



SteelHead™ SD Installation Guide

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

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

Part Number
712-00302-02

Contents

Welcome	7
About this guide	7
Document conventions	7
Safety guidelines	7
Documentation and release notes	8
Contacting Riverbed	8
1 - SteelHead SD Overview	9
Introducing SteelHead SD	9
SteelHead SD software architecture	11
SteelHead SD port mapping between the VMs and physical ports	11
New features in SteelConnect 2.12	12
SaaS accelerator	12
Services hubs	12
Zscaler and Cloudi-Fi enhancements	13
Multisite administrator RBAC	13
Troubleshooting enhancements	13
Cold standby uplink support	14
Local IPFIX NetFlow export	14
Underlay and routing enhancements on SteelHead SD appliances	14
Static routing on SDI gateways and SteelHead SD appliances	15
Improved DHCP options on SteelHead SD appliances	15
LAN-side internet breakout on SteelHead SD appliances	15
Active-active HA improvements on SteelHead SD appliances	15
Routing features by model	17
Hardware and software requirements	18
Firewall requirements	18
Ethernet network compatibility	18
SNMP-based management compatibility	19
NIC support	19
Licensing	19
SteelConnect SD-WAN service licensing	20
SteelHead WAN optimization service licensing	20
Upgrading SteelHead SD	20

Upgrading from SteelHead SD 2.0 to SteelConnect 2.12	21
Upgrading from SteelHead SD 1.0 to SteelConnect 2.12	21
Preparing your site for installation.....	22
Before you begin	22
2 - Installing SteelHead SD	23
Configuring your network using SteelConnect Manager.....	23
Defining an organization	24
Adding sites	25
Changing the default zone in a site	25
Adding shadow appliances	27
Registering appliances	27
Configuring the primary and LAN ports in SCM	29
Assigning the in-path IP address and default gateway in SCM	31
Configuring SteelConnect to act as DHCP server	32
Cabling the SteelHead SD appliance.....	35
Port definitions	35
Cabling the SteelHead SD appliance	36
Enabling WAN optimization in SCM	37
Identifying the primary IP address of the SteelHead	38
Enabling WAN optimization on the virtual SteelHead instance	39
Configuring the in-path interface and default gateway	39
Next steps	41
Troubleshooting	41
Can't generate config error	41
License server errors	41
The certificate from license server doesn't match the private key	41
Firmware upgrade error	41
A - SteelHead SD Technical Specifications	43
SteelHead SD 570-SD and 770-SD appliance specifications.....	43
Status lights and ports.....	43
Technical specifications	44
Environmental specifications	45
SteelHead SD 3070-SD appliance specifications	45
Status lights and ports.....	46
Technical specifications	48
Power requirements and consumption	49
Environmental specifications	49
B - Port Mapping for SteelHead SD	51
SteelHead SD 570-SD and 770-SD appliances	51
Physical ports	51
CVM ports	51

Physical port to flows port mapping	51
Service chain virtual machines	51
vSwitch mapped VM ports	52
Bridged VM ports for internal communication.....	53
SteelHead SD 3070-SD appliance	53
Physical ports	53
CVM ports	53
Physical port to flows port mapping	53
SVM ports.....	53
RVM ports	54
vSH ports.....	54
C - SteelConnect Connection Ports.....	55
Ports for UDP, TCP, and ICMP connections.....	55
Outbound connections	55
Inbound/outbound connections.....	56
Tunneled SSH client connections	56

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-130, SDI-330, SDI-1030, and SDI-5030 and SDI-2030 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
<i>italics</i>	Within text, new terms and emphasized words appear in <i>italic</i> typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in bold typeface.
Courier	Code examples appear in Courier font: <pre>amnesiac > enable amnesiac # configure terminal</pre>
< >	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.

SteelHead SD Overview

This chapter provides an overview of the SteelHead SD architecture, new features, hardware and software requirements, licensing, and upgrading from SteelHead SD 1.0 or 2.0 to SteelConnect 2.12. It includes these sections:

- [“Introducing SteelHead SD” on page 9](#)
- [“SteelHead SD software architecture” on page 11](#)
- [“New features in SteelConnect 2.12” on page 12](#)
- [“Routing features by model” on page 17](#)
- [“Hardware and software requirements” on page 18](#)
- [“NIC support” on page 19](#)
- [“Licensing” on page 19](#)
- [“Upgrading SteelHead SD” on page 20](#)
- [“Preparing your site for installation” on page 22](#)
- [“Before you begin” on page 22](#)

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

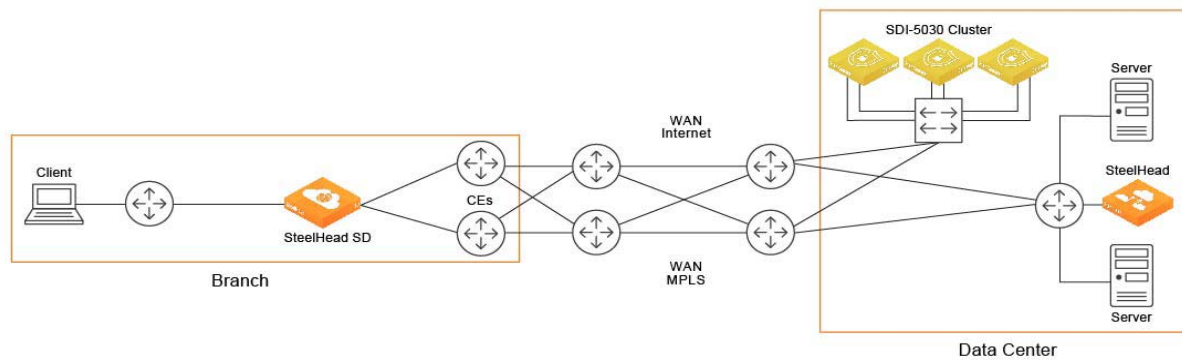
SteelHead SD combines SD-WAN and cloud networking capabilities (powered by SteelConnect) with Riverbed WAN optimization (powered by RiOS) into a single appliance. SteelHead SD seamlessly integrates advanced SD-WAN functionality with industry-leading WAN optimization, security, and visibility services 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-GbE data center gateway with active-active HA. The SteelConnect SDI-2030 gateway can also serve as a very large branch office appliance 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 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*.

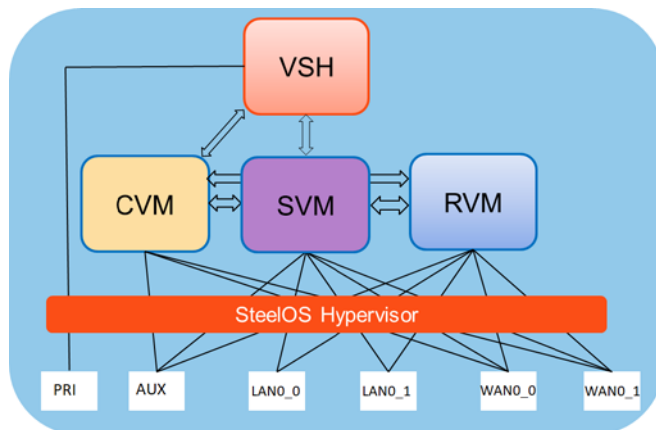
SteelHead SD port mapping between the VMs and physical ports

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. You can also configure a LAN-side standby uplink in case the AUX port goes down. For details, see the *SteelHead SD User Guide*.

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



New features in SteelConnect 2.12

SteelConnect 2.12 includes these new features:

SaaS accelerator

SteelHeads and SteelHead Mobile clients can accelerate SaaS traffic by working with SteelConnect. Using SCM, you can configure SaaS applications for acceleration, and then register SteelHeads or Mobile Controllers with SCM to accelerate their SaaS traffic. SCM 2.12 supports acceleration of these applications: Box, Microsoft Office 365 (including Exchange, SharePoint, Office WebApps, and Authentication and Identify Services), Salesforce, ServiceNow, and Veeva.

Services hubs

The services multihub feature has been enhanced to support up to three shared services hubs. A shared services hub can be a regional data center or an AWS/Azure cloud site that hosts services and applications. Leaf sites connect to a services hub using point-to-point AutoVPN tunnels enabling users at these leaf sites to access services hosted at the services hub locations. Shared services hubs support bidirectional connectivity between services hubs and leaf sites. Shared services hubs have these restrictions:

- Unlike regular hubs, shared services hubs do not support transit functions or leaf-to-leaf connectivity.

- Shared services hubs are supported on SDI-1030, SDI-2030, and SDI-5030 gateways; SDI-VGW virtual gateways, AWS Cloud gateways; and Azure Cloud gateways. (You cannot configure an SDI-130 or SDI-330 gateway or a SteelHead SD appliance as a hub device.)

Zscaler and Cloudi-Fi enhancements

SteelConnect 2.12 includes these Zscaler and Cloudi-Fi enhancements:

- Faster ZEN outage detection and quicker failover to backup ZEN nodes using enhanced monitoring of Zscaler tunnels. If the primary IPsec VPN tunnel or an intermediate connection goes down, all traffic is rerouted through the backup IPsec tunnel to a secondary ZEN in approximately 15 to 60 seconds, depending on the configuration and cause of failure.
- Internet Key Exchange (IKE) v2 support for enhanced security over all overlay tunnels including tunnels to Zscaler ZEN nodes.
- REST API integration that provides quicker Zscaler integration from SCM using the Zscaler partner APIs. Zscaler REST API integration delivers the ability to import ZEN nodes within SCM (Zscaler only).

Multisite administrator RBAC

Multisite administrator role-based access control (RBAC) enables you to create multiple administrator roles to manage a subset of sites within the organization. Site tags comprised of one or more sites are created and associated with an administrator role. A common use case for this feature enables enterprises to create administrators that are responsible for sites in a certain geographic region. Administrators manage sites and all SteelConnect constructs (that is, appliances, uplinks, zones, routes, rules, and features) for the sites within the scope of the site tags defined by region and associated with that administrator role. Multisite administrator RBAC isn't supported on SDI-5030 gateways.

Troubleshooting enhancements

- Improved tunnel details and status in SCM with better clarity. Support for extensions to tunnel visibility and overlay tunnel status. Tunnel reports have been unified:
 - Dashboard (duplex tunnel map view)
 - Health Check > Overlay Routes (by Site)
 - Health Check > Tunnel Health (by Tunnel)
 - Health Check > Proxy Tunnels (by Tunnel)
- System log improvements, including new log messages, log messages that are intuitive and understandable, and a central location for logs. In addition, the logs now list interface names, IP addresses, and time stamps. A subset of the system logs can be exported to the remote system log server to conserve space.
- New CLI framework, including:
 - **show** commands to aid in debugging issues and provide appliance information, including **show connections**, **show tunnels**, and **show flows**.

- a **show path** command that displays the potential paths for a given destination prefix. It also shows the current connections on the appliance using the paths. The show path tool is also available in SCM.
- a **configuration network** command for static IP network uplinks for situations when DHCP is not an option. (The appliance must be offline from SCM. This command is only supported when connected via telnet.)
- a **configuration core** command for the core hostname when the appliance is offline from SCM.
- a **troubleshoot** command that provides for enhanced day zero troubleshooting that includes all interfaces reachable through the SCM. This command provides connectivity information about the core or SCM on all physical ports on the appliance. You can export the output as log files via a USB drive, create log files with a specific name, and list all log files.
- support for system dumps. By default, when you request a system dump, it is uploaded to riverbed.support.com. You can also specify an external server for uploads in SCM under the Organization > System Dump tab.
- support for the tcpdump utility.
- support package enhancements so that you can gather the data needed when an issue is encountered, including cluster details.

Cold standby uplink support

In SteelConnect 2.12, you can enable an uplink to act as a backup uplink that assumes the active role if no other uplinks are available. The local and remote backup uplink tunnels are not probed unless their corresponding active uplinks are down. The local and remote backup uplinks for overlay or underlay data traffic are not used unless their corresponding active uplinks are down. The cold standby uplink is supported on SDI-130, SDI-330, SDI-1030, and SDI-2030 gateways; the SDI-VGW virtual gateway; and the SteelHead SD 570-SD, 770-SD, and 3070-SD appliances. (The SDI-5030 data center uplinks are always active by design.)

Local IPFIX NetFlow export

With SteelConnect 2.12, IP Flow Information Export (IPFIX) NetFlow records can be directly exported to NetProfiler or any third-party flow collectors. IPFIX NetFlow exports use standard UDP protocol format. NetFlow exports are supported on both LAN and WAN interfaces and reports both overlay and underlay traffic on the interface. In addition, you can configure NetFlow exports and SNMP integration on a collector for advanced visibility. IPFIX NetFlow export is supported on SDI-130, SDI-330, SDI-1030, and SDI-2030 gateways; the SDI-VGW virtual gateway; and the SteelHead SD 570-SD, 770-SD, and 3070-SD appliances.

Underlay and routing enhancements on SteelHead SD appliances

SteelConnect 2.12 provides these underlay and routing enhancements on SteelHead SD 570-SD, 770-SD, and 3070-SD appliances, and the SDI-2030 gateway located at the branch):

- **OSPF routing** - With SteelConnect 2.12, you can distinguish between static and overlay routes for OSPF. This distinction enables you to configure redistribution policies separately for each type of route. For overlay OSPF routes, you can associate a site with the route redistribution policy which enables you to redistribute it based on the sites from which they were reported.
- **Loop prevention in subnet autodiscovery** - You can enable discovery of subnets based on the tag/community lists present in the route to prevent loops. All routes matching the tag/community lists are reported as local subnets of the configured site. Tag and community lists can be configured in inclusion or exclusion lists.
- **Soft reset for BGP parameters** - Soft refresh enables route updates without tearing down existing peering sessions. A soft reset uses stored update information to allow you to apply new BGP policy without disrupting the network.
- **User-defined route maps for increased flexibility** - Support for user-defined route maps enables you to create route maps that include all available match and set criteria options.
- **Increased BGP route preference support** - You can now set BGP local preference, Multi-Exit Discriminator (MED) options, the origin type in route maps, metric distance, and next-hop self.
- **Differentiation between static and overlay BGP routes** - You can differentiate between static and overlay routes when you configure the Overlay to BGP option. The policies applied on redistribution of other routes are also applicable on overlay routes.
- **Routing table search** - Ability to search the routing tables for an appliance by serial number or for appliances by site name.

Static routing on SDI gateways and SteelHead SD appliances

With SteelConnect 2.12, you can configure static routing on SDI gateways in addition to SteelHead SD appliances. Static routes support IPv4 destination networks. You can also configure the distance metric which prioritizes the routing protocol when two routes have the same route destination.

Improved DHCP options on SteelHead SD appliances

The zone DHCP tab enables you to configure LAN clients with DNS servers located on internet (outside of the intranet) on guest zones. The zone DHCP tab also allows you to configure LAN clients with Preboot Execution Environment (PXE) boot using the Trivial File Transfer Protocol (TFTP), a Session Initiation Protocol (SIP) server, or an HTTP proxy.

LAN-side internet breakout on SteelHead SD appliances

The LAN-side internet breakout capability enables redirection of backhauled internet traffic to break out from the LAN-side of the gateway. Previous releases only allowed internet breakout over the WAN uplinks.

Active-active HA improvements on SteelHead SD appliances

SteelConnect 2.12 provides these high-availability (HA) enhancements:

- You can configure a 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.
- There is a new configuration option to specify the SteelHead SD appliance as the master appliance.
- Support is now available for SteelHead SD *mixed-mode* HA, where one SteelHead SD appliance is licensed as SD-WAN-only and the peer SteelHead SD appliance is licensed for SD-WAN and WAN optimization.

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>
SteelHead Management Console	<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>You use the SteelHead Management Console to manage WAN optimization features on vSH instances.</p> <p>JavaScript and cookies must be enabled in your web browser.</p>
SteelConnect and SteelConnect Manager (SCM)	<p>SteelHead SD requires SteelConnect 2.11 or later.</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)	We recommend that SCC 9.9 is installed.

Firewall requirements

The SteelHead SD 570-SD, 770-SD, and 3070-SD appliances, and SDI-2030 gateways located at the branch 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 [Appendix C, "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

Ethernet standard	IEEE standard
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 is supported on the SteelConnect SDI-130, SDI-330, SDI-1030, SDI-5030, and SDI-VGW virtual gateways. SNMPv1, 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, and SD-3070 appliances, and SteelConnect SDI-2030 gateway 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*.

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 because 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

SteelConnect 2.12 requires a WAN optimization subscription license if you want to use the WAN service. The WAN optimization subscription license is an optional purchase.

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 SteelHead SD

This section describes how to upgrade SteelHead SD. It includes these topics:

- [“Upgrading from SteelHead SD 2.0 to SteelConnect 2.12” on page 21](#)
- [“Upgrading from SteelHead SD 1.0 to SteelConnect 2.12” on page 21](#)

Upgrading from SteelHead SD 2.0 to SteelConnect 2.12

SteelHead SD features require the virtual SteelHead (vSH) image, which is contained within the SteelConnect 2.12 image. All SteelHead SD 2.0 customers will be automatically upgraded to SteelConnect 2.12. SteelConnect automatically upgrades to 2.12 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*.

If you need to upgrade the SteelHead appliances in your deployment, see the *SteelCentral Controller for SteelHead Installation Guide* and the *SteelHead Installation and Configuration Guide*.

Upgrading from SteelHead SD 1.0 to SteelConnect 2.12

SteelHead SD features require the virtual SteelHead (vSH) image, which is contained within the SteelConnect 2.12 image. All SteelHead SD 1.0 and 2.0 customers will be automatically upgraded to SteelConnect 2.12. SteelConnect automatically upgrades to 2.12 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 SteelConnect 2.12 upgrade process:

- SteelHead SD 1.0 supported an active-passive HA scheme. Because SteelConnect 2.12 supports active-active HA, you can't upgrade your SteelHead SD 1.0 HA seamlessly to SteelConnect 2.12 HA. You must first manually unpair your master and backup appliances in SCM, upgrade to SteelConnect 2.12, 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 SteelConnect 2.12. 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 SteelConnect 2.12, 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 2.12 upgrade process.
- SteelConnect 2.12 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 SteelConnect 2.12 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 SteelConnect 2.12. 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 SteelConnect 2.12. The AUX port is mandatory for back-to-back connectivity for SteelConnect 2.12 HA deployments.
- If you need to upgrade the SteelHead appliances in your deployment, see the *SteelCentral Controller for SteelHead Installation Guide* and the *SteelHead Installation and Configuration 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.

Installing SteelHead SD

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

- [“Configuring your network using SteelConnect Manager” on page 23](#)
- [“Cabling the SteelHead SD appliance” on page 35](#)
- [“Enabling WAN optimization in SCM” on page 37](#)
- [“Enabling WAN optimization on the virtual SteelHead instance” on page 39](#)
- [“Next steps” on page 41](#)
- [“Troubleshooting” on page 41](#)

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*.

Configuring your network using SteelConnect Manager

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.

This section describes how to configure a basic network with a single company headquarters. You’ll define an organization, establish network zones (including a guest zone), add users, and then deploy into the SteelHead SD appliance into the sites. You design first and deploy the hardware last. This section includes these tasks:

- [“Defining an organization” on page 24](#)
- [“Adding sites” on page 25](#)
- [“Changing the default zone in a site” on page 25](#)
- [“Adding shadow appliances” on page 27](#)
- [“Registering appliances” on page 27](#)
- [“Configuring the primary and LAN ports in SCM” on page 29](#)
- [“Assigning the in-path IP address and default gateway in SCM” on page 31](#)
- [“Configuring SteelConnect to act as DHCP server” on page 32](#)

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. When you create a site, the zone is automatically created and an uplink is automatically created for the internet path.
- **Zone** - Zones are at the center of an SD-WAN network. Layer 2 network segments or VLANs within sites that are VLAN-tagged traffic. A zone always has a VLAN tag assigned to it. Every site has at least one zone and can have multiple zones. When you create a site, SteelConnect automatically adds a default zone.

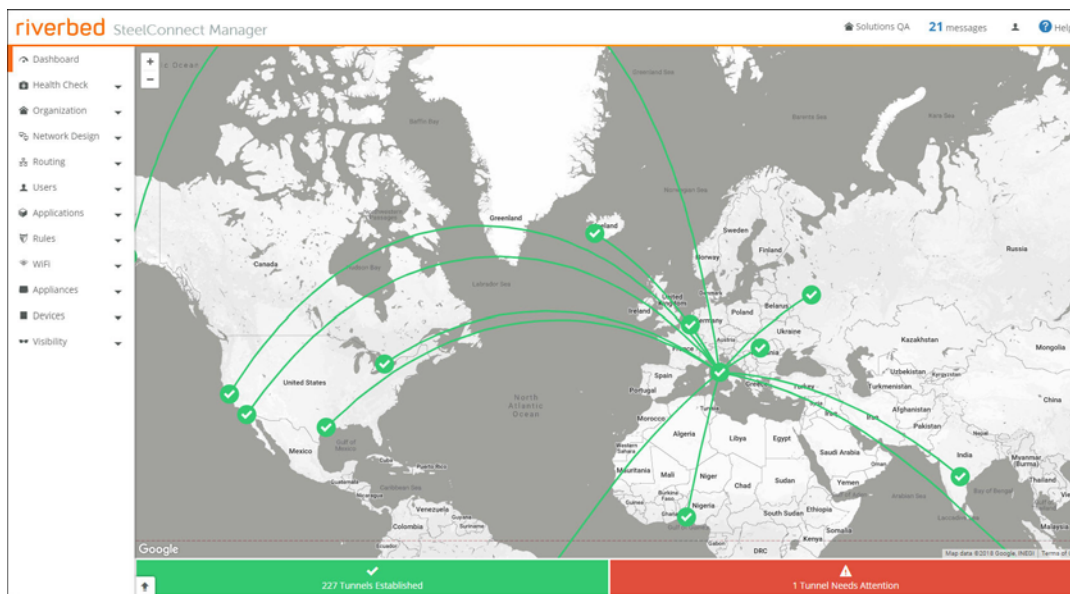
SCM is delivered with a default organization and site. You add your company name and basic information for your organization or change and customize this information later. For details about defining an organization, network, sites, zones, and uplinks, see the *SteelConnect Manager User Guide*.

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**.

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.

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. Specify the site’s address, country, and time zone. Make sure the time zone matches the site’s location.
6. Click **Submit**.

After you create the site, it appears on the dashboard map. Repeat [Step 2](#) through [Step 6](#) to add additional sites.

A default 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 “Designing a Network,” in the *SteelConnect Manager User Guide*.

Changing the default zone in a site

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.

Note: While creating or modifying a zone, don't specify the same subnet in more than one zone when dynamic routing (BGP or OSPF) is enabled. Dynamic routing doesn't support duplicate subnets for multiple zones.

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 network topology.

In this tutorial, you want this zone to be part of the VPN and to automatically connect your VPN connection using automated VPN.

Regular zones are always part of RouteVPN by default.

4. Click **Submit**.

The LAN zone is complete.

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

Next, you'll create a new zone for guests. Within the guest zone, you can determine how guests can register their devices: using their mobile phone number (SMS), email address, or social media applications (Facebook, Twitter, Google).

Note: Guest zones are only allowed to send traffic over to the internet.

After you create a guest zone you can't change it to a standard zone.

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

To create a guest zone

1. Return to the Zones page and click **New Zone**.
2. Select the site from the drop-down list.
3. Type *Guest* to describe the zone.
4. Under guest zone, click **On** to add some extra intraclient security and isolate the guests from each other.
5. Optionally, specify the IPv4 network using a.b.c.d/nm 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**.

You can add additional zones to a site, if necessary. For details on creating 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**.
3. Select Create Shadow Appliance.
4. Select 570-SD, 770-SD, or 3070-SD from the model drop-down list.
5. Select the site where you want to deploy the shadow appliance from the site drop-down list.
6. Click **Submit**.
7. 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 SteelHead SD appliances to transform them from shadow appliances to physical appliances.

8. Choose Network Design > Uplinks to see that SCM has automatically assigned uplinks to the new gateways. 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*.

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

Register Hardware Appliance

Appliance serial # Enter serial #

Deploy into site >> Do not deploy into a site yet <<

Cancel Submit

4. Type the SteelConnect serial number. Make sure you use the SteelConnect gateway serial number that begins with XN.
5. Click **Submit**.
6. Repeat these 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 enables your settings on the appliance.

This automatic provisioning makes the appliances easily replaceable, if necessary.

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*.

A complete mesh overlay connects across all sites and shares all networks that are involved with RouteVPN using full permissions.

The last task is to cable the physical appliances, using the first WAN port for the internet. After powering on the appliances, each appliance will download the latest 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.

After AutoVPN establishes the tunnels, you can view the dashboard map to see a visible representation of the network. Each tunnel on the dashboard represents both directions. Click a site marker to verify that the locations are completely connected with a full-mesh VPN. SCM displays the established connections as green lines between the sites. The lines change to red if the tunnel switches to offline.

For troubleshooting, see "Provisioning" in the *SteelConnect Manager User Guide*.

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

The screenshot shows the 'PRIMARY' port configuration window in SteelConnect Manager. The window has a title bar with a close button (X) and a tabbed interface with 'Info / Mode', 'MACs / Devices', and 'Counters'. The 'Info / Mode' tab is active, showing two main sections: 'Info' and 'Mode'.

Info Section:

- Port Label:** PRIMARY
- Link Status:** up 100M
- STP Status:** Unknown
- Site:** Branch10
- Appliance:** Branch10 > 570-SD [sv-cf1-beta]
- Type:** Discrete
- MAC:** 00:0E:B6:6A:8F:60
- LLDP Remote:** Unknown
- RX Bytes:** ...
- RX Packets:** ...
- RX Errors:** ...
- TX Bytes:** ...
- TX Packets:** ...
- TX Errors:** ...

Mode Section:

- Port mode:** SteelHead Primary (dropdown menu)
- Buttons:** Cancel, Submit

Port Description Section:

- Port description:** Port description (limit 16 characters) (text input field)

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

LAN0_0

Info / Mode | MACs / Devices | Counters

Info

Port label LAN0_0

Link status Up 1G

STP status Unknown

Site Branch10

Appliance Branch10

 > 570-SD [sv-cf1-beta]

Type Discrete

MAC 00:0E:B6:C1:D5:AF

LLDP remote Unknown

RX bytes 207843427 ~ 198M ⬆ +166k

RX packets 3196714 ~ 3121k ⬆ +2k

RX errors ...

TX bytes 1990

TX packets 21

TX errors ...

Mode

Port mode i Singlezone

Zone i • Nothing selected

Cancel Submit

Port Description

Port description i Port description (limit 16 chara

8. Select Singlezone for the Port mode.
9. Select the zone from the drop-down list.
10. Optionally, provide a description of the port.
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

The screenshot shows the SteelConnect Manager interface for a zone named 'Branch10_1100'. The 'IP' tab is active, displaying the 'IPv4 network and gateway' configuration. The 'IPv4 Network' field contains '172.16.20.0/24' and the 'IPv4 Gateway' field contains '172.16.20.2'. Below this, the 'IPv6 status, network, and gateway' section shows a toggle for 'Use IPv6' set to 'Off'. The interface includes a top navigation bar with tabs for IP, Gateways, DHCP, VLAN, WAN, Settings, ADDL Networks, and Discovered Networks. There are also 'Cancel' and 'Submit' buttons at the bottom right of the configuration area.

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, its primary interface tries 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

Branch10_1101 Actions X

IP **Gateways** DHCP VLAN WAN Settings ADDL Networks Discovered Networks

Automatic SteelConnect default gateway

When turning this option on, a SteelConnect gateway appliance deployed in the site will be automatically configured as the default gateway for this zone. It will then **use the default gateway IP addresses specified on the 'IP' tab**. If you want to control all gateway assignments for this zone manually, or you want to use a third-party default gateway for this zone, please turn this option off.

Default Gateway configuration Automatic **Manual**

Gateway assignments

This table shows all SteelConnect gateways that are members of this zone. You can create several memberships, also in remote sites. Every member gateway will be able to route into the zone's network. Default gateway entries that have been added automatically cannot be edited or deleted - if you want to control all gateway parameters, turn off automatic default gateway assignment and create a default gateway manually.

[+ Add assignment](#)

Type / Appliance	IPs	Flags	
Default Gateway Branch10 > 570-SD [sv-cf1-beta]	172.16.20.2 fd00:ced0:ced0:c::1	DHCP/RA	Edit Delete

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 SteelHead SD 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	<p>The primary port is the management interface that enables you to connect to the SteelHead Management Console.</p> <p>Preferably the primary port connects to a DHCP reachable port on a switch.</p> <p>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.</p>
AUX	<p>The AUX port can be used as an additional WAN uplink on SteelHead SD. A SteelHead SD appliance with WAN optimization enabled has a virtual SteelHead instance running inside the SteelHead SD appliance. Any traffic that is optimized is sent out through any of the WAN interfaces, including the AUX interface, if it has been configured for that purpose.</p> <p>The AUX port is also the dedicated port for SteelHead SD HA deployments. 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.</p> <p>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.</p>

Port	Description
WANX_X	<p>WAN ports function as uplinks for internet service providers that connect to the internet.</p> <p>Connect the WAN port to a WAN router using a straight-through cable.</p> <p>For SteelHead SD 570-SD and 770-SD appliances, the default internet access port is WAN0_0 or WAN0_1.</p> <p>For SteelHead SD 3070-SD appliances, the default internet access port is WAN3_0 or WAN3_1.</p>
LANX_X	<p>Connect the LAN port to the LAN switch using a straight-through cable.</p> <p>For SteelHead SD 570-SD and 770-SD appliances, the default port is LAN0_0 and LAN0_1.</p> <p>For SteelHead SD 3070-SD appliances, the default port is LAN3_0 or LAN3_1.</p>
Console	<p>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.</p>

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

The screenshot shows the configuration page for a SteelHead-SD appliance. At the top, there's a header with the appliance name '570-SD' and an 'Actions' dropdown. Below this is a navigation bar with tabs: Live, IPs, AutoVPN, HA, Routing, BGP, **Services**, and Location. The 'Services' tab is selected and highlighted. The main section is titled 'WAN Optimization Service'. It contains a paragraph explaining that the service is disabled by default and that enabling it will disrupt network connectivity. Below this is a note about attaching zones to physical ports. The configuration fields include: 'WAN Optimization Service' with a toggle set to 'Enabled' (green button), 'SteelHead Zone' with a dropdown menu showing 'Branch10 -> Branch10_1100 [1100]', and 'SteelHead Inpath IP Address' with a text input field containing '172.16.20.22'. At the bottom right are 'Cancel' and 'Submit' buttons.

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 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 32](#).
- **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 address bar 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

The screenshot shows the 'In-Path Interfaces' page. At the top, there's a breadcrumb trail: 'Networking > In-Path Interfaces'. Below this is a section titled 'In-Path Settings' with a checkbox labeled 'Enable Link State Propagation'. A dark blue 'Apply' button is located below the settings. The main part of the page is a table titled 'In-Path Interface Settings:'.

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

5. Select the interface to expand the page.

Figure 2-16. Configuring the in-path interface

The screenshot shows the 'In-Path Interface Settings' page for the 'inpath0_0' interface. The interface is expanded, showing various configuration options. The 'Interface' section is highlighted.

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

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 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 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 the firmware upgrade. If the upgrade continues to fail, contact Riverbed Support at <https://support.riverbed.com>.

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” on page 43
- “SteelHead SD 3070-SD appliance specifications” on page 45

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

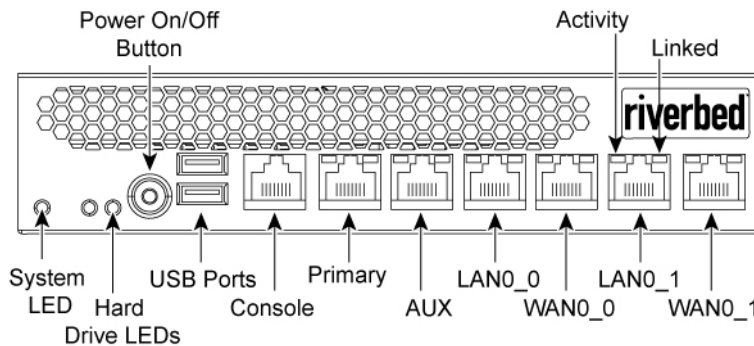
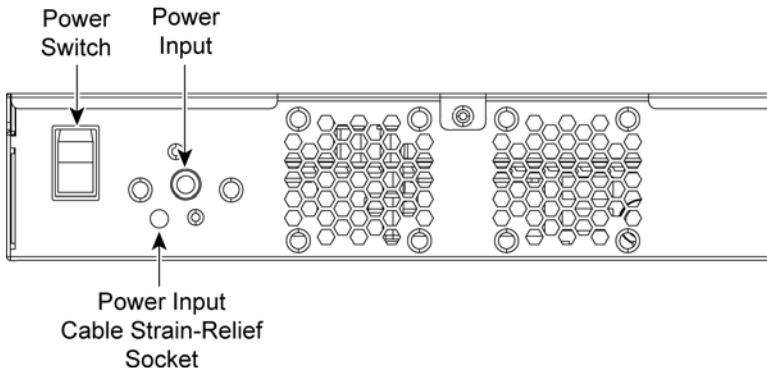


Figure A-2. Back panel



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
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)

Specification	570-SD desktop L-M-H	770-SD desktop L-M-H
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)	0°-45°C 32°-113°F	0°-45°C 32°-113°F
Temperature (storage)	-40° - 65°C -40°-149°F	-40° - 65°C -40°-149°F
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.

Status lights and ports

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

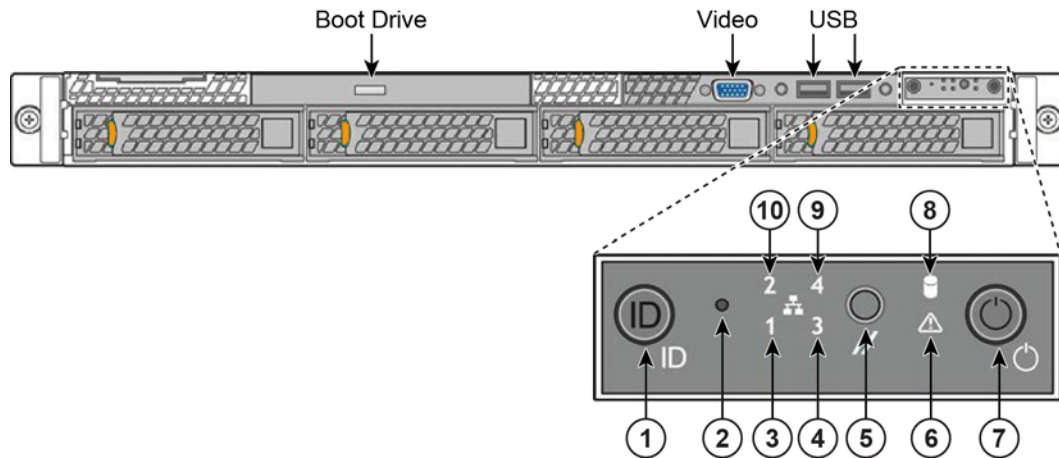
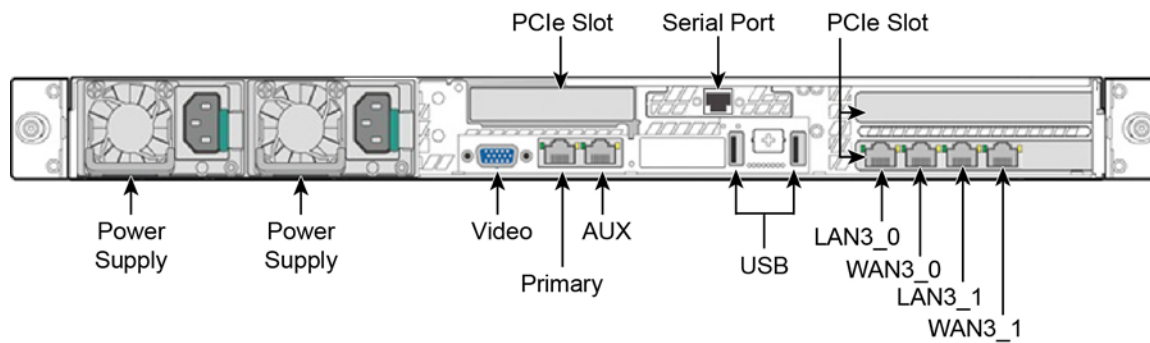


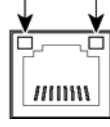
Figure A-4. SteelHead SD 3070-SD appliance back panel



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	<p>Maintenance = Blue</p> <p>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.</p> <p>A duplicate System ID LED is on the back of the appliance to the left of the video port.</p>
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	<p>Link = Green</p> <p>Activity = Blinks green. The blink rate is consistent with the amount of network activity.</p> <p>The appliance doesn't use LEDs 4 and 9.</p>
5	System Cold Reset Button	Pressing this button reboots the appliance.
6	System Status LED	<p>The System Status LED shows the current health of the server system.</p> <p>Healthy = Green</p> <p>Degraded = Yellow</p> <p>Critical = Blinks yellow</p> <p>A duplicate System ID LED is on the back of the appliance to the right of the AUX port.</p>
7	Power Button with Integrated LED	<p>System On = Green</p> <p>System Off = No light</p>
8	Drive Activity	Activity = Blinks green
	LEDs on Disk Drives	<p>Activity LED</p> <p>Read/Write Activity = Blinks green</p> <p>Disk Fault LED</p> <p>Failed Disk = Orange</p> <p>RAID Rebuild = Blinks orange</p>
	LEDs on Primary and AUX Ports	<p>Left LED</p> <p>Link = Green</p> <p>Activity = Blinks green</p> <p>Right LED</p> <p>10 Mbps data rate = No light (with link on left LED)</p> <p>100 MBps data rate = Green</p> <p>1000 MBps data rate = Yellow</p>

Reference	LED/Button	Description
	LEDs on Default 4-Port Copper Bypass Card	<p>Link/Activity LED Link = Green Activity = Blinks green</p> <p>Speed/Bypass/Disconnect LED 1000 Mbps = Yellow 100 Mbps = Green 10 Mbps = Off Bypass = Blinks green Disconnect = Blinks yellow</p> <p>Speed/Bypass/Disconnect Link/Activity</p> 
	LEDs on Power Supply	<p>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</p>

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 200-240 VAC/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)

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 51](#)
- [“SteelHead SD 3070-SD appliance” on page 53](#)

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 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.



SteelConnect Connection Ports

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

Ports for UDP, TCP, and ICMP connections

SteelConnect uses 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>.ocado.cc
Configuration and API	TCP	3900	<hostname>.riverbed.cc -or- <hostname>.ocado.cc
Tunneled SSH	TCP	3901	<hostname>.riverbed.cc -or- <hostname>.ocado.cc
Reporting	TCP	3902	<hostname>.riverbed.cc -or- <hostname>.ocado.cc
SD-WAN Controller	TCP	3904	<hostname>.riverbed.cc -or- <hostname>.ocado.cc
Reporting	TCP	3905	<hostname>.riverbed.cc -or- <hostname>.ocado.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