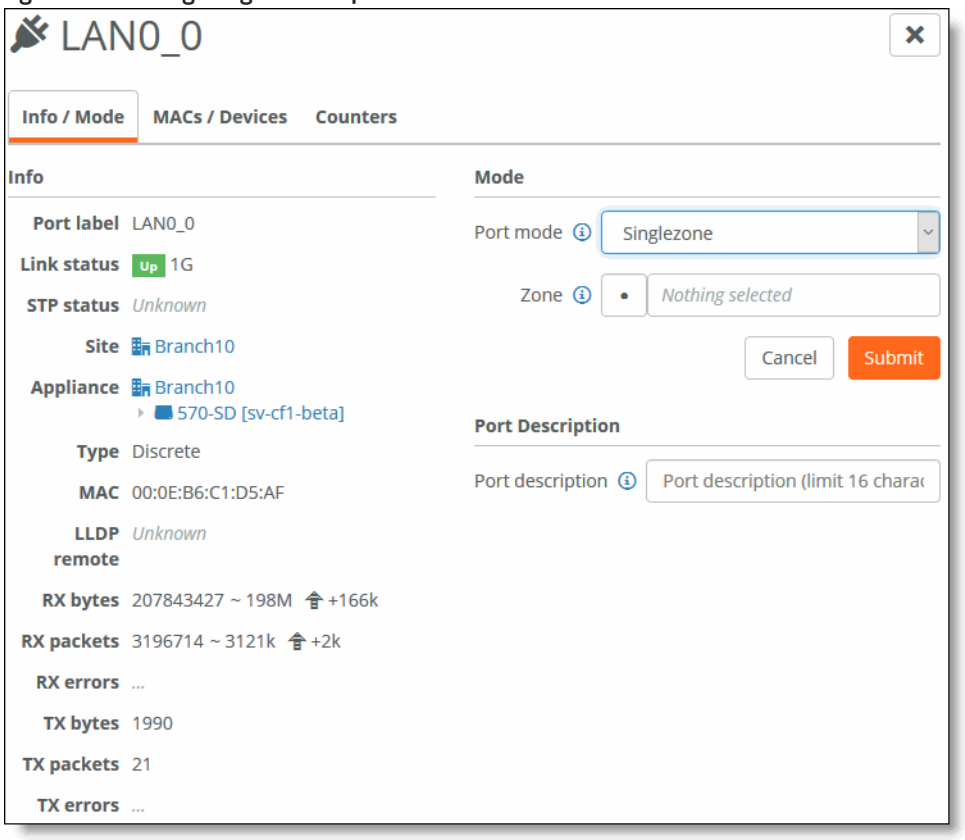
Figure 2-5. Configuring the primary port



4. Select SteelHead Primary for the Port mode.
5. Optionally, provide a description of the port.
6. Click **Submit**.

7. Select the LAN port for the SteelHead SD appliance. The Info/Mode tab is displayed.

Figure 2-6. Configuring the LAN port



8. Select Singlezone for the Port mode.

9. Select the zone from the drop-down list.

10. Optionally, specify a patch label.

11. Click **Submit**.

You can continue configuring your LAN ports and WAN uplinks or you can do this later. For detailed information about configuring multizone LAN trunk ports, see the *SteelHead SD User Guide*. For detailed information on WAN uplinks, see the *SteelConnect Manager User Guide*.

Next, you configure an IP address for the in-path interface (inpath0_0). The default gateway for that IP address will be the default gateway of the zone you select.

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

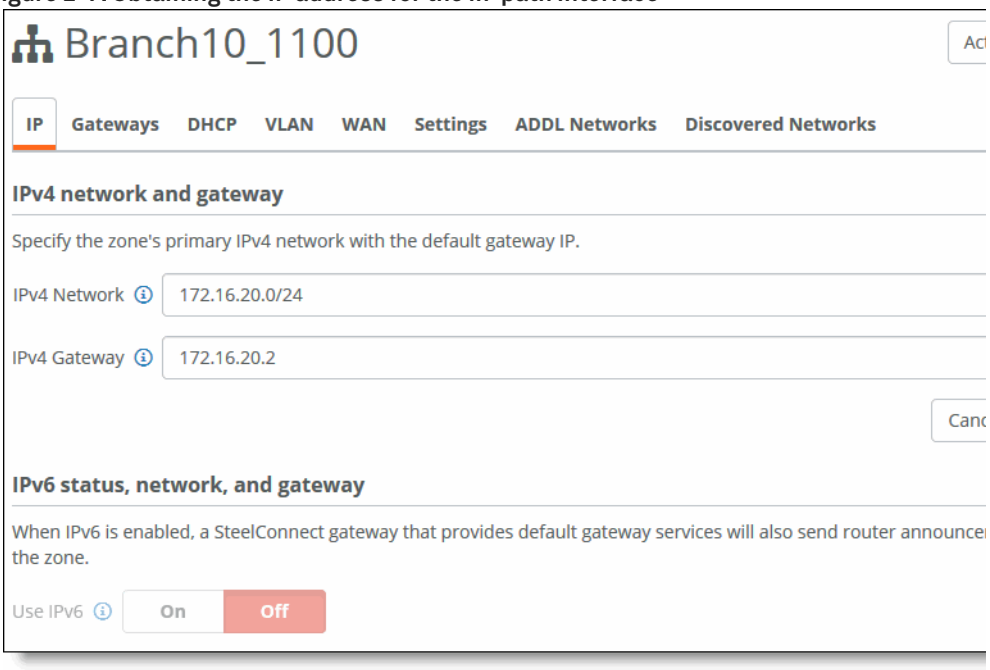
A single in-path interface address is assigned in SCM for the SteelHead SD appliance. You choose an IP address for the LAN zone in which the SteelHead SD is installed. You will use this IP address to configure the in-path interface on the virtual SteelHead appliance.

Note: If the LAN port attached to the SteelHead SD appliance is in a VLAN trunk, the virtual SteelHead appliance 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.

To assign the in-path IP address and 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.
3. 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 2-7. Obtaining the IP address for the in-path interface



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.

4. 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 appliance.

Configuring SteelConnect to act as DHCP server

For SteelConnect to act as a DHCP server, you configure the SteelHead LAN and primary ports to connect to the same switch so that the SteelConnect gateway acts as the DHCP server. This configuration provides the primary IP address of the virtual SteelHead and reports it in SCM.

As the virtual SteelHead instance boots within SteelHead SD, it's primary interface tires to obtain the primary IP address via DHCP. We highly recommend that the SteelHead SD primary port is attached to a network where a DHCP service is available. There are two ways to connect to a DHCP server:

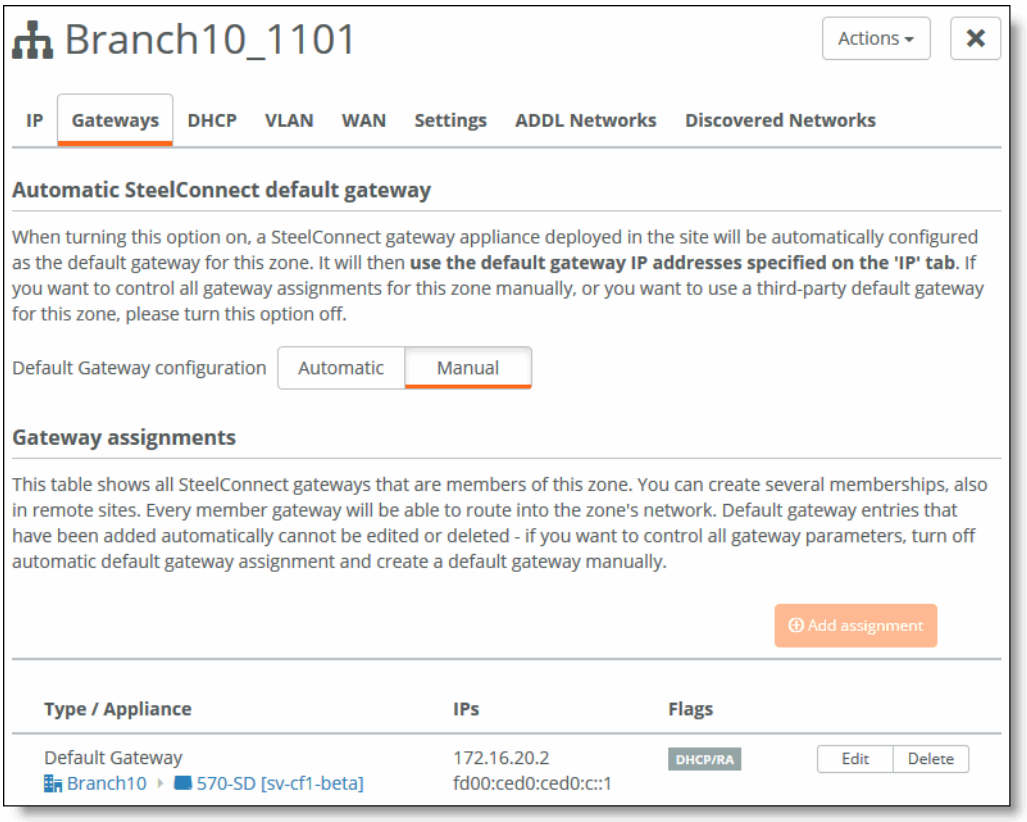
- **Through the switch** - Connect the LAN port and primary port to the switch port and configure in the same VLAN.
- **Back-Back** - Connect the LAN port directly to the primary port.

To configure SteelConnect to act as a DHCP server

1. When you cable the appliance, make sure you connect the LAN port and primary port to the same switch.
2. Choose Networks Design > Zones.
3. Select the zone with the SteelHead SD appliance to expand the page.
4. Select the Gateways tab.
5. Under Default Gateway configuration, click **Manual**.

6. Under Gateway assignments, click **Edit**. (You can also add a new assignment if necessary.)

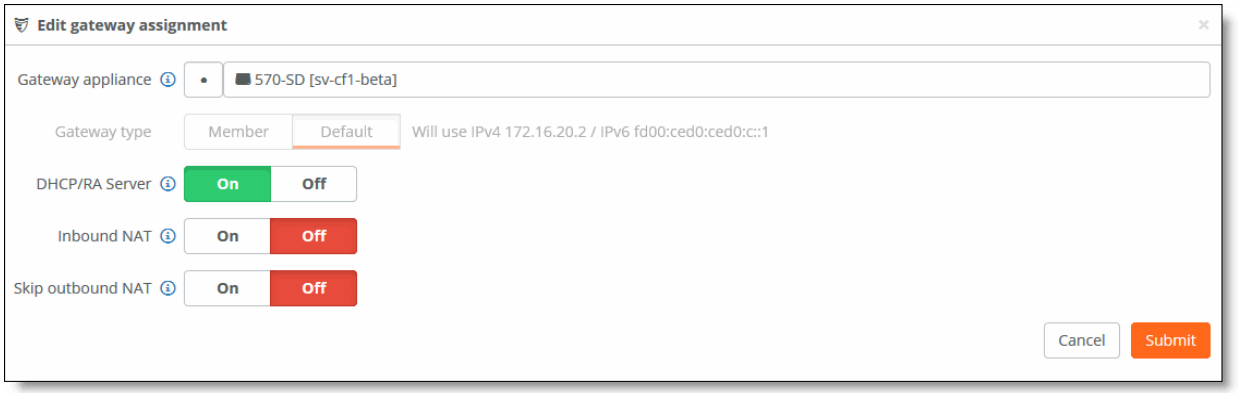
Figure 2-8. Editing the gateway to act as the DHCP server



7. Make sure the DHCP/RA Server is on. (It will be green.)

8. Click **Submit**.

Figure 2-9. DHCP/RA Server setting to On

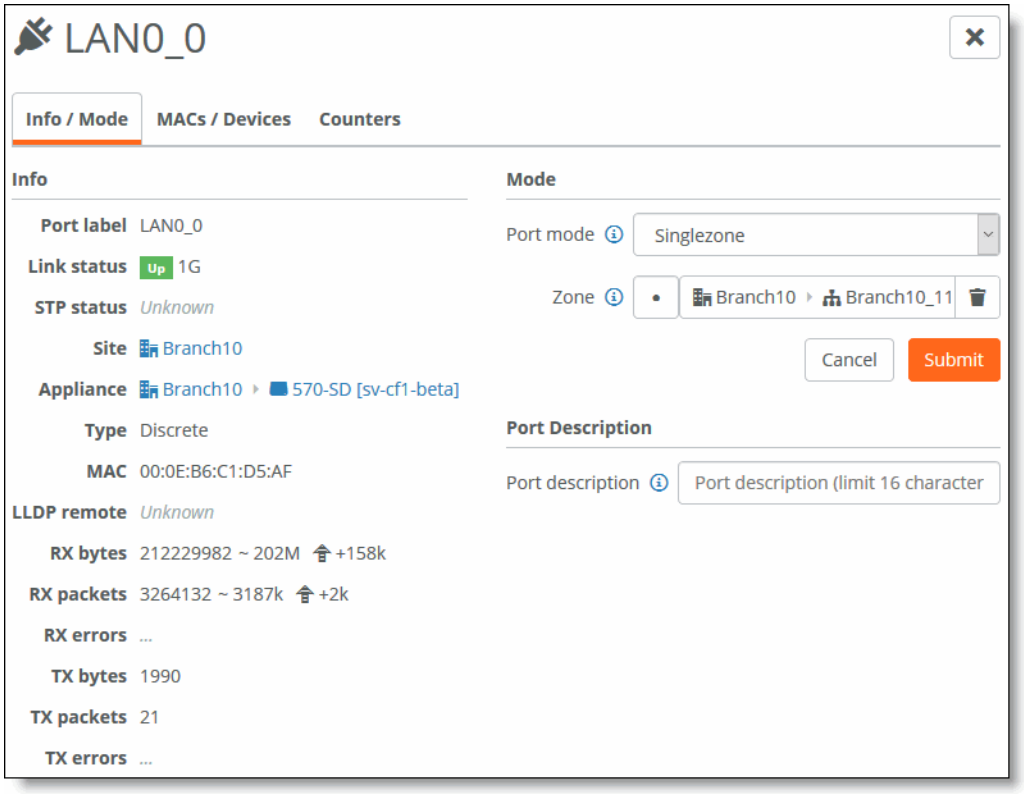


9. Choose Appliances > Ports to associate the LAN port to the appropriate Zone.

10. Select the site with the SteelHead SD appliance from the drop-down list.

11. Select the LAN port you want to associate.

Figure 2-10. Associating the LAN port to a zone



12. Select the zone from the Zone drop-down list.

13. Click **Submit**.

Cabling the appliance

In SteelHead SD, both the WAN and LAN ports are connected through the service virtual machine (VM).

The key task is to connect at least one WAN port to an uplink from a service provider that provides a path to the internet:

- On the SteelHead SD 570-SD or 770-SD appliances, use a straight-through cable to connect either the WAN0_0 or WAN0_1 ports to a WAN router with an internet uplink or an MPLS uplink for back-hauled internet traffic.
- On the SteelHead SD 3070-SD appliance, use a straight-through cable to connect either the WAN3_0 or WAN3_1 port to a WAN router. Internet reachability can be via a local breakout or via a data center over MPLS—whichever you prefer.

WAN ports require an IP address as they represent the uplink configuration. The SteelHead in-path interface must have an IP address and VLAN ID—this can be in any SteelConnect zone.

After powering on the appliances, each appliance will download the latest SteelConnect firmware if necessary, and reboot. After the appliances are updated with the latest firmware, SteelConnect will automatically start building a secure overlay of VPN tunnels.

Important: We recommend you cable the primary port to a DHCP reachable port on the switch.

Port definitions

For port locations, see Appendix A, "SteelHead SD Technical Specifications."

Port	Description
Primary	The primary port is the management interface that enables you to connect to the SteelHead Management Console. Preferably the primary port connects to a DHCP reachable port on a switch. In a deployments where data store synchronization is used between two adjacent SteelHead appliances, the primary interface must be used for the data synchronization of traffic.
AUX	The AUX port can be used as an additional WAN uplink on SteelHead SD. The AUX port is also the dedicated port for SteelHead SD HA deployments. The AUX port is not available for data store synchronization between two adjacent SteelHead appliances, the primary interface must be used for the synchronization traffic.
WANX_X	WAN ports function as uplinks for internet service providers that connect to the internet. Connect the WAN port to a WAN router using a straight-through cable. For SteelHead SD 570-SD and 770-SD appliances, the default internet access port is WAN0_0 or WAN0_1. For SteelHead SD 3070-SD appliances, the default internet access port is WAN3_0 or WAN3_1.
LANX_X	Connect the LAN port to the LAN switch using a straight-through cable. For SteelHead SD 570-SD and 770-SD appliances, the default port is LAN0_0 and LAN0_1. For SteelHead SD 3070-SD appliances, the default port is LAN3_0 or LAN3_1.
Console	Connects you to the controller virtual machine (CVM) using a serial cable. CVM is the runtime management platform that connects you to the hypervisor via SSH. Typically, you should be able to troubleshoot and modify network issues using SCM.

Cabling the SteelHead SD appliance

This section describes how to cable a SteelHead SD appliance.

For detailed information on how to cable the SteelConnect SDI-2030 gateway, see the *SteelConnect Gateway Hardware Installation Guide (SDI-2030, SDI-5030)*.

To cable the SteelHead SD

1. Plug the straight-through cable into the primary port on the SteelHead SD appliance. We recommend that this is a DHCP port that connects to a DHCP server.

Figure 2-11. Connecting the primary port to the LAN switch

2. Plug the straight-through cable into at least one LAN port (LAN0_0, LAN0_1, and so on) to the LAN port on the switch.

Figure 2-12. Connecting the LAN switch to the LAN port

3. Connect at least one WAN port to an uplink from a service provider. For example, on a SteelHead SD 570-SD or 770-SD appliance, use a straight-through cable to connect the WAN0_0 or WAN0_1 port to a WAN router. On a SteelHead SD 3070-SD appliance, connect either the WAN3_0 or WAN3_1 port to a WAN router. Internet reachability can be via a local break-out or via a data center over MPLS.

Figure 2-13. Connecting the WAN port to the WAN router

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 appliance in-path IP address. The in-path IP address must be within the LAN zone subnet that you have defined.

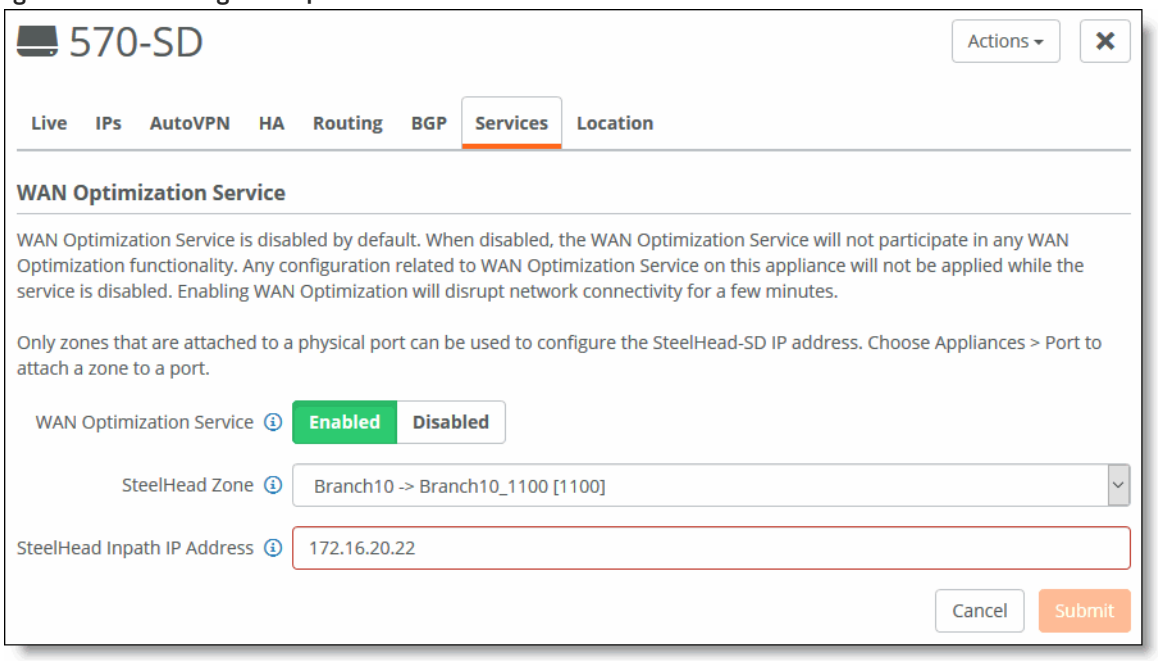
The WAN optimization service is disabled by default. When disabled, the WAN optimization service will not participate in any WAN optimization functionality. If disabled, any configuration related to WAN optimization service on this appliance will not be applied.

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

1. Choose Appliances > Overview.
2. Select the SteelHead SD appliance to expand the page.
3. Select the Services tab.

Figure 2-14. Enabling WAN optimization in the SCM



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 Inpath IP** - 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.
- **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.

5. Click **Submit**.

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

Identifying the primary IP address of the SteelHead

You use the primary IP address of the SteelHead 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 "Configuring SteelConnect to act as DHCP server" on page 33.
- **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 (see Figure 2-2) 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

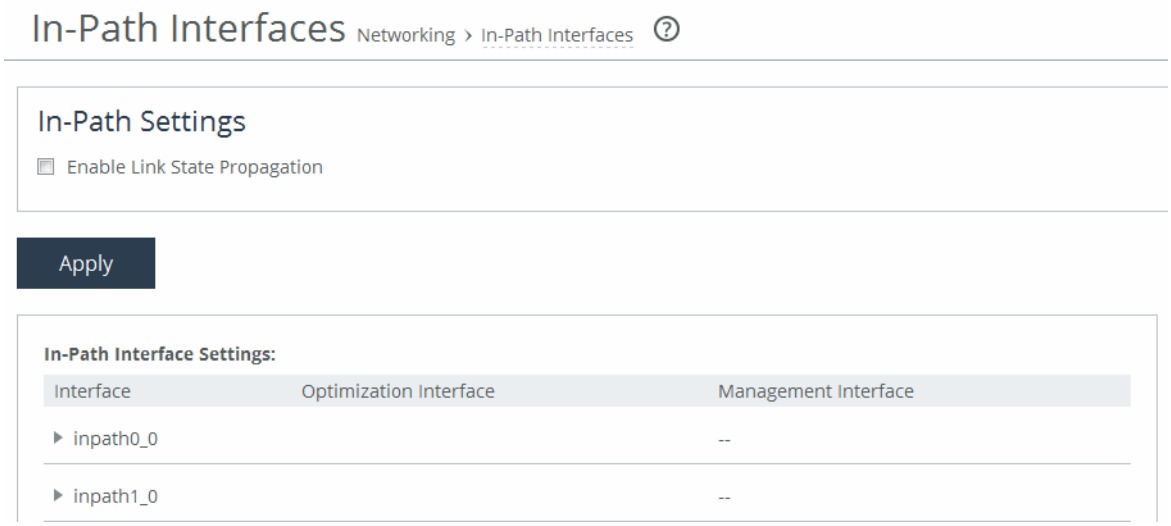
These instructions describe how to configure the in-path interface and default gateway using the SteelHead Management Console.

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 virtual SteelHead

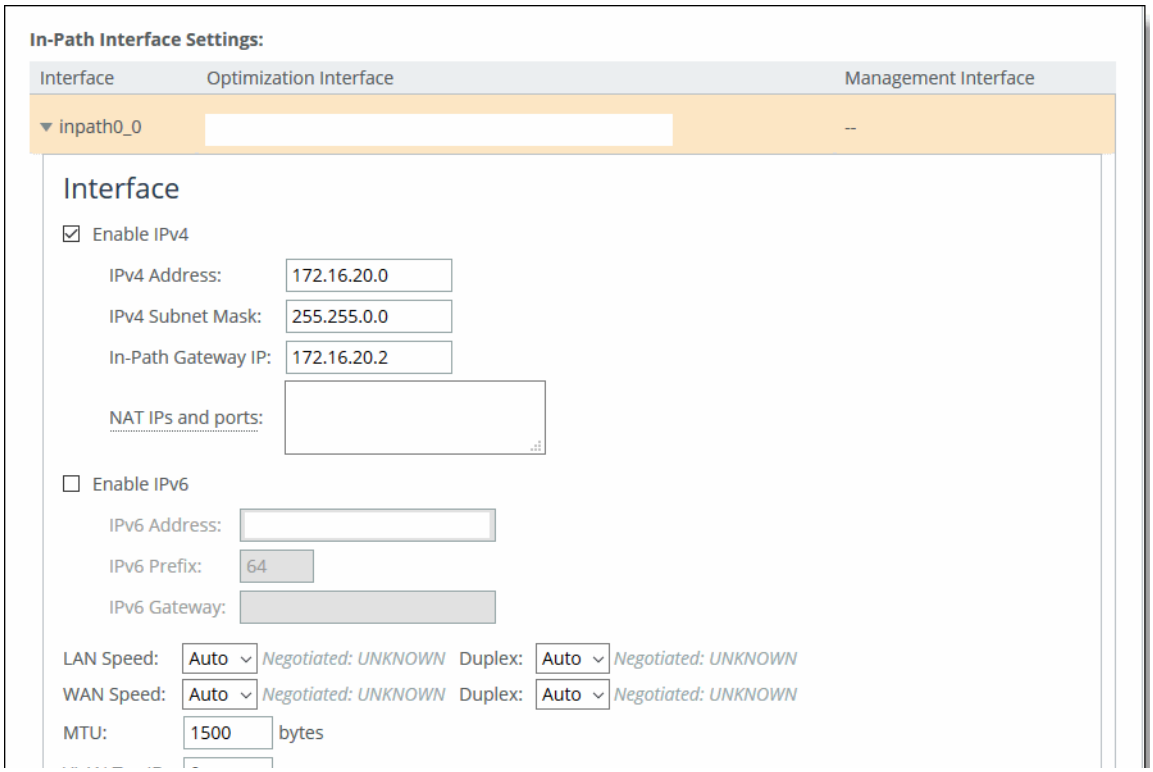
1. Using the Primary IP address you obtained from SCM, SCC, or the DHCP server, enter it in the location box of your web browser using HTTPS. The sign in page for the SteelHead Management Console is displayed.
2. Specify the default user login (**admin**) and password (**password**).
3. Click **Sign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

Figure 2-15. In-Path Interfaces page



5. Select the interface to expand the page.

Figure 2-16. Configuring the in-path interface



6. Type the IP address that you obtained from SCM. For details, see “To assign the in-path IP address and default gateway in SCM” on page 32.

7. Type the subnet mask address. The subnet mask on the in-path 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 obtained in SCM for the default gateway. For details, see “To assign the in-path IP address and default gateway in SCM” on page 32.

9. Click **Apply**.

10. You can refine your in-path WAN optimization settings using the SteelHead Management Console. For details, see the *SteelHead User Guide*.

Next steps

Connect to SCM and finish configuring the SD-WAN features for SteelHead SD. For details, see the *SteelHead SD User Guide* and *SteelConnect Manager User Guide*.

Troubleshooting

This section contains some basic troubleshooting procedures.

Can’t generate config error

Typically, this error occurs when assignments are missing for the appliance in SteelConnect. For example in SCM, make sure the uplinks are assigned and the ports are enabled for the appliance.

License server errors

If there is an error connecting to the license server or the license server returns an HTTP error status, make sure you have connectivity to the internet. If you have internet connectivity and automatic licensing continues to fail, go to the Riverbed Licensing Portal at https://licensing.riverbed.com/ and follow the instructions for retrieving your licenses.

The certificate from license server doesn’t match the private key

If an error is displayed stating that there is no valid certificate. This means that the appliance entitlement certificate is out of date and the certificate on the license server needs to be validated. Contact Riverbed Support at https://support.riverbed.com.

Firmware upgrade error

If you have multiple site level DNS addresses configured at the site level, the firmware download might fail on SteelHead SD appliances. We recommend that you have only one DNS IP address defined when you configure a site in SCM. A single-site level DNS configuration resolves both SCM and the upgrade image hostname. If you encounter this error, make these configuration changes in SCM and retry firmware upgrade. If the upgrade continues to fail, contact Riverbed Support at https://support.riverbed.com.

A

SteelHead SD Technical Specifications

This appendix describes the status lights, ports, and technical and environmental specifications for SteelHead SD 570-SD, 770-SD, and 3070-SD appliances. It includes these sections:

SteelHead SD 570-SD and 770-SD appliance specifications

This section describes the status lights, ports, and technical and environmental specifications.

Status lights and ports

Figure A-1. Front panel

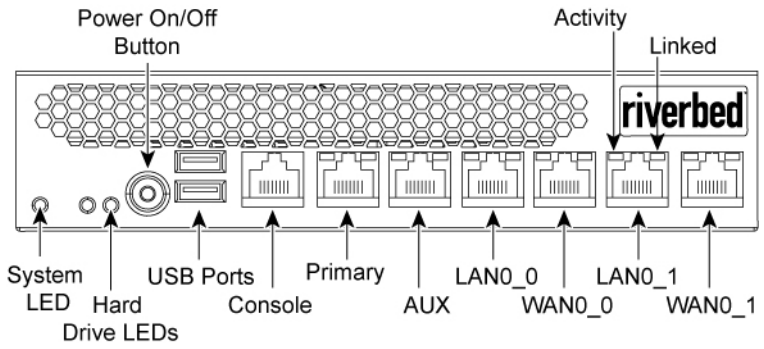
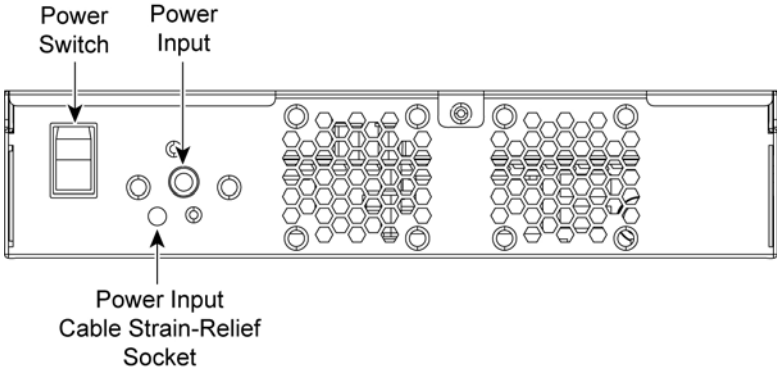


Figure A-2. Back panel



This table summarizes the system LEDs.

LED	Status
System	Healthy = Blue Degraded = Yellow Critical = Red Power Off = None
Power Button LED	System Off = No Light Standby Mode = Yellow Power On = Blue
Hard Drive LED	Activity = Blinks Blue Failed Disk = Orange
Primary LED	Left LED Link = Green Activity = Blinks Green Right LED GB = Yellow 100 MB = Green 10 MB = No Light (with link on left LED)
LAN/WAN LEDs	Left LED Link = Green Activity = Blinks Green Bypass/Disconnect = Yellow Right LED GB = Yellow 100 MB = Green 10 MB = No Light (with link on left LED)

Technical specifications

This table summarizes the technical specifications for the appliances.

Specification	570-SD desktop L-M-H	770-SD desktop L-M-H
Power (typical)	45 W	50 W
Volt-ampere (max)	63.8 VA	66.8 VA
BTU	145 BTU	165 BTU
Hard disk	1 x 320 GB 2.5” HDD 1 x 80 GB SSD	1 x 320 GB 2.5” HDD 1 x 160 GB SSD
RAM	8 GB	12 GB

Specification	570-SD desktop L-M-H	770-SD desktop L-M-H
Data store	70 GB SSD	150 GB SSD
Dimensions (LxWxH)	13 x 8 x 1.73 in. (330 x 204 x 44 mm)	13 x 8 x 1.73 in. (330 x 204 x 44 mm)
Weight (without packaging)	5.5 lb 2.4 kg	5.5 lb 2.4 kg
Voltage frequency	100-240 V 50-60 Hz	100-240 V 50-60 Hz
PSU	Single 84 W External 100-240 VAC, 50/60 Hz, 2-1 A	Single 84 W External 100-240 VAC, 50/60 Hz, 2-1 A
Included ports/max no. ports	4/4	4/4

Environmental specifications

This table summarizes the environmental requirements for the appliances.

Specification	570-SD desktop L-M-H	770-SD desktop L-M-H
Operating acoustic	45 dBA sound pressure (typical)	45 dBA sound pressure (typical)
Temperature (operating)	0º-45ºC 32º-113ºF	0º-45ºC 32º-113º F
Temperature (storage)	-40º- 65ºC -40º-149ºF	-40º- 65ºC -40º-149ºF
Relative humidity	20%-80% noncondensing	20%- 80% noncondensing
Storage humidity	5%-95% noncondensing	5%-95% noncondensing

SteelHead SD 3070-SD appliance specifications

This section describes the status lights, ports, and technical and environmental specifications. For details on NIC support, see “NIC support” on page 19 and the *Network and Storage Card Installation Guide*.

Status lights and ports

Figure A-3. SteelHead SD 3070-SD appliance front panel with LEDs and buttons

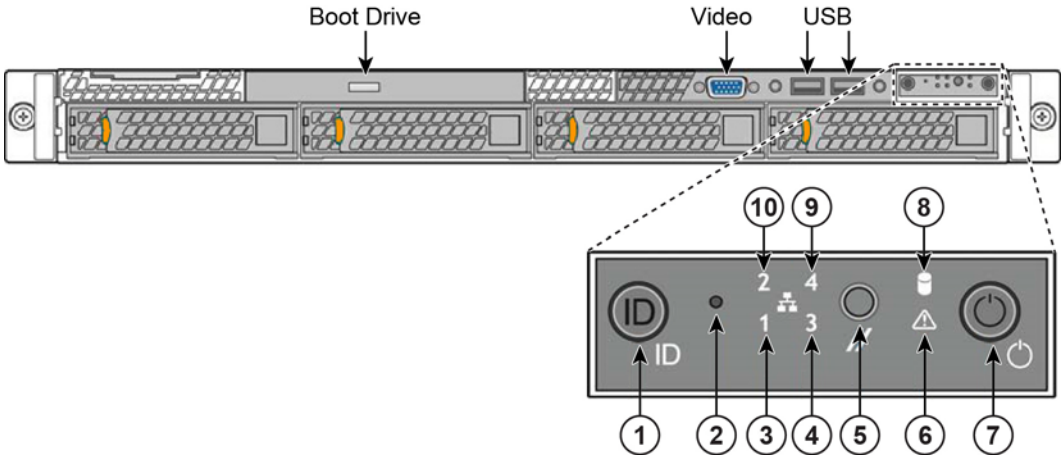
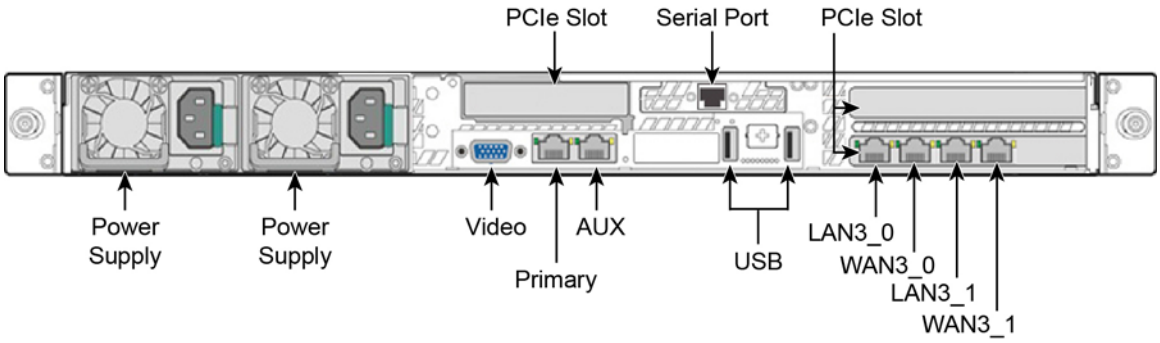


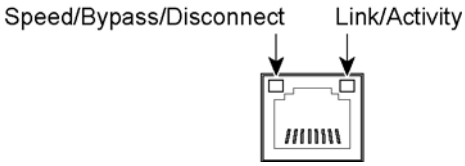
Figure A-4. SteelHead SD 3070-SD appliance back panel



Note: On the SteelHead SD 3070-SD appliance, the appliance uses the NIC in slot 3 for the default interface names so the ports are labeled WAN3_0 and WAN3_1. If you ordered a custom NIC instead of the default NIC for the appliance, then the NIC is installed in slot 2 and your NIC ports will appear in SCM as WAN2_0 and WAN2_1. The lowest WANX_X will be the default uplink.

This table summarizes the appliance LEDs and buttons.

Reference	LED/button	Description
1	System ID Button with Integrated LED	Maintenance = Blue Toggles the integrated ID LED and the blue server board ID LED on and off. The System ID LED identifies the system for maintenance when installed in a rack of similar server systems. You can also remotely turn on and turn off the System ID LED using the IPMI **chassis identify** command, which causes the LED to blink for 15 seconds. A duplicate System ID LED is on the back of the appliance to the left of the video port.
2	NMI Button	Pressing the NMI button puts the appliance in a halt state and issues a nonmaskable interrupt (NMI). This helps when performing diagnostics for a given issue where a memory download is necessary to determine the cause of the problem. To prevent an inadvertent system halt, the NMI button is located behind the front control panel faceplate and is only accessible with the use of a small-tipped tool such as a pin or paper clip.
3 10	Network Activity LED Primary Auxiliary	Link = Green Activity = Blinks Green. The blink rate is consistent with the amount of network activity. The appliance doesn't use the LEDs 4 and 9.
5	System Cold Reset Button	Pressing this button reboots the appliance.
6	System Status LED	The System Status LED shows the current health of the server system. Healthy = Green Degraded = Yellow Critical = Blinks Yellow A duplicate System ID LED is on the back of the appliance to the right of the AUX port.
7	Power Button with Integrated LED	System On = Green System Off = No Light
8	Drive Activity	Activity = Blinks Green
	LEDs on Disk Drives	**Activity LED** Read/Write Activity = Blinks Green **Disk Fault LED** Failed Disk = Orange RAID Rebuild = Blinks Orange
	LEDs on Primary and AUX Ports	**Left LED** Link = Green Activity = Blinks Green **Right LED** 10 MBps data rate = No Light (with link on left LED) 100 MBps data rate = Green 1000 MBps data rate = Yellow

Reference	LED/button	Description
	LEDs on Default 4-Port Copper Bypass Card	**Link/Activity LED** Link = Green Activity = Blinks Green **Speed/Bypass/Disconnect LED** 1000 Mbps = Yellow 100 Mbps = Green 10 Mbps = Off Bypass = Blinks Green Disconnect = Blinks Yellow 
	LEDs on Power Supply	Power on and healthy = Green Power off = Off Standby = Blinks Green Power lost but second power supply has power = Amber Power on with warning events (high temperature, high power, high current, slow fan) = Blinks Amber

Technical specifications

This table summarizes the technical specifications for the appliances.

Specification	Value
Form factor	1U
Hard disk	2 x 1000 GB, 2 SSD x 160
Data store	320 GB SSD
RAM	16 GB
Dimensions (LxWxH)	25.21 x 17.24 x 1.7 in. (640.4 x 438 x 43.2 mm)
Weight (without packaging)	27 lb (12.2 kg)
Voltage frequency	100-127 V, 200-240 V
PSU	2 x 450 W 100-127 VAC/8A, 50/60 Hz 200-240VAC/4A, 50/60 Hz
PCI-e expansion slots	2
Included ports/max no. ports	4/12

Power requirements and consumption

This table summarizes the power specifications for the appliances. The appliances are rated at the following power characteristics when operating at nominal AC input voltages (120 V and 230 V).

System	3070-SD	3070-SD
Configuration	All (L/M/H)	All (L/M/H)
PSU type	2 x 450 W	2 x 450 W
AC input	120 V	230 V
Max. amps	1.54 A	.76 A
Max. watts	152.8 W	145.4 W
Typical watts	122 W	116 W
Max. volt-ampere	154 VA	147 VA
Power factor	98.96 W/VA	99.16 W/VA
BTU (typical)	417 BTU	397 BTU

Environmental specifications

This table summarizes the environmental requirements for the appliances.

Specification	Environmental requirements
Operating acoustic	7.0 BA sound power (typical) 52 dBa sound pressure
Temperature (operating)	50°-95°F (10°-35°C)
Temperature (storage)	-40°-158°F (-40°-70°C)
Relative humidity	50% to 90%, noncondensing with a maximum wet bulb of 28°C (at temperatures from 25° to 35°C)

B

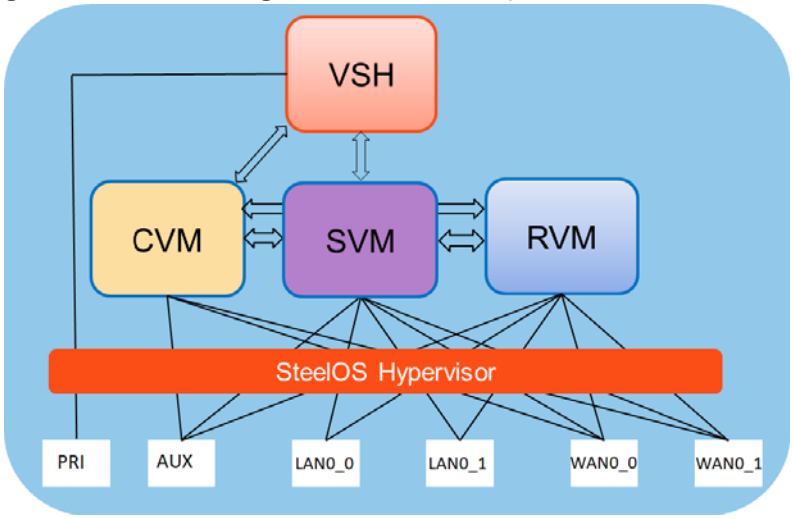
SteelHead SD Port Mappings

This chapter summarizes the port mappings for the SteelHead SD 570-SD, 770-SD, and 3070-SD appliances. It includes these sections:

Port mapping between the VMs and physical ports

The service virtual machine (SVM) and routing virtual machine (RVM) connect to all ports on the SteelHead SD appliance except for the primary (PRI) port. The primary port is connected directly to the virtual SteelHead (vSH). The controller virtual machine (CVM) is connected to the AUX port and the WAN uplinks only. For details on SteelHead SD architecture, see "Introducing SteelHead SD" on page 9.

Figure 2-17. Port mapping between VMs and physical ports



Note: The 3070-SD ports are LAN3_0, LAN3_1, WAN3_0, WAN3_1.

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:

```
XNXXXXD8XXXA9FF9-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

Source	Port name	IP address	Protocol	Remote end	Purpose
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_0, WAN3_1, 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, see “NIC support” on page 19.

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.

C

SteelConnect Connection Ports

This topic describes the ports used by SteelConnect for inbound, outbound and SSH connections.

Ports for UDP, TCP, and ICMP connections

SteelConnect appliances use these ports to establish connections.

Outbound connections

Service	Protocol	Default port	Destination
DNS - Gateways only	UDP/TCP	53	Any
NTP - Gateways only	UDP	123	Any
HTTP redirect for portal	TCP	80	Any
Uplink IP reflector	TCP	80	rfl.x.riverbed.cc
SteelConnect Manager/Core Server	TCP	443	core.riverbed.cc/ core.ocedo.cc
Portal	TCP	80/443	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
Configuration and API	TCP	3900	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
Tunneled SSH	TCP	3901	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
Reporting	TCP	3902	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
SD-WAN Controller	TCP	3904	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
Reporting	TCP	3905	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
Uplink Monitoring	ICMP		Any

Inbound/outbound connections

Service	Protocol	Default port	Destination
AutoVPN	UDP	500/4500	Any

Tunneled SSH client connections

Service	Protocol	Default port	Destination
Workstation	TCP	3903	<*myCC*>.riverbed.cc
SSH proxy	TCP	3903	<*myCC*>.riverbed.cc

Notes

<hostname> should be the same as what appears in the URL for SCM. For example, if your SCM is testcompany.riverbed.cc, then you would use testcompany for the <hostname>.

The API port is listed as port 3900. In most cases, it is 3900. This can be verified by performing a DNS query for _cc._tcp.<hostname>.riverbed.cc.

_cc._tcp.<hostname>.riverbed.cc SRV service location:

priority = 10

weight = 10

port = 3900

svr hostname = <hostname>.riverbed.cc

where port equals the port number that should be used for API port.

To configure VPN port numbers in the SCM, choose Network Design > Sites, select a particular site, and then select the WAN/AutoVPN tab. Under the AutoVPN Advanced Settings, change the AutoVPN Port to a different port number.

The HTTP redirect for Portal-TCP port 80 is required to allow the TCP three-way handshake to complete. After that has completed, the portal sends a redirect to the client. The client doesn't actually exchange any HTTP data with the external site. Additionally, it must be the MGMT zone IP address of the appliance in question that goes external. In the strictest sense, the source need not be all client IPs, but only the IPs of the Appliance MGMT zone IPs.