riverbed®

SteelHead™ SD In-Field Upgrade Guide

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

Version SteelHead SD 2.0, SteelConnect 2.11

August 2018

riverbed®

Contents

Contents

Welcome

Welcome to the *SteelHead SD In-Field Upgrade Guide*. This guide describes how to upgrade a SteelHead CX570, CX770, or CX3070 appliance to a SteelHead SD 570-SD, 770-SD, or 3070-SD appliance.

Before you begin, make sure you familiarize yourself with the:

- *SteelHead SD Installation Guide*
- *SteelHead SD User Guide*
- *SteelConnect Manager User Guide*

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

This guide includes information relevant to these products and product features:

- Riverbed SteelHead SD (SteelHead SD)
- Riverbed SteelHead (SteelHead)
- Riverbed SteelConnect (SteelConnect)
- SteelConnect Manager (SCM)
- Steel Operating System (SteelOS)
- Riverbed Optimization System (RiOS)
- Riverbed command-line interface (CLI)

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>]**

Convention	Meaning
{}	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 https://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, interface behavior, feature changes and compatibility, and hardware and software requirements. It includes these sections:

- "Introducing SteelHead SD" on page 11
- "SteelHead SD software architecture" on page 13
- "Transforming your SteelHead network" on page 14
- "SteelHead features unchanged after upgrading to SteelHead SD" on page 15
- "SteelHead features changed after upgrading to SteelHead SD" on page 16
- "Interface behavior before and after upgrading" on page 19
- "SteelHead SD and SteelConnect feature compatibility by model" on page 20
- "Hardware and software requirements" on page 22
- "NIC support" on page 23
- "Before you begin" on page 24

This guide describes how to perform an in-field upgrade on a SteelHead CX570, CX770, or CX3070 appliance to a SteelHead SD 570-SD, 770-SD, or 3070-SD appliance. It doesn't provide detailed information about configuring and managing SD-WAN or WAN optimization features. For details, see the *SteelConnect Manager User Guide*, *SteelHead SD User Guide*, and *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
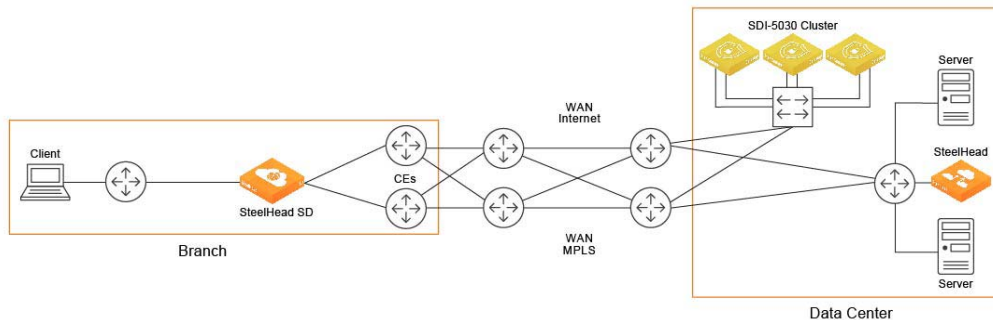
SteelHead SD supports these configurations:

- **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 on configuring WAN optimization features, see the *SteelCentral Controller for SteelHead User Guide* and the *SteelHead User Guide*.

- **SD-WAN only** - In this configuration, WAN optimization 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 on 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 software 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 that 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.

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 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
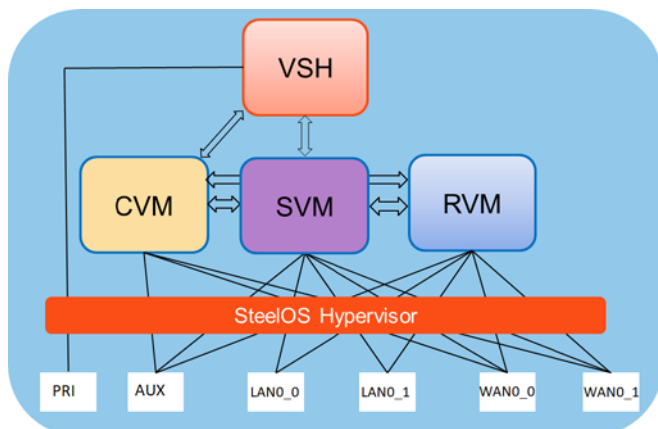
Transforming your SteelHead network

Although SteelHead and SteelHead SD share the same hardware, they run different software and serve very different purposes.

To illustrate these differences, examine this table.

	SteelHead CX3070	**SteelHead SD 3070-SD**
Software	RiOS	SteelOS
Network device type	Layer 2	Layer 3
Purpose	WAN optimization	SD-WAN and, optionally, WAN optimization
Icon		

An in-field upgrade of the SteelHead CX appliance is much more than a simple upgrade; it requires a transformation of the SteelHead appliance from a Layer 2 WAN optimization device to a Layer 3 edge router.

Before you begin the upgrade process, it is important to determine what kind of network topology you have and how it will change when you convert to SteelHead SD. The conversion process requires that you transform your network where the SteelHead SD appliance acts as an SD-WAN device using Layer 3 networking protocols and that also performs WAN optimization.

Figure 1-4. Transforming a SteelHead deployment

It is imperative that you plan your network architecture and deployment. You will have to rearchitect the network WAN, Layer 3 hops with the gateway, WAN uplinks, SD-WAN features, SCM cloud management, and high availability (HA).

We recommend that you contact Riverbed sales engineering before you begin the in-field upgrade process so that they can assist you with designing and deploying your SD-WAN network.

SteelHead features unchanged after upgrading to SteelHead SD

The majority of SteelHead features remain unchanged when you upgrade to SteelHead SD.

SteelHead feature	Feature after upgrading to SteelHead SD
Layer 7 optimization blades	All Layer 7 SteelHead optimization blades are supported. For example, HTTP, SSL, CIFS/SMB, MAPI, Oracle Forms, NFS, Lotus Notes, and storage replication (for example, SnapMirror) all operate normally and are unchanged.
	The Citrix optimization blade is supported but the ability to support the optimization of Multi-Stream ICA within the blade is no longer possible because the QoS functionality is taken care of by the service virtual machine (SVM) in SteelHead SD.
	You cannot optimize UDP traffic using the SteelHead IP blade as traffic is not redirected through the virtual SteelHead.
SteelHead SaaS and the new SaaS Accelerator	SteelHead SD 2.0 supports SteelHead SaaS and the SaaS Accelerator. The SaaS Accelerator is not available on SteelConnect 2.11 gateways.
Web proxy	SteelHead SD supports SteelHead Web proxy.
CIFS prepopulation	SteelHead SD supports SteelHead CIFS prepopulation.
Active Directory integration	SteelHead SD supports SteelHead Active Directory integration. Because the virtual SteelHead instance has full control of the primary interface, it supports Active Directory integration and server-side out-of-path deployments.
Data store synchronization	SteelHead SD supports SteelHead data store synchronization on the primary interface with an adjacent SteelHead appliance.

SteelHead feature	Feature after upgrading to SteelHead SD
Caching DNS service	SteelHead SD supports the SteelHead caching DNS service. With the caching DNS service, because the AUX port isn't available to the virtual SteelHead, caching DNS is limited to the primary interface only.
Transport performance features	SteelHead SD supports SteelHead high speed TCP and bandwidth estimation, satellite features such as SCPS, and single-ended connections.
Management, reporting, and diagnostics	SteelHead SD supports SteelHead domain, host, and port labels, as well as in-path and peering rules.
Secure vault	SteelHead SD supports SteelHead secure vault. The secure vault password is retained when you upgrade from SteelHead to SteelHead SD.
Management access controls	SteelHead SD supports SteelHead management access controls including Radius and TACACS, and role-based access.
TCP dump export	SteelHead SD supports SteelHead export of TCP dumps.

SteelHead features changed after upgrading to SteelHead SD

This table summarizes the features that have changed after converting to SteelHead SD.

SteelHead feature	Feature after upgrading to SteelHead SD
WAN-optimization only mode	WAN-optimization only mode is not supported on SteelHead SD.
Hybrid networking services (path selection, secure transport, QoS)	Hybrid networking services (path selection, secure transport, QoS) are not supported on SteelHead SD. The network services of QoS, path selection and secure transport replaced by SteelConnect SD-WAN counterparts. Any QoS feature configuration on the original SteelHead must be converted to the new QoS in SCM. MX-TCP, because it was part of QoS, is not supported on SteelHead SD. Citrix Multistream ICA is not supported on SteelHead SD.
Multiple in-path interfaces for WAN optimization	SteelHead SD does not support multiple in-path interfaces for WAN optimization. Given that SteelHead SD is a Layer 3 gateway, multiple LAN ports and segments can be mapped to a single in-path interface. There is no longer a need for multiple in-path interfaces on an SteelHead SD appliance. After upgrading from SteelHead to SteelHead SD you must reconfigure your multiple in-path interfaces to a single in-path configuration.
Virtual in-path or WCCP/PBR	Virtual in-path or WCCP/PBR is not supported on SteelHead SD. The concept of virtual in-path is not relevant for the WAN optimization of SteelHead SD. Thus, there is no need for WCCP or PBR.
Simplified Routing and VLAN transparency	Simplified Routing and VLAN transparency is not supported on SteelHead SD. Because the in-path interface on the virtual SteelHead instance within SteelHead SD doesn't sit physically in-path on the network, there is no need for Simplified Routing or VLAN transparency.
IPSec, subnet side rules, MXTCP and link state propagation	IPSec, subnet side rules, MXTCP and link state propagation are not supported on SteelHead SD.

SteelHead feature	Feature after upgrading to SteelHead SD
Serial high availability (HA)	After upgrading, serial HA is not supported on SteelHead SD 2.0. SteelHead appliances in an HA pair must be individually shut down and upgraded separately.
	Active-active (1:1) HA is supported on SteelHead SD 2.0.
NIC bypass (fail-to-wire)	Currently, NIC level bypass or fail-to-wire is not supported in SteelHead SD.
	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.
	The traditional SteelHead bypass functionality doesn't apply 1:1 to a SteelHead SD appliance because it is now an SD-WAN appliance that acts as a Layer 3 hop (or a custom edge router in some cases). Enabling NIC bypass mode without proper routing architecture support can lead to unintended traffic path behavior and can have security implications.
Fail-to-block	If a SteelHead SD appliance fails, the appliance goes into fail-to-block mode.
	If only the SteelHead WAN optimization service fails, then traffic is passed through unoptimized and the SteelConnect SD-WAN service remains fully operational.
	If only the SteelConnect SD-WAN service fails, then all traffic on the gateway is blocked.
Data store synchronization	Data store synchronization is supported only on the primary interface because the AUX interface isn't available to the virtual SteelHead. (The AUX port is the dedicated port used in HA configurations; it can also be used as an additional WAN uplink.)
RADIUS/Authentication server under Sites	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.
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 cannot optimize UDP traffic using the SteelHead IP blade.

SteelHead feature	Feature after upgrading to SteelHead SD
Source NAT on underlay traffic	Source NAT on underlay traffic is not supported on SteelHead SD 570-SD, 770-SD, 3070-SD, and SDI-2030. 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*.
SteelHead Management Console GUI pages	These SteelHead Management Console GUI elements are not supported in SteelHead SD 2.0: ■ QoS reports. ■ Flow export settings: Export QoS and application statistics to Cascade Flow Collectors. ■ Subnet side rules. ■ WCCP settings. ■ Connection forwarding settings. ■ Failover settings. ■ In-Path Settings: Enabling Link State Propagation. ■ IPSec settings. ■ AUX interface setting in the Base Interfaces page. ■ Caching DNS: Listen on AUX interface check box.

Interface behavior before and after upgrading

Interface attribute	Before upgrade (SteelHead)	After upgrade (SteelHead SD)
Appliance management	SteelHead Management Console	SCM
Primary port interface	- SteelHead management via the SCC or SteelHead Management Console. - DHCP or statically configured.	The virtual SteelHead instance within the SteelHead SD does not have control of the physical network ports except for the Primary interface. - The primary port is used for management of the virtual SteelHead on SteelHead SD using the SCC or SteelHead Management Console. - DHCP or statically configured using the SteelHead SD Management Console. The primary IP address can be acquired using DHCP from the SteelConnect DHCP service. You must cable the primary back to a LAN port using 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.
Auxiliary (AUX) port interface	Backup management port.	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.
In-path management	Management through the SCC or SteelHead Management Console.	Management of the vSH through the in-path management interface must be reconfigured.
In-path interface	Typically one or two SteelHead in-path interfaces are configured (for example, internet and MPLS) over physical LAN and WAN pairs.	The inpath0_0 interface must be reconfigured after upgrade.
SCC hosting	Typically, in the data center and used to manage remote SteelHeads using MPLS paths.	The virtual SteelHead on SteelHead SD will continue to be managed via SCC over MPLS path.
Internet connectivity options	Local breakout or through MPLS from headquarters site.	Internet breakout options must be configured appropriately in SCM.
Baseboard Management Controller (BMC)	Available to remotely power the appliance off and on.	For SteelHead SD 2.0, this port is unavailable.

SteelHead SD and SteelConnect feature compatibility by model

Feature	SteelHead 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 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*.
	Upgrading from SteelHead to SteelHead SD requires the RiOS 9.7.1a virtual SteelHead (vSH) image. The 9.7.1a vSH image is contained within the SteelHead SD 2.0/SteelConnect 2.11. The supported SteelHead to SteelHead SD upgrade paths are: – 9.6.1 > SteelHead SD 2.0 (includes 9.7.1a vSH) – 9.6.2 > SteelHead SD 2.0 (includes 9.7.1a vSH) – 9.6.2a > SteelHead SD 2.0 (includes 9.7.1a vSH) – 9.7.0 or 9.7.0a > 9.7.1 > SteelHead SD 2.0 (includes 9.7.1a vSH)
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)	To use the SCC to upgrade SteelHead to SteelHead SD, you must have SCC 9.7.1 installed.
	Important: Upgrading SCC to 9.8 removes the in-field upgrade option in SCC. The SCC must be running version 9.7.1 for the SteelHead SD in-field upgrade wizard to appear.

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 details on 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 details on the WAN optimization service MIB, see the *SteelHead User Guide*.

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

NIC support

Network interface cards (NICs) are supported on the SteelHead SD 3070-SD appliances for nonbypass traffic. NICs aren't supported on the SteelHead SD 570-SD and 770-SD appliances.

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 appliance 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

Important: If you have the Two-Port 10-GbE Fiber SR NIC (410-00302-03/NIC-1-010G-2SR-BP) installed on the CX3070 appliance, you must remove the card before you begin the in-field upgrade. The CX3070 motherboard contains 1GB NICs that can be used for uplinks if capacity planning doesn't mandate 10-GB. You can buy or exchange the 10-GB bypass NIC with a 10-GB nonbypass NIC prior to upgrading if you prefer.

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

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.)

- Make sure at least one WAN port has internet connectivity.

- We highly recommend that your network provides a DHCP service so the appliance can establish a connection automatically.

2

In-Field Upgrade Workflow

This chapter describes the workflow for performing an in-field upgrade from a SteelHead CX570, CX770, or CX3070 appliance to a SteelHead SD 570-SD, 770-SD, or 3070-SD appliance.

Workflow for performing an in-field upgrade

Task	Reference
1. Download the SteelHead SD software image. (The SteelHead SD software is contained within the SteelConnect 2.11 image.)	The first email that you receive contains the link to download the software image. The software reimages the appliance and includes the RiOS 9.7.1a release as part of the SteelConnect 2.11 image. For details, see "SteelConnect SD-WAN service licensing" on page 27.
	If you didn't receive this email, contact your sales representative or Riverbed Support at https://support.riverbed.com.
2. Write down the SteelConnect serial number beginning with XN.	The first email that you receive contains the SteelConnect serial number beginning with XN. You will need this serial number later in the installation process. For details, see "SteelConnect SD-WAN service licensing" on page 27.
3. Redeem your license token.	The second email you receive contains the token to redeem your license. For details, see "SteelConnect SD-WAN service licensing" on page 27.
	If you didn't receive this email, contact your sales representative or Riverbed Support at https://support.riverbed.com.
4. Log in to SteelConnect Manager (SCM) portal and choose Organizations > Licenses to redeem the token.	The final email contains the URL to connect to SteelConnect Manager, default login and password, and the instructions for redeeming your token. For details, see "SteelConnect SD-WAN service licensing" on page 27.
	If you don't receive these emails, contact your sales representative or Riverbed Support at https://support.riverbed.com.
5. Back up or save your SteelHead configuration to an external machine before you begin the in-field upgrade.	For details on how to back up or save your SteelHead configuration, see "Backing up your SteelHead configuration" on page 56.

Task	Reference
6. Add dual in-line memory modules (DIMMs) to upgrade your SteelHead appliance to a SteelHead SD appliance.	For details, see "Upgrading the appliance memory" on page 31.
7. Add and register the appliances in SteelConnect Manager (SCM).	For details, see the "Adding and Registering Appliances in SCM" on page 41.
8. If necessary, recable your appliance.	Before proceeding with the software upgrade, make sure WAN port on the appliance have internet connectivity so that the system can reach SCM after the software upgrade is complete. For details, see "Recabling the appliance" on page 47.
9. Install the SteelHead SD software image.	For prerequisites and requirements, see "Requirements and prerequisite tasks prior to upgrading" on page 51. For details, see "Upgrading the SteelHead Software" on page 51.
10. These settings are required for the SteelHead SD to contact SCM for the first time and for WAN optimization to function properly: – Configuring the primary and LAN ports. – Configuring the in-path interface. – Identifying the in-path gateway IP address. – Identifying the primary IP address of the SteelHead. – Configuring SteelConnect to act as the DHCP server. – Enabling WAN optimization in SCM. – Configuring WAN optimization on the virtual SteelHead.	For details, see the *SteelHead SD Installation Guide*. For details on configuring SD-WAN, see the *SteelHead SD User Guide*, and the *SteelConnect Manager User Guide*.

3

SteelHead SD Licensing

This chapter describes the procedures for obtaining licenses for the SteelHead SD. It includes these sections:

- "SteelConnect SD-WAN service licensing" on page 27
- "SteelHead WAN optimization service licensing" on page 30

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 conversion process. After purchasing the SteelHead SD in-field upgrade kit, you will receive three emails:

- The first email contains the download link for the SteelHead SD software, links to the upgrade guide, and the SteelConnect and virtual SteelHead serial numbers.

Figure 3-1. Example of first email containing link to download SteelHead SD software

Dear Riverbed Customer ,

VIEW YOUR ACCOUNT

Thank you for your recent purchase to upgrade your Steelheads to
Steelhead SDs.

VISIT SUPPORT

Note: SteelHead appliances must have the required amount of RAM in
order for this upgrade to be successful. If the upgrade kit that contains
the memory has been purchased for this upgrade, please follow the
steps below to install the memory before attempting the software
upgrade:

EMAIL SUPPORT

1. Power down the appliance.
2. Add the memory that came with your upgrade kit.
3. Power on the Steelhead.

Detailed steps for installing the memory kit can be found here.

Instructions for installing the software:

1. Please make sure the Steelhead appliance is currently running
   RIOS version   . This is a mandatory requirement
   for performing the upgrade
2. Download the new SteelHead SD software from the Riverbed
   Support Portal here.   **SteelHead SD Software download link**
3. Install the new software.

Detailed steps for installing the software can be found in the SteelHead
SD Installation Guide here.

You have purchased the upgrades for the following serial number(s):

Steelhead Serial Number	VGW Serial Number
	XN

SteelConnect Serial Number

Please contact the Riverbed Support team or your local Riverbed sales
team if you have any installation or evaluation issues.

Sincerely,
Riverbed Support

Note: The email you receive may differ slightly from this example.

Important: Write down the SteelConnect serial number that starts with XN. You will need the serial number to register your SteelHead SD appliances.

■ The second email contains the license token. Each token is redeemable only once. After you upgrade the software, you redeem the token in SCM and all hardware nodes and license keys are added to your organization.

Figure 3-2. Example of the token email
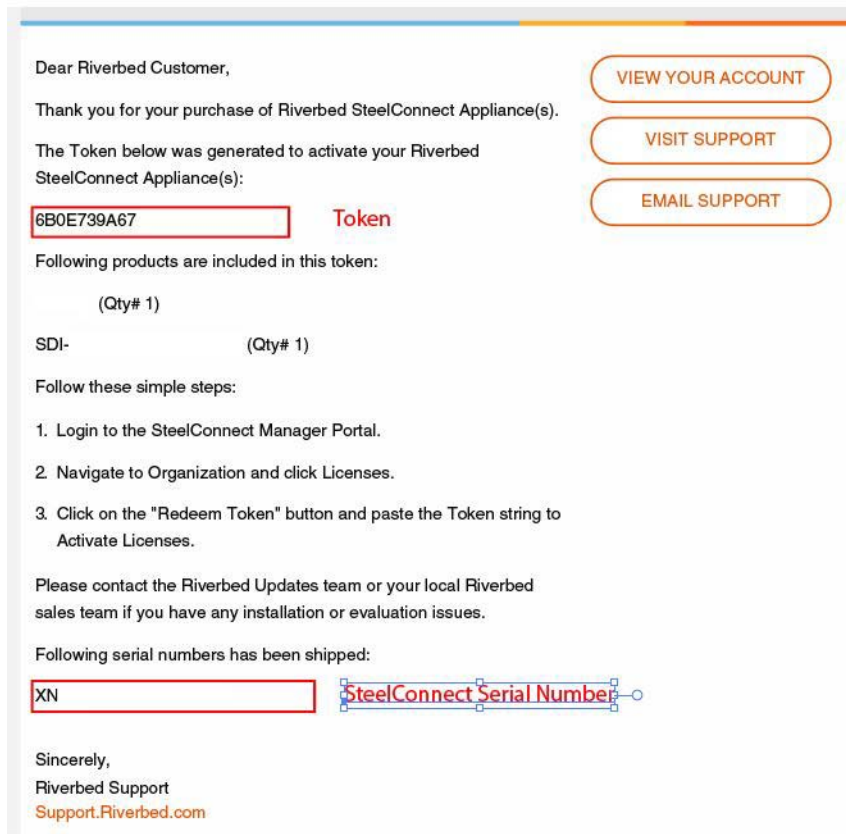
■ The third email contains the URL for connecting to SteelConnect Manager instance and the default login (**admin**) and default password (**pppp**). This email is requested by the sales team and sent by the Riverbed Cloud Operations team.

To redeem the SD-WAN service token

1. Open the email you received from Riverbed and copy the token.

2. Connect to SteelConnect Manager. The default login is **admin**, and the default password is **pppp**.

Note: You should receive an email from the Riverbed Cloud Operations team that contains the URL for connecting to the SteelConnect Manager instance and login information. If you haven't received this email, contact your sales representative or Riverbed Support at https://support.riverbed.com.

3. Choose Organization > Licenses.

4. Click **Redeem Token** and paste the token into the text box.

5. Click **Submit**.

SteelHead WAN optimization service licensing

The SteelHead WAN optimization service requires an MSPEC license. Once you connect the 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.

Because each license key is generated for a specific appliance, ensure that you install your license key on the appropriate appliance.

For details on installing licenses using the CLI or the Management Console, see the *SteelHead User Guide* or the *SteelCentral Controller for SteelHead User Guide*.

4

Upgrading the SteelHead Appliance Memory

This chapter describes how to upgrade the SteelHead CX570, CX770, and CX3070 dual in-line memory modules (DIMMs) to convert to a SteelHead SD 570-SD, 770-SD, or 3070-SD appliance. It also describes how to recable the appliance. It includes these sections:

- "Upgrading the appliance memory" on page 31
- "Adding DIMMs to the SteelHead CX570 appliance" on page 32
- "Adding a DIMM to the SteelHead CX770 appliance" on page 34
- "Adding a DIMM to the SteelHead CX3070 appliance" on page 37
- "Troubleshooting" on page 40

Upgrading the appliance memory

To upgrade your SteelHead appliance to a SteelHead SD appliance, you must add additional memory. The amount of memory depends on your appliance model.

Your in-field upgrade kit contains these DIMMs to upgrade your appliance to a SteelHead SD:

SteelHead model name	Current DIMM	Upgrade kit DIMM	Total DIMM to be added	Total DIMM after upgrade	Upgraded SteelHead SD model name
CX570	1 x 2 GB	3 x 2 GB	4 x 2 GB	8 GB	570-SD
CX770	2 x 2 GB	1 x 8 GB	2 x 2 GB	12 GB	770-SD
			1 x 8 GB		
CX3070	3 x 4 GB	1 x 4 GB	4 x 4 GB	16 GB	3070-SD

The hardware upgrade takes about 30 minutes.

Prerequisites and requirements

- Make sure you are upgrading a SteelHead CX570, CX770, or CX3070 appliance. Any other SteelHead models can't be field upgraded to a SteelHead SD appliance.
- Check the serial number of the appliance to make sure it is eligible for upgrade. Refer to the first email from Riverbed—all SteelHead serial numbers slated for upgrade are listed in that email. For details regarding the emails you will receive, see "SteelConnect SD-WAN service licensing" on page 27.

- Back up your configuration on the SCC or SteelHead Management Console. For details, see "Backing up your SteelHead configuration" on page 56.

- If you have the Two-Port 10-GbE Fiber SR NIC (410-00302-03/NIC-1-010G-2SR-BP) installed on the CX3070 appliance, you must remove the card before you begin the in-field upgrade. The CX3070 motherboard contains 1-GB NICs that can be used for uplinks if capacity planning doesn't mandate 10-GB. You can buy or exchange the 10G bypass NIC with a 10-GB nonbypass NIC prior to upgrading if you prefer. For details on NIC support, see "NIC support" on page 23.

Adding DIMMs to the SteelHead CX570 appliance

The SteelHead CX570 appliance has one 2-GB DIMM in slot A1. You add the three 2-GB DIMMs to slots BI, A0, and B0 in the appliance.

To add DIMMs to the SteelHead CX570 appliance

1. Power down the appliance and unplug all peripheral devices and the power cable.

2. To remove the chassis cover, unscrew the screws as shown in Figure 4-1.

Figure 4-1. Removing the chassis cover

3. Slide the cover back and lift upward. The DIMMs are shown in Figure 4-2.

Figure 4-2. Locating the DIMM slots

4. Add the three 2-GB DIMMs to fill all the slots. Make sure you align the memory-module edge connector with the slot alignment keys and insert it into the slot. The module slot has two alignment keys that allow you to install the module in only one direction.

Figure 4-3. Inserting the DIMM into the connector slot and securing
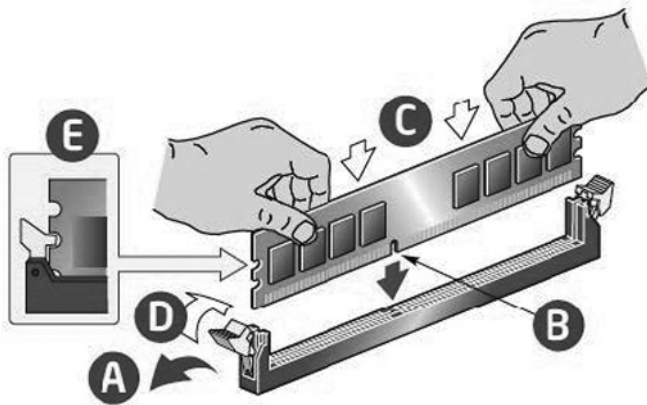
5. Press down on the DIMM with your thumbs while pulling up on the ejectors with your index fingers to lock the module into the slot.

6. Ensure that all ejector tabs are in the upright locked position. If the ejector tabs aren't in the upright locked position, the memory might not be recognized when you reboot the appliance.

7. To replace the chassis cover, place the top cover on the appliance and slide it toward the front of the chassis until the recessed front edge fits smoothly under the chassis edge.

Figure 4-4. Installing the appliance cover

8. Install the screws on the sides, and then install the screw at the back.

9. Replace the power cords and peripherals.

10. Power on the appliance.

11. Connect to the SteelHead Management Console and choose Reports > Diagnostics: System Details. Under Memory, the status states OK.

12. Under Memory, click the right arrow (>) to expand the page. The installed and available memory is listed.

If the screen doesn't show OK or if the memory listed is incorrect, open the appliance and make sure that each memory module is seated firmly in the slots and that the white ejector tabs are in the upright, locked position.

Adding a DIMM to the SteelHead CX770 appliance

The SteelHead CX770 appliance has two 2-GB DIMMs in slots A1 and B1. First, you must move the DIMM in slot A1 to B0, and then you add the 8-GB DIMM to slot A1.

If the DIMMs aren't in the correct slots, the system won't recognize the new memory when you boot the appliance.

To add a DIMM to the SteelHead CX770 appliance

1. Power down the appliance and unplug all peripheral devices and the power cable.

2. To remove the chassis cover, unscrew the screws as shown in Figure 4-5.

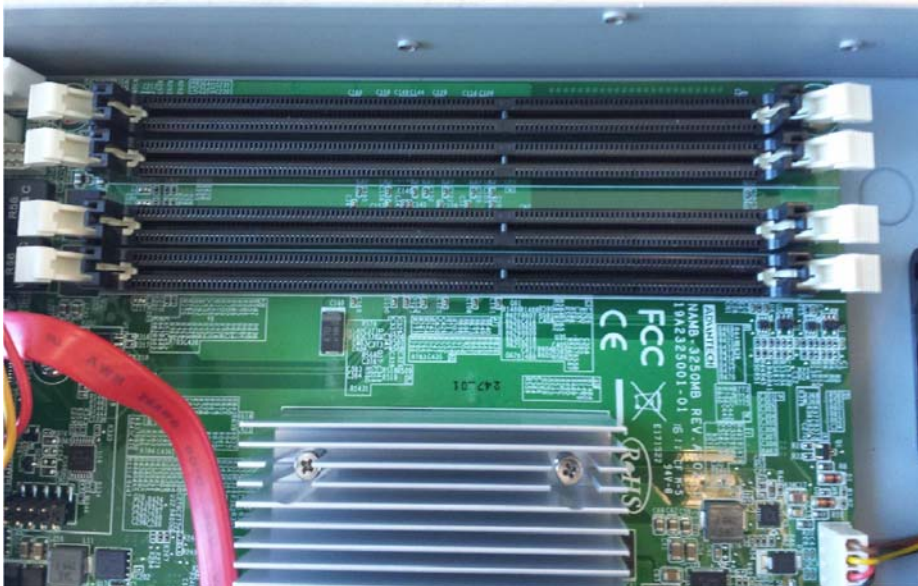**Figure 4-5. Removing the chassis cover**

3. Slide the cover back and lift upward. The DIMMs are shown in Figure 4-6. The system has two 2-GB DIMMs in slots A1 and B1.

Figure 4-6. Locating the DIMM slots

4. Move the 2-GB DIMM in slot A1 to slot B0.

5. Add the new 8-GB DIMM in slot A1. Make sure you align the memory-module edge connector with the slot alignment keys and insert it into the slot. The module slot has two alignment keys that allow you to install the module in only one direction.

Figure 4-7. Inserting the DIMM into the connector slot and securing
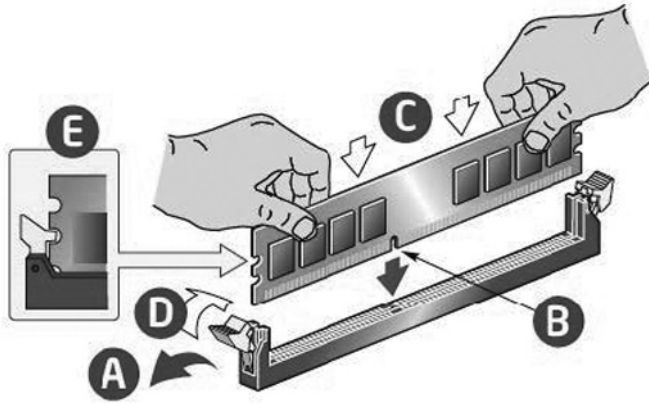
Important: Make sure you add the memory to the correct slot. If you don't add the memory to the correct slot, the system won't recognize the new memory when you boot the appliance.

6. Press down on the DIMM with your thumbs while pulling up on the ejectors with your index fingers to lock the module into the slot.

7. Ensure that all ejector tabs are in the upright locked position. If the ejector tabs aren't in the upright locked position, the memory won't be recognized when you reboot the appliance.

8. To replace the chassis cover, place the top cover on the appliance and slide it toward the front of the chassis until the recessed front edge fits smoothly under the chassis edge.

Figure 4-8. Installing the appliance cover

9. Install the screws on the sides, and then install the screw at the back.

10. Replace the power cords and peripherals.

11. Power on the appliance.

12. Connect to the SteelHead Management Console and choose Reports > Diagnostics: System Details. Under Memory, the status states OK.

13. Under Memory, click the right arrow (>) to expand the page. The installed and available memory is listed.

If the screen doesn't show OK or if the memory listed is incorrect, open the appliance and make sure that each memory module is seated firmly in the slots and that the white ejector tabs are in the upright locked position.

Adding a DIMM to the SteelHead CX3070 appliance

Figure 4-9 shows memory module slot locations. You add a 4-GB DIMM to the empty slot located at D1. If you don't add the DIMM to the correct slot, the system won't recognize the new memory when you boot the appliance.

Figure 4-9. Memory module slot locations in 1U appliances
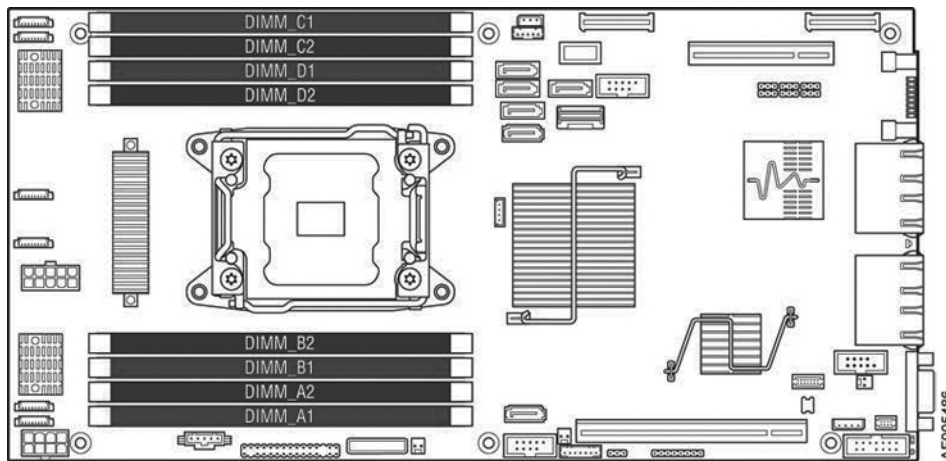
To add a DIMM to the SteelHead CX3070 appliance

1. Power down the appliance and unplug all peripheral devices and the power cable.

2. To remove the chassis cover, unscrew the four screws (letter A).

Figure 4-10. Removing the appliance cover
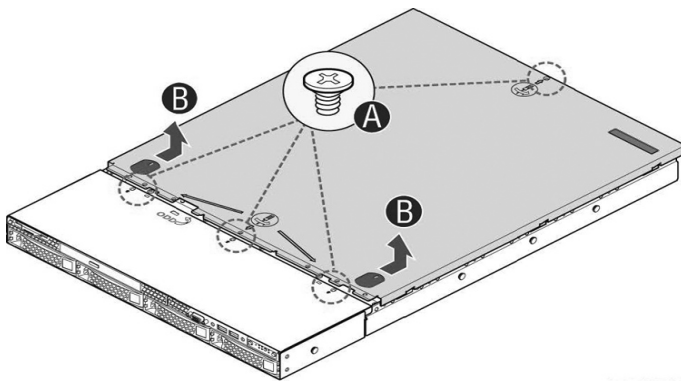
3. Slide the cover back and lift upward (letter B).

4. Locate the air duct and lift straight up.

Figure 4-11. Removing the air duct
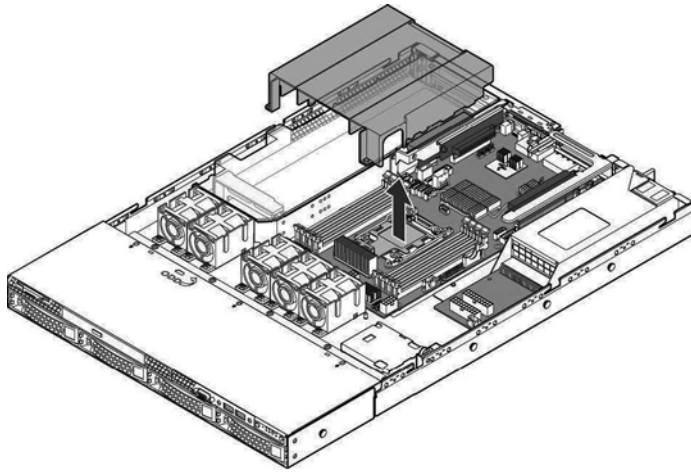
5. If you have the Two-Port 10-GbE Fiber SR NIC (410-00302-03/NIC-1-010G-2SR-BP) installed, you must remove the card before you begin the in-field upgrade. The CX3070 motherboard contains 1-GB NICs that can be used for uplinks if capacity planning doesn't mandate 10-GB. You can buy or exchange the 10-GB bypass NIC with a 10-GB nonbypass NIC prior to upgrading if you prefer. For details on NIC support, see "NIC support" on page 23.

6. Add the 4-GB DIMM to slot D1. The DIMM locations are labeled on the appliance.

    Align the memory-module edge connector with the slot alignment keys and insert it into the slot. The module slot has two alignment keys that allow you to install the module in only one direction.

Figure 4-12. Inserting the DIMM into the connector slot and securing
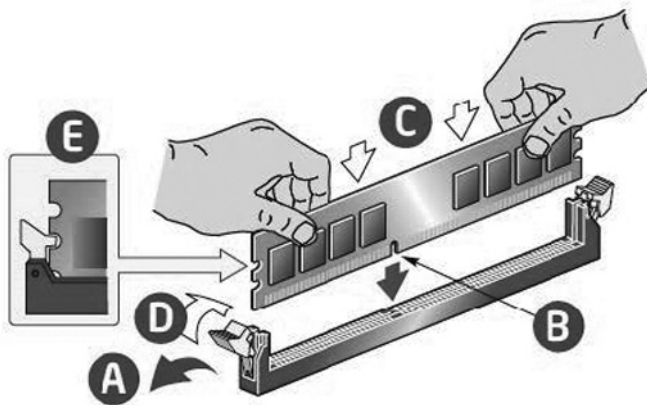
Important: Make sure you add the memory to the correct slot. If you don't add the memory to the correct slot, the system won't recognize the new memory when you boot the appliance.

7. Press down on the DIMM with your thumbs while pulling up on the ejectors with your index fingers to lock the module into the slot.

8. Ensure that all ejector tabs are in the upright locked position. If the ejector tabs aren't in the upright locked position, the memory might not be recognized when you reboot the appliance.

9. Before replacing the air duct, ensure the HDD cable is inside the air duct.

10. Align the two holes on the air duct with the alignment pins on the chassis, and lower the air duct into place.

Figure 4-13. Installing the air duct
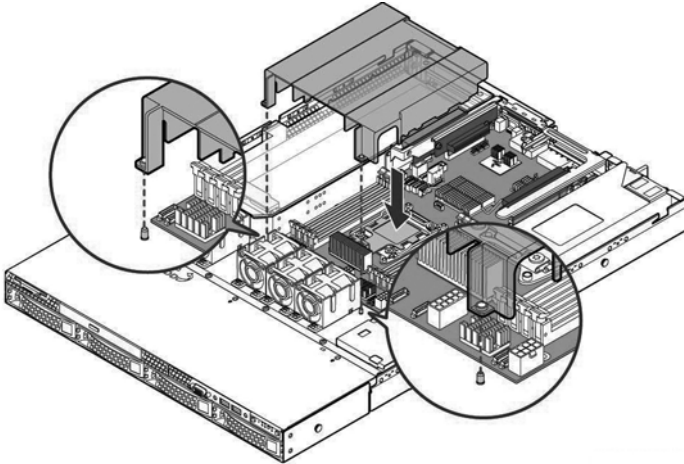
11. To replace the chassis cover, place the top cover on the appliance and slide it toward the front of the chassis until the recessed front edge fits smoothly under the chassis edge and the locking pins (letter A) are fully engaged.

Figure 4-14. Installing the appliance cover
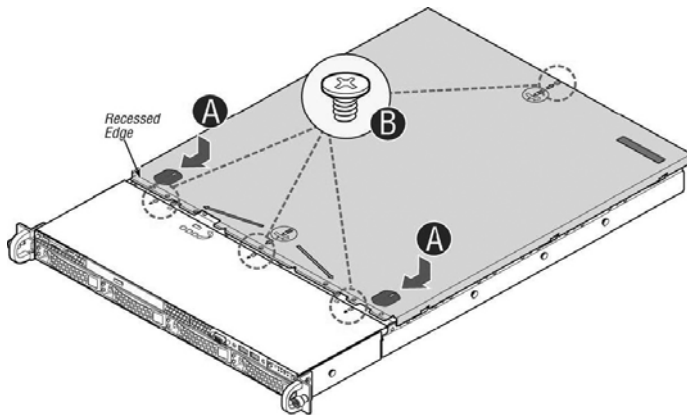
12. Install the three screws at the front, and then install the screw at the back (letter B).

13. Replace the power cords and peripherals.

14. Power on the appliance.

15. Connect to the SteelHead Management Console and choose Reports > Diagnostics: System Details. Under Memory, the status states OK.

16. Under Memory, click the right arrow (>) to expand the page. The installed and available memory is listed.

If the screen doesn't show OK or if the memory listed is incorrect, open the appliance and make sure that each memory module is seated firmly in the slots and that the white ejector tabs are in the upright locked position.

Troubleshooting

If you haven't performed the memory module installation correctly, an error message appears:

```
Image install of 'image.img' failed. The upgrade image provided does not support this model.
```

Open the appliance and make sure that each memory module is seated firmly in the slots and that the white ejector tabs are in the upright locked position.

5

Adding and Registering Appliances in SCM

This chapter describes how to add and register SteelHead SD appliances using SteelConnect Manager (SCM). It includes these sections:

This chapter doesn't describe how to configure SD-WAN features in detail. For details, see the *SteelHead SD Installation Guide*, the *SteelHead SD User Guide*, and the *SteelConnect Manager User Guide*.

Overview

For each SteelHead appliance you'll be upgrading, you must add it to SCM as a shadow appliance and register it.

To register SteelHead appliances that you are converting, you will need the SteelHead SD serial number that was sent via email by Riverbed. The SteelConnect serial number starts with XN. Make sure you register your appliances using the SteelConnect serial number. If you don't, the SCM won't autodetect the appliances when you register them.

DHCP versus static IP

The inpath0_0 interface address on the virtual SteelHead instance is needed for initial contact between the SteelHead and SCM during the upgrade process. These settings are preconfigured in SCM so the SteelHead doesn't revert to DHCP after initial contact with SCM.

We recommend you use the DHCP server when you are upgrading SteelHeads to SteelHead SD. If you are using DHCP for uplink IP addresses, no additional configuration is needed. SteelConnect will use DHCP to obtain the system inpath0_0 interface address. After the new image is downloaded and reflashed, the appliance reboots and acquires a temporary WAN IP address via DHCP for communication over the internet. It then contacts SCM and the Riverbed licensing servers to download certificates and complete the installation as a SteelHead SD appliance.

If your network isn't running a DHCP server, you can use a static IP address, but you must preconfigure these in-path IP addresses, gateways, and DNS servers on the SteelHead appliances and in SCM before beginning the in-field upgrade process. At least one WAN uplink interface (for example, WAN0_0, WAN0_1, WAN3_0, WAN3_1) must have internet connectivity.

For details on configuring SD-WAN settings, see "Designing a Network" in the *SteelConnect Manager User Guide*.

Logging in to SCM

You log in to SCM using the URL that was emailed to you when you purchased the in-field upgrade kit. The email 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.

For details on configuring SD-WAN settings, see "Quick Start" and "Designing a Network," in the *SteelConnect Manager User Guide*.

To log in to SCM

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.

    SCM will open with a default organization.

Figure 5-1. SCM Dashboard
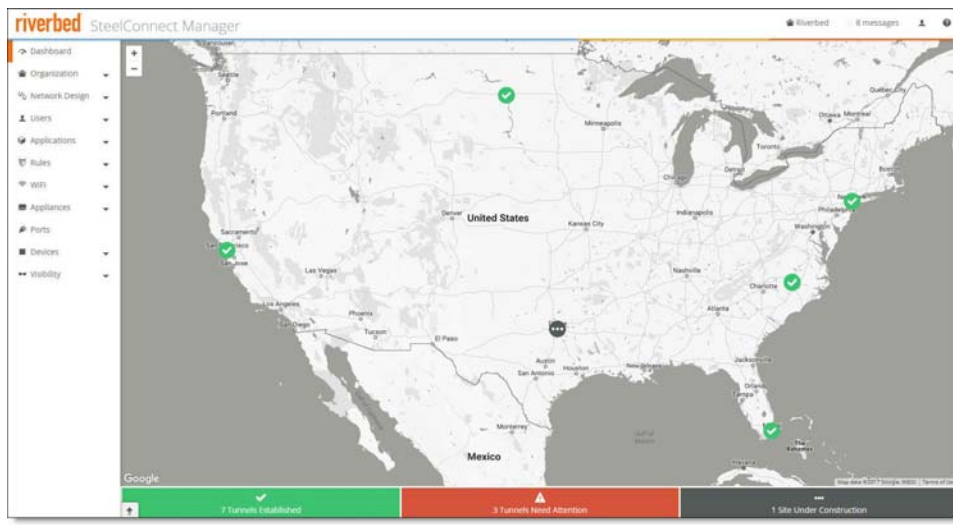
The dashboard shows a visual representation of your organization. Double-click to zoom in. For more details, see "Monitoring the Network" in the *SteelConnect Manager User Guide*.

Defining an organization

The first task is to define an organization. SCM uses these terms to describe your company:

- **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 or SteelHead SD appliances 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. 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. You'll want to edit the default organization.

After adding the company name, you'll add basic information. You can always change and customize this information later.

To change the default name and location of the organization

1. Choose Organization to display the default organization settings.

Figure 5-2. Changing 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 details on 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 **Add a New Site**.

3. Select Create Site to create a site for the data center.

Figure 5-3. Creating site

4. Add a site tag: for example, headquarters.

5. Add the site's location: for example, San Francisco.

6. Specify the site's address, country, and time zone. Make sure the time zone matches the site's location.

7. Click **Submit**.

After you create the site, it appears on the dashboard map. Repeat these steps to add sites for the branch offices.

Adding zones

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 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 to the LAN zone on the SteelHead

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**.

The LAN zone is complete. 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 for the future and then later drop the physical appliance into the topology with no further configuration needed.

When you add an appliance for future deployment, it's called a *shadow appliance*. Shadow appliances are basically placeholders that represent the physical appliances until you register them with their serial numbers.

To add a shadow appliance

1. Choose Appliances and click **Add appliances**.

2. Select Create Shadow Appliance.

3. Select the SteelHead SD appliance from the model drop-down list.

4. Choose Headquarters as the site to deploy the shadow gateway.

5. Click **Submit**.

6. Repeat Step 2 through Step 5, for the remaining appliances.

Registering SteelHead SD appliances

The next task is to register the physical appliances to transform them from shadow appliances into physical appliances.

To register appliances

1. Locate the SteelConnect serial number either from the email that you received from Riverbed or from the appliance label. The SteelConnect serial number starts with XN.

Figure 5-4. Locating the serial number that starts with XN

2. Choose Appliances > Overview.

3. Select the shadow appliance, and select Actions > Register hardware.

Figure 5-5. Registering appliances

4. Type the serial number.

5. Optionally, you can select the site for the appliance or set that later.

6. Click **Submit**.

7. Repeat these steps for each appliance.

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. This automatic provisioning makes the appliances easily replaceable, if necessary. A complete mesh overlay connects across all sites and shares all networks that are involved with RouteVPN using full permissions.

After AutoVPN establishes the tunnels, you can view the dashboard map to see a visible representation of the network. 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.

Recabling the appliance

After you register your hardware you might need to recable the appliances to ensure the at least one WAN port has connectivity 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, which 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. For details on DHCP versus static IP, see "Backing up your SteelHead configuration" on page 56.

You cable at least one LAN port (for example, LAN0_0, LAN0_1, and so on) to the LAN port on a switch.

SteelHead SD port definitions

For details on port mappings, see Appendix B, "SteelHead SD Port Mappings."

Port	Description
Primary (PRI)	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.

Port	Description
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.

Recabling the appliance

This sections describes how to recable the appliance (if necessary).

To recable the SteelHead SD appliance

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

Figure 5-6. Connecting the primary port to the LAN switch

2. Plug the straight-through cable into at least one LAN port (LAN0_0, LAN0_1, or LAN3_0, LAN3_1 on the 3070-SD appliance) to the LAN port on the switch.

Figure 5-7. Connecting the LAN switch to the LAN port
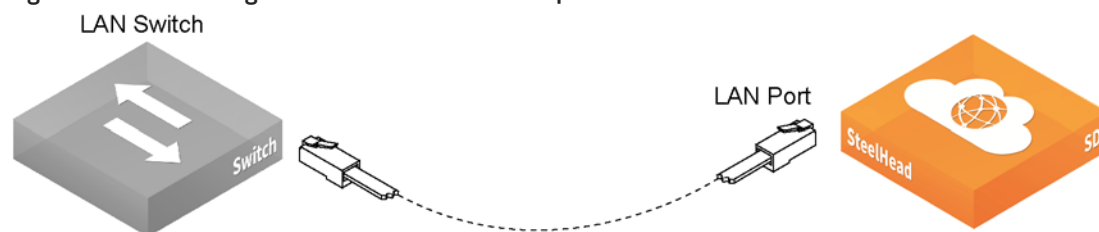
3. Connect at least one WAN port to an uplink from a service provider.

For example, on a 570-SD or 770-SD appliance, use a straight-through cable to connect the WAN0_0 or WAN0_1 port to an internet uplink or to an MPLS uplink for back-hauled internet traffic. On a 3070-SD appliance, 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.

Figure 5-8. Connecting the WAN port to the WAN router

After you finish these tasks, you are ready to install the software. For details, see Chapter 6, "Upgrading the SteelHead Software." .

6

Upgrading the SteelHead Software

This chapter describes how to install the software image to upgrade your SteelHead appliance to a SteelHead SD appliance. It includes these sections:

- "Requirements and prerequisite tasks prior to upgrading" on page 51
- "DHCP versus static IP" on page 54
- "Network design prerequisites" on page 54
- "Backing up your SteelHead configuration" on page 56
- "Upgrading software using the SCC" on page 56
- "Upgrading software using the SteelHead Management Console" on page 61
- "What's next" on page 67
- "Troubleshooting" on page 68

Important: These instructions assume that you have upgraded your appliance memory, added and registered your appliances, and configured basic SD-WAN features using SCM. For details, see Chapter 4, "Upgrading the SteelHead Appliance Memory," and Chapter 5, "Adding and Registering Appliances in SCM." .

Requirements and prerequisite tasks prior to upgrading

Make sure you follow these requirements before you begin the in-field upgrade process.

- Downgrading from a SteelHead SD to a SteelHead isn't supported. The SteelHead SD installer removes all the existing partitions and installs a new SteelHead SD product image.
- Only SteelHead SD CX570, CX770, and CX3070 appliances are qualified for in-field upgrades.
- Upgrading from SteelHead to SteelHead SD requires the RiOS 9.7.1a virtual SteelHead (vSH) image. The 9.7.1a vSH image is contained within the SteelHead SD 2.0/SteelConnect 2.11. The supported SteelHead to SteelHead SD upgrade paths are:
  - 9.6.1 > SteelHead SD 2.0 (includes 9.7.1a vSH)
  - 9.6.2 > SteelHead SD 2.0 (includes 9.7.1a vSH)
  - 9.6.2a > SteelHead SD 2.0 (includes 9.7.1a vSH)
  - 9.7.0 or 9.7.0a > 9.7.1 > SteelHead SD 2.0 (includes 9.7.1a vSH)

- We strongly recommend you use the SCC for in-field upgrades. If you aren't currently running an SCC to manage your network, consider purchasing the SCC or obtaining an SCC evaluation before you begin the upgrade process. The SCC must be running version 9.7.1.

Important: Upgrading SCC to 9.8 removes the in-field upgrade option in SCC. The SCC must be running version 9.7.1 for the SteelHead SD in-field upgrade wizard to appear.

- 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.)

- In addition to the SteelHead serial number, SteelHead SD requires the SteelConnect serial number. The SteelConnect serial number always begins with the prefix XN. The serial numbers are in the email from Riverbed that you received when your sales order was confirmed. For details, see "SteelConnect SD-WAN service licensing" on page 27.

- Your SteelHead configuration must be backed up or saved and copied to an external machine, preferably using the SteelCentral Controller for SteelHead (SCC), prior to starting the upgrade process. The in-field upgrade process reimages the appliance and saves static network uplink settings, the SteelHead serial number, and secure vault settings. The SCC resets the admin user password to the default value, the secure-vault password is retained, and other user permission and passwords can be restored by the SCC. For details, see "Backing up your SteelHead configuration" on page 56.

- Prior to performing the software upgrade, make sure the SteelHead hardware has been upgraded with the additional required memory. For details regarding upgrading the hardware, see "Upgrading the appliance memory" on page 31.

- Perform the installation during off-peak hours or a maintenance window so that the entire upgrade process can complete. The upgrade image is 2.5 GB. This can take up to 3.5 hours depending on latency.

- If you have low-bandwidth or a high-latency connection to the SteelHead during the SCC image push, increase the timeout period from the default of three hours. (During SCC image pushes, RiOS is still running so you can make CLI changes.) You can override the timeout on the SCC CLI using this command:

```
cmc upgrade timeout <timeout-in-seconds>
```

Bandwidth (kbps)	Latency (ms)	Time to download	Recommended timeout
10000	40	45 minutes	Default
5000	40	1 hour 10 minutes	Default
2000	40	2 hours 45 minutes	4 hours
1500	40	3 hours 35 minutes	5 hours

- We recommend you use a DHCP server when you are upgrading SteelHeads to SteelHead SD. With a network running a DHCP server, you don't have to preconfigure the SteelHeads or SCM. If your network isn't running a DHCP server, you must preconfigure the in-path IP address, gateways, and DNS server on the SteelHead and in SCM before beginning the in-field upgrade process. For details, see "Backing up your SteelHead configuration" on page 56 and "Preconfiguring the SteelHead if you are using a static IP address" on page 61.

- Be aware that for a non-DHCP environment, a static IP process on the SteelHead Management Console must be preconfigured prior to upgrading the software. For details, see "Preconfiguring the SteelHead if you are using a static IP address" on page 61.

- We strongly recommend you use the SCC for in-field upgrades. If you aren't currently running an SCC to manage your network, consider purchasing the SCC or obtaining an SCC evaluation before you begin the upgrade process. The SCC must be running version 9.7.1. Upgrading SCC to 9.8 removes the in-field upgrade option in SCC.

- If the SCC isn't an option and you use the SteelHead Management Console to download the image, you can't download the image from a local file due to image size limitations. We recommend you use the secure copy protocol (SCP) to download the image. It can take up to 3.5 hours to download the image to a client on the LAN using SCP. For details on downloading the image using SCP, see "To install the image using the SteelHead Management Console" on page 65.

- You can also use the SteelHead CLI to download and install the image for individual SteelHead appliances. If you use the CLI, you can download the image, save it, and install it later. If you use the SteelHead Management Console GUI to download and install the image, you don't have the option to install the image later—the download and installation can't be interrupted. For details on downloading and installing images using the CLI, see "To install the image using the CLI" on page 67.

- Upgrades aren't supported via an upstream proxy—an alternate network solution to bypass any intermediate proxies is required.

- Cloud Accelerator (SaaS) settings aren't restored from the SCC backup configuration after upgrading the software. You must manually reenable SaaS cloud acceleration manually and reconfigure all settings using SCC CLI pushes as described in comments or manually reconfigure the settings on each SteelHead appliance after you have completed the upgrade process. For details, see "Restoring Service Cloud Accelerator registration and application settings" on page 60.

- After upgrading, SteelHead SD appliances will be set to the default admin password (**password**). You must reconfigure the admin password for the virtual SteelHead and update the stored password on the SCC.

DHCP versus static IP

If you are using DHCP for uplink IP addresses, no additional configuration is needed. SteelConnect will use DHCP to obtain the system primary IP address. After the new image is downloaded and reflashed, the appliance reboots and acquires a temporary WAN IP address via DHCP for communication over the internet. It then contacts SCM and the Riverbed licensing servers to download certificates and complete the installation as a SteelHead SD appliance.

Figure 6-1. DHCP communication
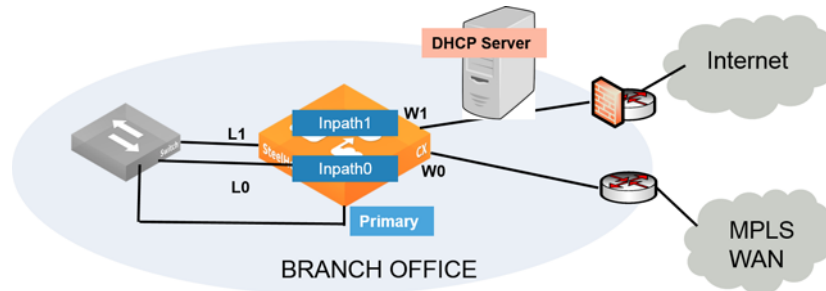
For a non-DHCP site, the software saves and reuses the SteelHead in-path interface IP address. After the new image is downloaded and reflashed, the appliance reboots and uses this saved IP address for communication over the internet.

Prior to upgrading, you must have at least one SteelHead in-path interface that has an IP address that can reach the internet. You must also preconfigure the default gateway and DNS server on the SteelHead and in SCM before beginning the software upgrade process. In addition, at least one uplink interface (that is, WAN0_0, WAN0_1, WAN3_0, WAN3_1) must have internet connectivity. For details, see "Preconfiguring the SteelHead if you are using a static IP address" on page 61.

Note: If your network uplinks use DHCP, choose the DHCP option; it is the easiest. The preconfiguration settings aren't necessary if you use DHCP and the SCC to upgrade and manage your SteelHead SD appliances.

Network design prerequisites

Make sure that you understand that the conversion transforms the SteelHead appliance from a Layer 2 WAN optimization device to a SteelHead SD Layer 3 device. For details, see "Transforming your SteelHead network" on page 14.

Keep in mind that you shouldn't make any router changes prior to completing the in-field upgrade process. If you have a CE router in your network, it must stay in place until the full software upgrade is completed. The SCM and SCC must communicate with the SteelHead during the upgrade process as well as obtain configuration settings and restore the configuration after the conversion. Basically, there are two approaches to conversion:

- Convert SteelHead to SteelHead SD with no changes to ensure successful conversion occurs and the network working.

- Optionally, remove the CE router from your network and put the SteelHead SD at the edge and use it as a CE router. If you choose this option, it involves SCM changes and a cable change. For details, consult with your Riverbed sales engineer or Riverbed Professional Services at http://www.riverbed.com/services/index.html.

Network example #1

This is the ideal conversion scenario in that it allows you to keep the innermost LAN client systems untouched (that is, the LAN clients and LAN router is kept on same subnet) and it doesn't involve disruptions to the CE router or the WAN-side of the network.

**Figure 6-2. Network example #1**

1. You change the subnet between the LAN router and the SteelHead SD before the upgrade process, otherwise, you won't be able to reach the LAN router.

2. Before completing the in-field upgrade process, you configure the virtual SteelHead inpath0_0 interface using the SteelHead Management Console or the SCC to be within the new small subnet created between the LAN router and the converted SteelHead SD appliance. For details, see "Configuring WAN optimization on the virtual SteelHead" in the *SteelHead SD Installation Guide*.

3. After completing the in-field upgrade, you must make a LAN router change that can be performed remotely that is minimally disruptive and low risk. For details, consult with your Riverbed sales engineer or Riverbed Professional Services at http://www.riverbed.com/services/index.html.

Network example #2

In this scenario, the clients, SteelHead SD, and router all share the same network where the SteelHead SD acts as a Layer 2 bridge between the clients and the router.

Figure 6-3. Network example #2
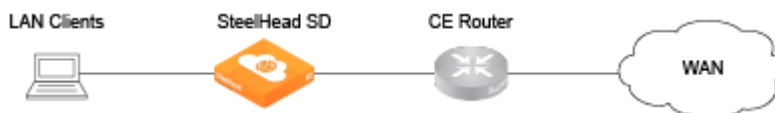
1. After completing the in-field upgrade, SteelHead transitions to SteelHead SD by changing the client LAN subnet. You configure the SteelHead SD LAN zone subnet in SCM. There are no changes on the CE router. For details on configuring the LAN zone, see the *SteelHead SD Installation Guide*.

2. After you complete the in-field upgrade, you manually configure an inpath0_0 interface and default gateway to match the new LAN subnet in the SteelHead Management Console or the SCC. For details, see "Configuring WAN optimization on the virtual SteelHead" in the *SteelHead SD Installation Guide*.

3. Optionally, the SteelHead SD can become the DHCP server for the LAN-side of the network. For example, you might have a preexisting DHCP server you want to keep using. You can also remove the DHCP service from some other device (for example, the CE router or another stand-alone server) and configure SteelHead SD to handle this role.

Backing up your SteelHead configuration

Your SteelHead configuration must be backed up (or saved and copied) to an external machine, prior to starting the upgrade process.

We recommend you do not use the SteelHead Management Console to upgrade your software. The in-field upgrade process reimages the appliance and saves static network uplink settings, the SteelHead serial number, and secure vault settings. Only the SCC resets the admin user password to the default value, the secure-vault password is retained, and other user permission and passwords can be restored by the SCC.

To back up your configuration using the SCC

- 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*.

Important: The backup/restore process in the SCC doesn't automatically restore the license keys. To ensure you have a backup of your license keys, you can create a SCC policy that contains the backed-up license keys prior to the upgrade and then push the policy after upgrade. The virtual SteelHead should perform autolicensing after the upgrade, if it doesn't either push the policy you created or go to the Riverbed Licensing Portal at https://licensing.riverbed.com/ and follow the instructions for retrieving your licenses.

To save your configuration using the SteelHead Management Console

- 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*.

Upgrading software using the SCC

To perform the in-field software upgrade using the SCC, you must be running version 9.7.1.

Important: Upgrading SCC to 9.8 removes the in-field upgrade option in SCC. The SCC must be running version 9.7.1 for the SteelHead SD in-field upgrade wizard to appear.

The SteelHead must be *entitled* before you begin the software upgrade to SteelHead SD. An entitled SteelHead is an appliance that is eligible for an in-field software upgrade using the SCC wizard. You must have already purchased the SteelHead to SteelHead SD license and have received the serial number that begins with XN for the appliance. The SCC will verify whether an appliance is eligible or ineligible when you select appliances in the wizard based on the model, the amount of memory in the appliance, and its entitlement status.

The only SteelHead models that can be upgraded are the Low/Medium/High versions of CX570, CX770, or CX3070 appliances. Make sure you have added additional memory before you begin the in-field software upgrade. For details, see "Upgrading the appliance memory" on page 31.

You must have a DNS record for **riverbedcmc** in the DNS server used by the SteelHead appliance during conversion. The **riverbedcmc** DNS entry points to the IP address of the SCC that is handling the SteelHead SD upgrade process. This DNS entry is required for the SCC in-field upgrade wizard to restore your SteelHead configuration back to the new SteelHead SD virtual SteelHead (vSH) after the software upgrade is complete. If that DNS name doesn't resolve, it must be configured manually via the CLI on the primary IP address.

How does the upgrade work on multiple SteelHeads

If there are multiple appliances being upgraded in the same job, they are run in parallel. If one fails, the remaining in-field upgrades continue to run. If a single task within a specific appliance upgrade fails, subsequent tasks don't run. For example, if you are upgrading SteelHead1 and SteelHead2 in a single job, both start with the Config Backup task. If the backup fails for SteelHead1, its remaining tasks (Image Upgrade, Reboot, Config Restore) abort, but SteelHead2 continues on to the Image Upgrade task after its Config Backup task completes successfully.

For details on backing up your configuration, see "Backing up your SteelHead configuration" on page 56.

To install your software using the SCC

1. Choose Manage > Upgrades > In-Field Upgrades to display the Upgrade SteelHead to SteelHead SD page.

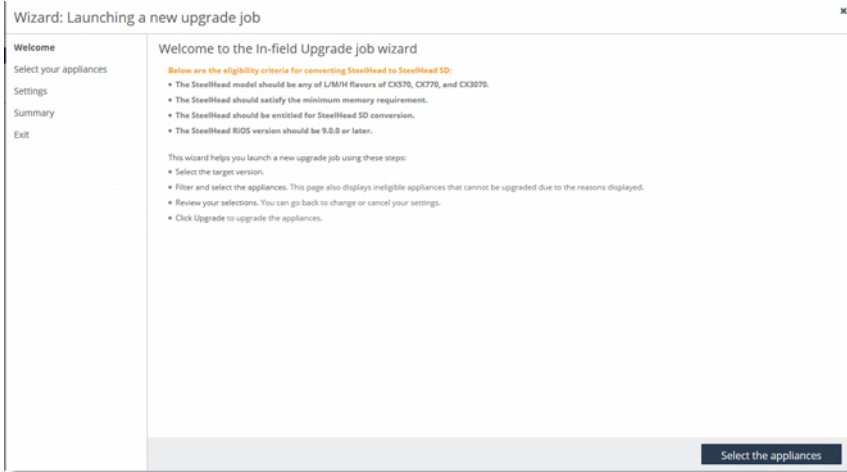**Figure 6-4. Upgrade SteelHead to SteelHead SD page**

	User	Create Time (UTC)	Status	Target Version	Number of appliances
▶	admin	2018-08-10 16:32:30	failed	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-09 23:31:23	failed	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-09 19:23:25	failed	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-09 00:38:14	successful	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-08 20:47:57	successful	2.11.0_1431 / RiOS - 9.7.1a (#40)	1
▶	admin	2018-08-08 20:22:11	successful	2.11.0_1431 / RiOS - 9.7.1a (#40)	1
▶	admin	2018-08-08 20:21:56	successful	2.11.0_1431 / RiOS - 9.7.1a (#40)	1
▶	admin	2018-08-08 14:50:19	successful	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-07 18:45:53	successful	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-07 17:57:20	successful	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-01 16:24:53	successful	2.11.0_1396 / RiOS - 9.7.1a (#36)	1
▶	admin	2018-08-01 15:31:54	successful	2.11.0_1396 / RiOS - 9.7.1a (#36)	1

Upgrade SteelHead to Steelhead SD   Upgrades › Upgrade SteelHead to Steelhead SD
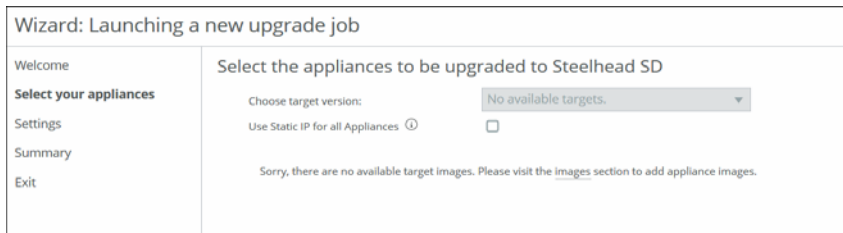
Launch new In-field Upgrade job...

2. Click **Launch new in-field Upgrade job** to display the welcome page of the wizard.

Figure 6-5. Welcome page

3. Click **Select the appliances** to display the Launching SteelHead SD upgrade job page.

Figure 6-6. Selecting the target version and appliances

4. Choose the SteelHead SD target image from the drop-down list. If there are no target images available, you are directed to the Local Images page to install the software image. You can select all appliances or you can filter appliances by:

    –   Hostname

    –   Current version

    –   Group

    –   IP address

    –   Model

    –   Serial number

5. In the drop-down list, select View Selected Appliances to display the filtered appliances. Select Return to eligible appliances to display the eligible appliances again.

6. Select the Use Static IP for all Appliances check box to use a static IP address for the selected appliances in networks where a DHCP server isn't available.

We recommend you use the DHCP server when you are upgrading SteelHeads to SteelHead SD. With a network running a DHCP server, you don't have to preconfigure the SteelHeads or SCM. If your network isn't running a DHCP server, you can use a static IP address, but you must preconfigure these in-path IP addresses, gateways, and DNS servers on the SteelHead appliances and in SCM before beginning the in-field upgrade process. At least one WAN uplink interface (for example, WAN0_0, WAN0_1, WAN3_0, WAN3_1) must have internet connectivity.

7. Click **Configure Settings** to display the Settings page. You can provide upgrade notes for the upgrade appliances to assist you in tracking the in-field upgrade job.

Figure 6-7. Notes for upgrade job

8. Click **Summary** to display the upgrade summary page.

Figure 6-8. Displaying summary information

9. Click **Upgrade** to begin the upgrade operation and display the Exit page, which displays exit information including the time for the upgrade process.

Figure 6-9. Launching the upgrade job

10. Click **Exit** to close the wizard.

After the image downloads and installs, the appliance reboots. After reboot, the appliance goes through the install steps referenced earlier. When the appliance is up and the virtual SteelHead service is started, it connects to the SCC again and restores its previous configuration, minus its IP address information.

Figure 6-10. Successful upgrade

11. After installing the software, connect to SCM and choose Appliances > Overview. You will see the new SteelHead SD listed with status Firmware Upgrade. After the system finishes the upgrade process, the status changes to Online.

Figure 6-11. Appliance online

After you the firmware has updated and is online, you must complete the steps to enable WAN optimization in both SCM and on the virtual SteelHead. For details, see "What's next" on page 67.

Restoring Service Cloud Accelerator registration and application settings

Service Cloud Accelerator (SCA) settings aren't restored from the SCC backup configuration after upgrading the software. You must reenable cloud acceleration manually and reconfigure all settings using SCC CLI pushes.

You can't push the CLI commands from a single policy push. You must individually push each of these CLI commands:

- To register with SCA:

```
service cloud-accel register
```

- To enable SCA:

```
service cloud-accel register
```

- To enable application control:

```
service cloud-accel platforms appid <appname> enable
```

For details on creating policies, see the *SteelCentral Controller for SteelHead User Guide*.

Upgrading software using the SteelHead Management Console

We strongly recommend that you use the SCC to manage the WAN optimization features in your SteelHead SD appliances. Although you can use the SteelHead Management Console or the CLI to configure individual SteelHead SD appliances, managing complex network deployments without the SCC is strongly discouraged.

You can lose all your configuration settings during the upgrade process if you use the SteelHead Management Console to upgrade your software. You must save and copy the SteelHead configuration prior to upgrading the software. For details, see "Backing up your SteelHead configuration" on page 56.

If you use the SteelHead CLI to download and install the image, you can download the image, save it, and install it later. If you use the SteelHead Management Console GUI to download and install the image, we recommend you install the image using the secure copy protocol (SCP). The download and installation can't be interrupted. In slow internet environments, it can take up to 3.5 hours to install the image using SCP.

Important: During the upgrade process using the SteelHead Management Console, a timeout can occur due to the length of time it takes for the image to download and install compared to a regular RiOS upgrade. The message "Image install of 'image.img' is in progress" appears, indicating that you can't initiate another upgrade action while the current upgrade is in progress. For details on extending the timeout period, see "Requirements and prerequisite tasks prior to upgrading" on page 51.

Preconfiguring the SteelHead if you are using a static IP address

If you are using the SteelHead Management Console to install the image, prior to upgrading, you must have at least one SteelHead in-path interface that has an IP address that can reach the internet. You must also preconfigure the default gateway and DNS server on the SteelHead and in SCM before beginning the software upgrade process. In addition, at least one uplink interface (for example, WAN0_0, WAN0_1, WAN3_0, WAN3_1) must have internet connectivity.

Configuring the SteelHead MOTD
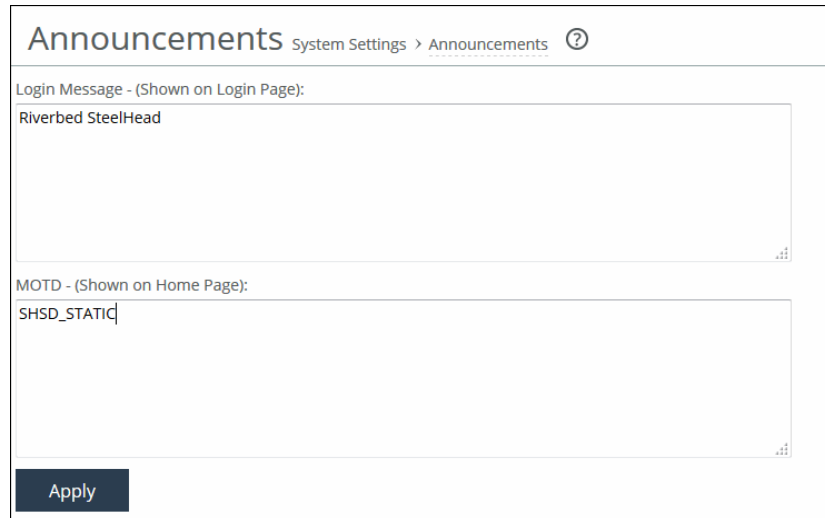
You must set the message of the day (MOTD) to SHSD_STATIC before you configure the DNS settings, inpath0_0 interface, and the default gateway. If you don't set the MOTD to SHSD_STATIC the in-field upgrade process will not complete properly.

To configure the MOTD

1. Connect to the SteelHead Management Console. For details, see the *SteelHead User Guide*.

2. Choose Administration > System Settings: Announcements.

3. Type **SHSD_STATIC** in the MOTD text box and click **Apply**.

Figure 6-12. Adding a string to the MOTD

4. Click **Apply** to apply your changes to the running configuration.

5. Click **Save to Disk** to save your settings permanently.

Configuring the DNS name server to reach SCM

On the SteelHead, you must ensure the DNS server resolves to an internet IP address that is internet reachable via the LAN uplink set in SCM.

To configure the DNS name server to reach SCM

1. Connect to the SteelHead Management Console. For details, see the *SteelHead User Guide*.

2. To configure the DNS name server, choose Networking > Networking: Host Settings.

Figure 6-13. Configuring DNS

3. Under DNS Settings, complete the configuration as described in this table.

Control	Description
Primary DNS Server	Specify the IP address for the primary DNS name server. The DNS server must resolve to and internet IP address that is internet reachable via the LAN uplink set in SCM. Starting with RiOS 9.5, IPv6 addresses are allowed.
Secondary DNS Server	Optionally, specify the IP address for the secondary name server. Starting with RiOS 9.5, IPv6 addresses are allowed.
Tertiary DNS Server	Optionally, specify the IP address for the tertiary name server. Starting with RiOS 9.5, IPv6 addresses are allowed.
DNS Domain List	Specify an ordered list of domain names. If you specify domains, the system automatically finds the appropriate domain for each of the hosts that you specify in the system.

4. Click **Apply** to apply your changes to the running configuration.

5. Click **Save to Disk** to save your settings permanently.

Configuring the inpath0_0 interface and default gateway on the SteelHead

You configure the in-path interface and the default gateway with the static IP address that you will use for uplinks (for example, inpath0_0 for WAN0_0 uplink, inpath0_1 for WAN0_1 uplink, and so forth).

■ You configure the inpath0_0 interface to point to the WAN uplink you configured in SteelConnect (for example, WAN0_0 uplink or WAN0_1 uplink).

- You configure the in-path default gateway to point to the zone gateway IP address in SteelConnect.

An in-path interface that isn't configured will result in the corresponding uplink being configured as DHCP in SCM.

To configure the inpath0_0 interface and default gateway on the SteelHead

1. Connect to the SteelHead Management Console. For details, see the *SteelHead User Guide*.

2. Choose Networking > Networking: In-Path Interfaces to display the In-Path Interfaces page.

Figure 6-14. Configuring in-path interfaces

3. Under In-Path Interface Settings, select the inpath0_0 interface name.

4. Complete the configuration as described in this table (depending on the IP version).

Control	Description
Enable IPv4	Select this check box to assign an IPv4 address. You can only assign one IPv4 address per in-path interface.
	Note: The primary and in-path interfaces can share the same subnet. The primary and auxiliary interfaces can't share the same network subnet.
	To remove an IPv4 address, clear this check box and click **Apply**.
IPv4 Address	Specify an IP address. This IP address is the in-path address for the WAN uplink on SteelConnect.
IPv4 Subnet Mask	Specify the subnet mask.
In-Path Gateway IP	Specify the IP address for the in-path default gateway. This is the in-path default gateway to point to the zone gateway IP address in SteelConnect.

5. Click **Apply** to apply your changes to the running configuration.

6. Click **Save to Disk** to save your settings permanently.

Installing the image using the SteelHead Management Console

If you are using the to SteelHead Management Console install the image, we recommend you install the image using SCP. The download and installation can't be interrupted. In slow internet environments, it can take up to 3.5 hours to install the image using SCP. You can also use HTTP or FTP to download the image to the appliance if the upgrade image is hosted on a local server.

These instructions describe how to install the image using SCP.

To install the image using the SteelHead Management Console

1. Prior to installing the image, we recommend you set up a free an SCP server, using one of these options:

   – For Windows: https://winscp.net/eng/docs/guide_windows_openssh_server

   – For Linux: https://help.ubuntu.com/lts/serverguide/openssh-server.html

2. Connect to the SteelHead Management Console. For details, see the *SteelHead User Guide*.

3. Choose Administration > Maintenance: Software Upgrade.

4. Type the SCP URL in the From URL text box in the format scp://username:password@host/path. You must use SCP to download the image. The download can take up to 3.5 hours.

Figure 6-15. Installing the image via a URL

5. Click **Install**.

    The software image is downloaded and installed on the other partition with RiOS still running on the appliance. The installer doesn't reboot the appliance. Thus, you can stop the upgrade process at this step and retain your original SteelHead image and configuration settings.

6. Choose Administration > Maintenance > Reboot/Shutdown.

7. Click **Reboot**. The appliance will reboot into the SteelHead SD installer to install the product image. The installation takes approximately 20 minutes.

Tip: To view the progress of the installation, connect the serial port to a terminal server (baud rate: 9600 bps; login: admin; password: riverbedAlmanor).

---

8. After installing the software, connect to SCM and choose Appliances > Overview. You will see the new SteelHead SD listed with status Firmware Upgrade. After the system finishes the upgrade process, the status changes to Online.

Figure 6-16. Appliance online

9. After the firmware has updated and is online, you must complete the steps to enable WAN optimization in both SCM and on the virtual SteelHead. For details, see "What's next" on page 67

To install the image using the CLI

1. Log in to the CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.

2. Enter configuration mode. For details, see the *Riverbed Command-Line Interface Reference Manual*.

   ```
   hostname (config) #
   ```

3. To fetch the image using SCP, run these commands:

   ```
   hostname (config) # image fetch ?
   <http, ftp, or scp URL (e.g. scp://username:password@host/path)>
   hostname (config) # image fetch  scp://username:password@host/path
   ```

4. To upgrade the image, run this command:

   ```
   hostname (config) # image upgrade <image filename>
   ```

What's next

The next tasks for configuring your SteelHead SD are outlined in "Installing SteelHead SD," in the *SteelHead SD Installation Guide*:

These tasks are required for the SteelHead SD to contact SCM for the first time and for WAN optimization to function properly:

- Configuring the primary and LAN ports.
- Configuring the in-path interface.
- Identifying the in-path gateway IP address.
- Identifying the primary IP address of the SteelHead.
- Configuring SteelConnect to act as DHCP server.
- Enabling WAN optimization in SCM.
- Configuring WAN optimization on the virtual SteelHead.

Troubleshooting

This section describes some basic troubleshooting procedures.

Insufficient memory or unsupported model

An error is displayed stating that the upgrade isn't supported if the appliance doesn't have enough system memory, the memory upgrade hasn't been performed, or the image is installed on a nonsupported SteelHead model. This error can also occur if the memory isn't seated properly in the appliance. If so, open the appliance and make sure that each memory module is seated firmly in the slots and that the white ejector tabs are in the upright locked position.

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.

Downgrade check

If a software downgrade is attempted or when the upgrade image version is lower than the currently running RiOS version, an error is displayed. For details on supported upgrade paths, see "Requirements and prerequisite tasks prior to upgrading" on page 51.

Image download or installation failure

If a failure occurs during the image download or installation (prior to reboot), the download can be reattempted.

SteelHead SD installer failure

If a failure happens after the system has already booted to the SteelHead SD installer and the partitioning has been done, the appliance will have to be USB remanufactured. Contact Riverbed Support at https://support.riverbed.com.

Can't generate config error

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

DNS error

If a DNS for the URL is displayed, the uplink interface might be in the process of changing or updating the configuration; wait two or three minutes and retry.

Upgrade failed

1. If the appliance appears in SCM, but it says "upgrade failed," wait a few minutes, then choose Appliances > Overview.

2. Select the appliance and Actions > Retry Upgrade. This action triggers a download of the upgrade firmware and possible a reboot, if necessary. It typically clears the error.

If the appliance doesn't come online

Perform the following tasks:

1. Check network cabling.

2. Connect to the appliance via the console port using a serial cable (baud rate: 9600 bps). Log in as administrator user (**admin**) and enter the default password (**riverbedAlmanor**). Select the Troubleshooting menu option and view the boot status in cloud-init and console messages.

3. Verify network connectivity to transition IP addresses (static IP or DHCP) for uplink interfaces.

4. Reboot or restart using the **setupd** command.

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.

- If you have a successful HTTP status but an error is returned in the serial number query. This error means that the appliance isn't entitled for a SteelHead SD in-field upgrade because the SCC checks for entitlement status prior to the upgrade process. Typically, you only get into this state if you manually upgrade the software using the SteelHead Management Console. Contact Riverbed Support at https://support.riverbed.com.

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.

Cannot log in after converting the appliances

After upgrading, SteelHead SD appliances will be set to the default admin password (**password**). You must reconfigure the admin password for the virtual SteelHead and update the stored password on the SCC.

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" on page 71
- "SteelHead SD 3070-SD appliance specifications" on page 73

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
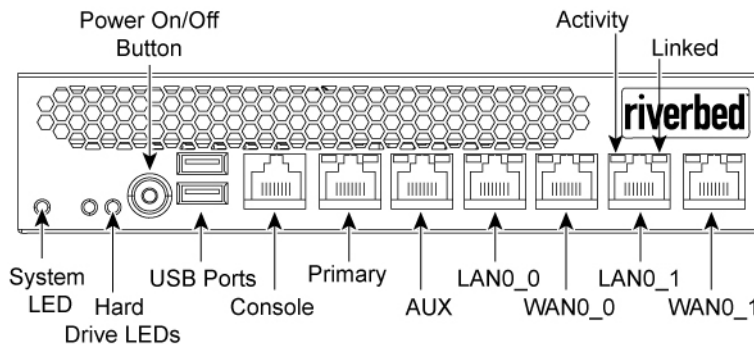
Figure A-2. Back panel
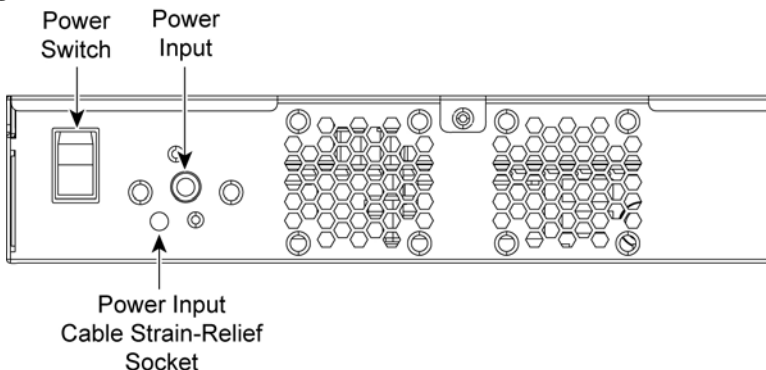
This table summarizes the system LEDs.

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.

Status lights and ports

Figure A-3. SteelHead SD 3070-SD appliance front panel with LEDs and buttons
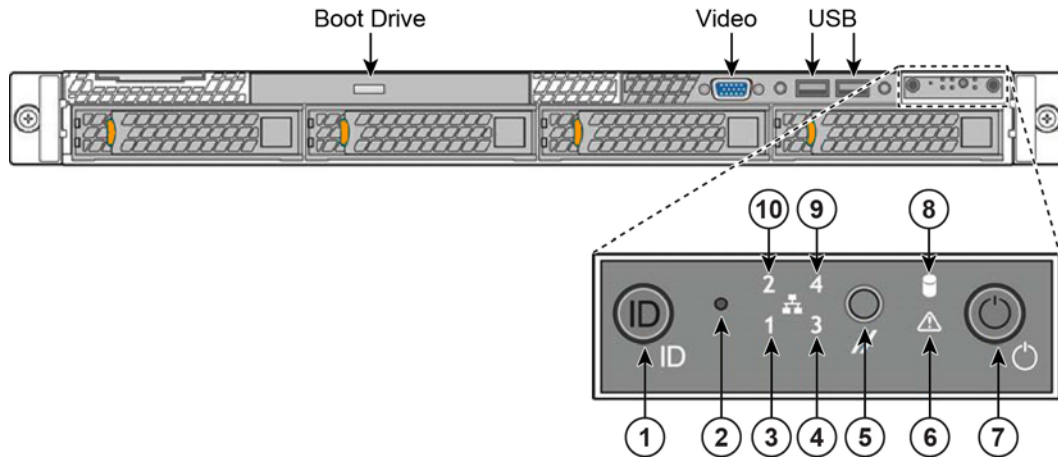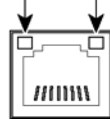
Figure A-4. SteelHead SD 3070-SD appliance back panel
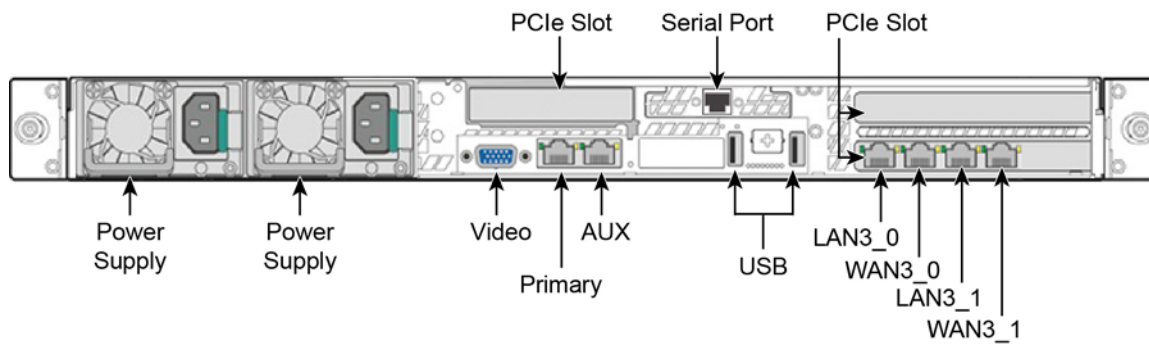
Note: On the SteelHead SD 3070-SD appliance, the appliance uses the NIC in slot 3 for the default interface names so the ports are labeled WAN3_0 and WAN3_1. If you ordered a custom NIC instead of the default NIC for the appliance, then the NIC is installed in slot 2 and your NIC ports will appear in 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 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 200-240 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 (10º-35ºC)
Temperature (storage)	-40º-158ºF (-40º-70ºC)
Relative humidity	50% to 90%, noncondensing with a maximum wet bulb of 28ºC (at temperatures from 25º to 35ºC)

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" on page 79
- "SteelHead SD 570-SD and 770-SD appliances" on page 80
- "SteelHead SD 3070-SD appliance" on page 81

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 software architecture, see "Introducing SteelHead SD" on page 11.

Figure 6-17. Port mapping between VMs and physical ports
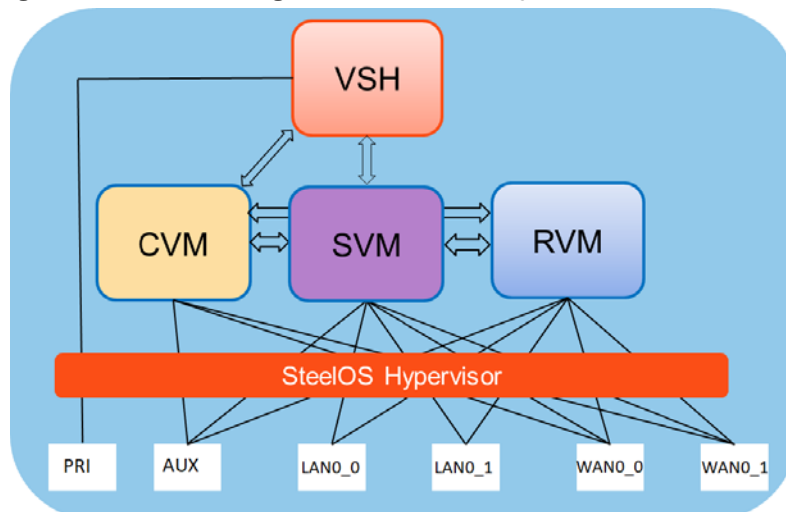
Note: The 3070-SD ports are LAN3_0, LAN3_1, WAN3_0, WAN3_1.

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

Node name	Interface name	Port
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_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 on add-on NICs, see "NIC support" on page 23.

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 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>.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.