riverbed

SteelHead™ SD Installation Guide

Version 1.0 (SteelConnect 2.5, RiOS 9.2.1-cf1)

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

November 2016

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

Part Number
712-00301-01

Contents

Welcome

Welcome to the *SteelHead SD Installation Guide*, Version 1.0 (SteelConnect 2.5/RiOS 9.2.1-cf1)**.** This guide describes how to install the Riverbed SteelHead SD (SteelHead SD).

Audience

This guide is written for storage and network administrators who are familiar with administering and managing WANs using common network protocols such as TCP, CIFS, HTTP, FTP, and NFS.

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)
- SteelHead (virtual edition) (vSH)
- SteelConnect Virtual Gateway (vGW)
- Steel Operating System (SteelOS)
- 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 http://www.riverbed.com/services/index.htm.
- **Documentation** - Have suggestions about Riverbed's online documentation or printed materials? Send comments to techpubs@riverbed.com.

1

SteelHead SD Overview

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

This guide describes how to install the manufactured SteelHead SD. It doesn't describe how to upgrade an existing SteelHead 570, 770, or 3070 to a SteelHead SD appliance. For details on upgrading SteelHead to SteelHead SD, see the *SteelHead SD In-Field Upgrade Guide*.

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

Introducing the SteelHead SD

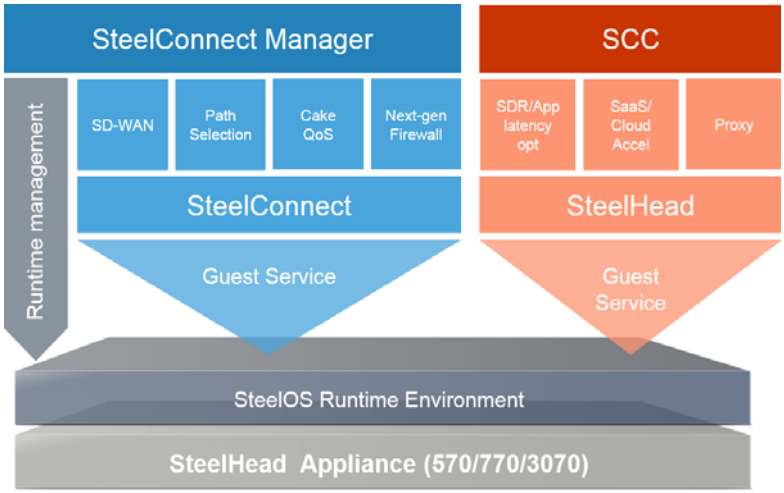
The SteelHead SD appliance integrates SD-WAN and WAN optimization services to identify and classify applications, enabling application-centric visibility and control across your hybrid WANs, cloud (SaaS, IaaS) networks, and branch LAN/WANs.

Three new models of SteelHead (570-SD, 770-SD, and 3070-SD) combine Riverbed WAN optimization, powered by RiOS, plus SD-WAN and cloud networking capabilities, powered by SteelConnect, delivered in a single appliance.

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.

Built on the same technology as the SteelHead, the SteelHead SD reduces bandwidth utilization and speeds up application delivery and performance while providing SteelConnect integration with the SteelOS run-time environment.

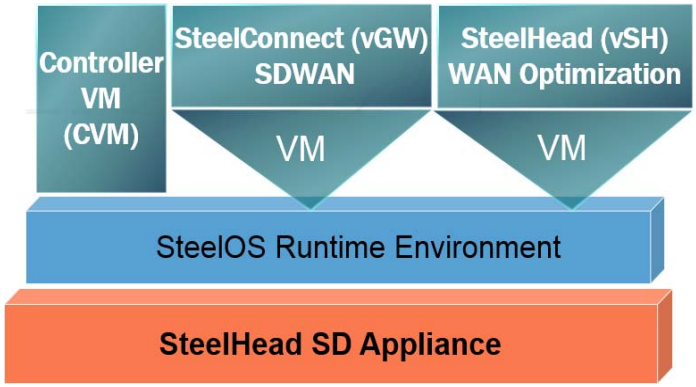
Figure 1-1. SteelHead SD architecture



SteelHead SD Services

The SteelHead SD is made up of the following services.

Figure 1-2. SteelHead SD services



SteelConnect SD-WAN service

SteelConnect Manager (SCM) handles the management and configuration of SD-WAN features. SCM connectivity requires AUX or one of the WAN ports that are used as uplink ports.

Only the SD-WAN service can be enabled or disabled via SCM. The WAN optimization service always remains enabled.

The SD-WAN service upgrades are managed via SCM. SCM pushes the new software version according to the schedule that you set up.

SD-WAN features require an SD-WAN subscription license. This license must be purchased prior to starting the conversion process.

For details about configuring SD-WAN features, see *SteelConnect Manager User Guide*.

SteelHead WAN optimization service

The SteelCentral Controller for SteelHead (SCC) or the SteelHead Management Console handles management and configuration of the WAN optimization features. Also, traditional 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.

The WAN optimization service runs a special RiOS image that can be upgraded or downgraded to RiOS versions via the SCC.

Note: The image used for SteelHead WAN optimization service VM is a special RiOS image that works only on SteelHead SD platforms. They are labeled SteelHead SD so that you can easily identify them. The standard virtual SteelHead images can't be used on the SteelHead SD appliance.

Controller virtual machine service

The controller virtual machine (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 the SCM, but if necessary, you can troubleshoot the SteelHead and SteelConnect gateway locally.

The CVM service pushes configurations to the SteelConnect virtual gateway and collects statistics and alarms from the virtual gateway.

The CVM has direct access to virtual gateway network APIs and handles USB bootstrapping.

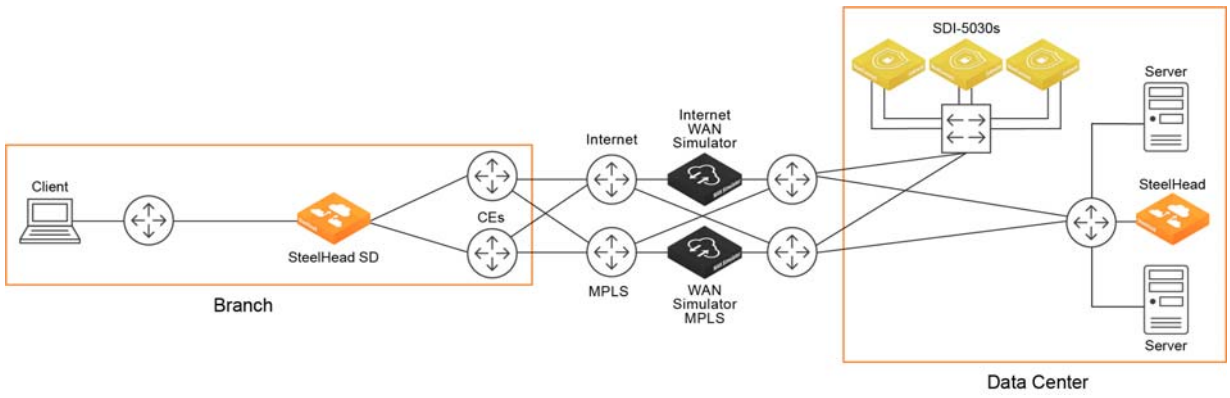
Deploying SteelHead SD

Typically, SteelHead SDs are located in the branch with SteelConnect SDI-5030s and a SteelHead located at the data center. Basically the SteelHead SD acts s an edge router that can perform WAN optimization.

The SteelHead SD supports only physical in-path and parallel High Availability (HA) deployments. Serial HA deployments are not supported.

The LAN interfaces are only accessible to the WAN optimization service and the WAN interfaces are only accessible to the SD-WAN service. All LAN traffic flows through SteelHead and RiOS first, and then it is passed through the virtual interface to the gateways. All WAN traffic flows through the SteelConnect gateway first, then it passes through the virtual interface to the WAN optimization service.

Figure 1-3. Typical single SteelHead SD deployment behind custom edge (CE) routers



Hardware and software dependencies

The SteelHead SD is comprised of the SteelHead WAN optimization and the SteelConnect SD-WAN services on a 570-SD, 770-SD, or 3070-SD appliance.

Riverbed component	Hardware and software requirements
SteelHead SD appliance	The 570-SD and 770-SD are desktop models. The 3070-SD requires a 19-inch (483 mm) four-post rack. For details, see the *Rack Installation Guide*.
SteelHead SD Management Console	The Management Console has been tested with all versions of Chrome, Mozilla Firefox Extended Support Release version 38, and Microsoft Internet Explorer 11. JavaScript and cookies must be enabled in your Web browser.
SteelConnect and SteelConnect Manager (SCM)	SteelHead SD requires SteelConnect 2.8.2 or later. If you already have SteelConnect, when you connect to the SCM it automatically upgrades your software using the schedule you have configured in the SCM. 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)	If you use the SCC to manage the WAN optimization service, you must have SCC 9.6.2 or later.

Network interface card support

The SteelHead SD supports these network interface cards (NICs) on the 3070-SD model. For details regarding installing additional NICs, see the *Network and Storage Card Installation Guide*.

NICs	Size (*)	Manufacturing Part #	Orderable Part #
Four-Port 1-GbE Copper Base-T	HHHL	410-00115-01	NIC-1-001G-4TX-BP
Two-Port 1-GbE Fiber SX	HHHL	410-00113-01	NIC-1-001G-2SX-BP
Four-Port 1-GbE Fiber SX	FHHL	410-00122-01	NIC-1-001G-4SX-BP
Two-Port 1-GbE Fiber LX	HHHL	410-00114-01	NIC-1-001G-2LX-BP
Four-Port 1-GbE Fiber LX	FHHL	410-00123-01	NIC-1-001G-4LX-BP
Two-Port 10-GbE Fiber SR	FHHL	410-00302-03	NIC-1-010G-2SR-BP
Two-Port 10-GbE Fiber LR	FHHL	410-00301-03	NIC-1-010G-2LR-BP

* HHHL = Half Height, Half Length, FHHL = Full Height, Half Length

Note: Although these are bypass NICs traditional to SteelHeads, bypass functionality isn't supported on the SteelHead SD.

Firewall requirements

Make sure the firewall ports 80 and 443 are open so that software installation and SCM operations aren't blocked.

Also, make sure firewall ports for FTP 20 and 21 are open so that the software installation doesn't block communication with hosts behind download.riverbed.com.

For details about firewalls for SCM, see the *SteelConnect Manager User Guide*.

Ethernet network compatibility

The SteelHead SD appliance supports these Ethernet networking standards.

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

SNMP-based management compatibility

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

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

Licensing

The SteelHead SD appliance requires licenses for the SteelConnect SD-WAN and SteelHead WAN optimization services.

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, you will receive two emails:

- The first email will have the license token, the SD-WAN SteelConnect gateway serial number, and the corresponding SteelHead SD serial number. After you upgrade the software, you redeem the token in the SCM and all hardware nodes and license keys are added to your organization. Each token is redeemable only once.
- The second email will have a link to the software image.

To redeem the SD-WAN service token

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

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/index.htm and follow the instructions for retrieving your licenses. The licensing portal requires a unique product 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.

Preparing your site for installation

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

Your site must meet these requirements:

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

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

Before you begin

- Make sure there is internet connectivity and the firewall ports 80 and 443 are open so that software installation and SCM operations are not blocked.
- Make sure the network provides a DHCP service so the appliance can establish a connection automatically.

2

Installing the SteelHead SD

This chapter describes how to install the SteelHead SD. It includes these sections:

The SteelHead SD appliance consists of the SteelHead WAN optimization service and the SteelConnect SD-WAN service through a gateway.

This chapter describes how to perform the initial installation for the SteelHead SD appliance. It doesn't provide detailed information about configuring and managing SD-WAN or WAN optimization features. For detailed information, see the *SteelConnect Manager User Guide* and the *SteelHead Management Console User's Guide*.

Configuring SteelHead SD using SteelConnect Manager

You use the SteelConnect cloud-based management system to install, configure, and manage the SteelHead SDs in your network. SteelConnect uses a zero-touch provisioning (ZTP) to install and manage your appliances, enabling you to configure and visualize the appliances in your network before you install and connect the hardware.

Using SteelConnect Manager (SCM), you perform the basic configuration of your network, register and connect the hardware, and configure the WAN optimization in-path settings to bring your SteelHead SD into production. This chapter describes these steps.

Defining an organization

SCM uses these terms to describe the network:

- **Organization** - A company representing an end customer. You can assign administrative rights to individual administrator accounts per organization. You can also manage appliances and licensing per organization.

- **Site** - A physical location of one or more office buildings, a hosting center, or a cloud location that make up the organization. A site houses a SteelConnect gateway and uses a permanent DNS alias. Every site requires a local network zone and at least one internet uplink. The zone is automatically created when you create a site.
- **Zone** - Layer 2 network segments or VLANs within sites that are VLAN-tagged traffic. A zone always has a VLAN tag assigned to it.

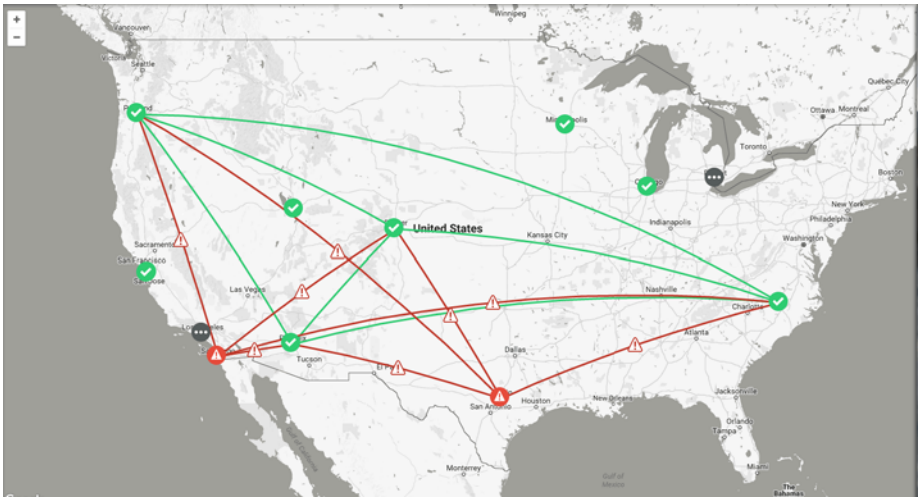
SCM is delivered with a default organization and site. You add your company name and basic information for your organization or change and customize this information later. For details about defining an organization, network, sites, zones, and uplinks, see the *SteelConnect Manager User Guide*.

To log in to SCM

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

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

Figure 2-1. SCM dashboard



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

To add sites

2. Choose Network Design > Sites.
3. Click **New Site** to expand the page.
4. Add a site tag: for example, headquarters.
5. Add the site's location: for example, San Francisco.
6. Type the site's address, country, and time zone.
7. Click **Submit**.

8. Repeat the steps for the remaining sites in your network topology.

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

Adding shadow appliances

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

To add shadow appliances

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

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

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

Registering appliances

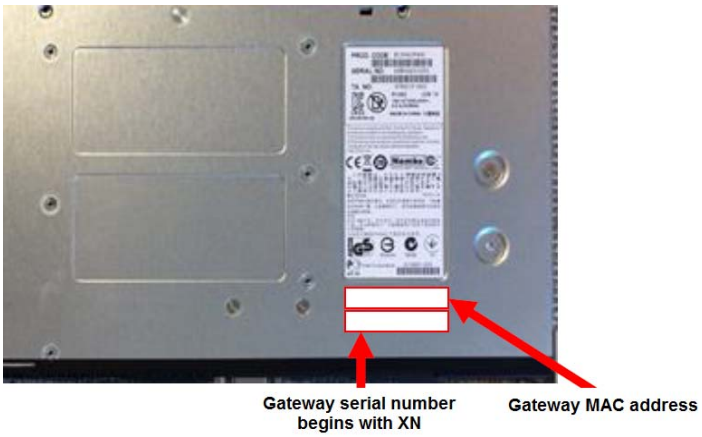
Next, you register the physical devices to transform them from shadow appliances into physical appliances using the SteelConnect gateway serial number.

For SteelHead appliances that are going through the conversion process, the SteelHead SD serial number is available in Riverbed email sent by Riverbed containing the SteelConnect serial number and token.

The SteelConnect serial number is also available on the appliance label. The SteelConnect gateway serial number always begins with the prefix XN. Find that serial number and MAC address on the appliance and write them down. (You will use the MAC address later in these procedures.)

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

Figure 2-2. 3070 SteelConnect gateway serial number and MAC address



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

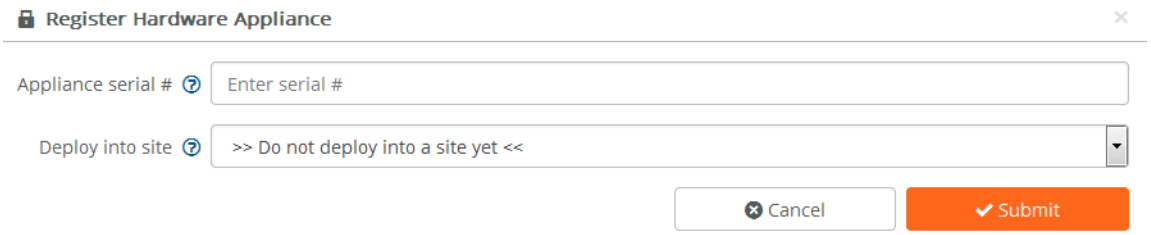
To register a hardware appliance

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

Figure 2-3. Example of a shadow appliance

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

Figure 2-4. Registering appliances



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

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

Configuring the zone uplink

Next, you verify the ports and configure the LAN zone uplinks. The LAN zone uplink is configured as a single-zone uplink for the SteelHead WAN optimization service.

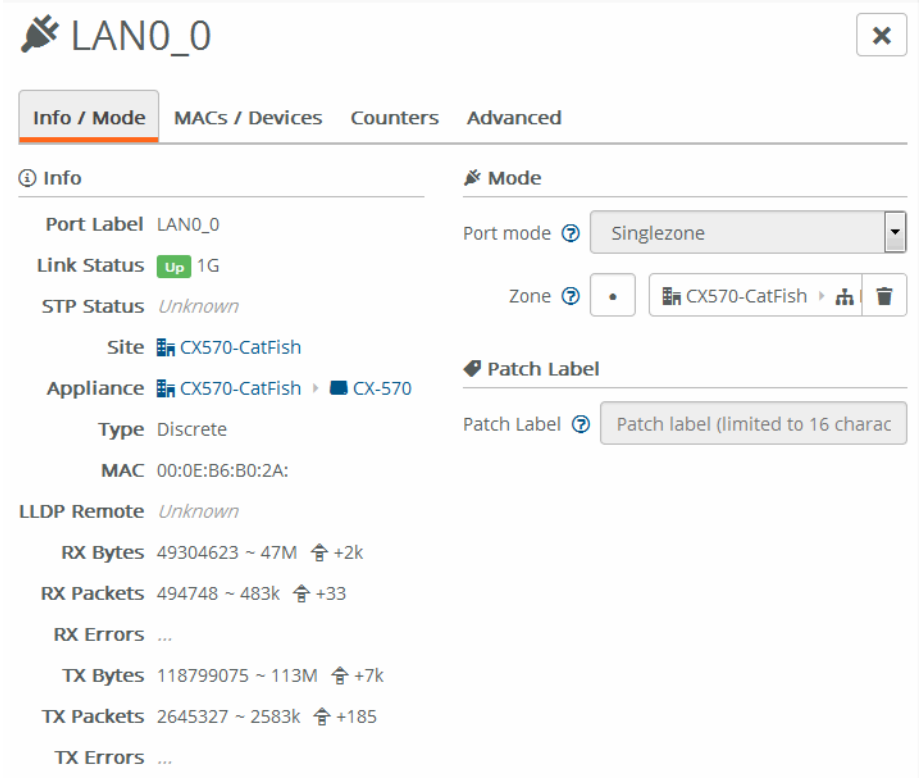
By default, the LAN port is disabled on the SteelHead SD appliances unless it is explicitly enabled. If you don't enable the LAN zone port of the gateway, SD-WAN won't see either the SteelHead WAN optimization service or the clients on the LAN side of the network.

To configure the zone uplink

1. Choose Ports and select the site and appliance from the drop-down list. The ports for the appliance are displayed.

2. Click the LAN port you want to configure to expand the page.

Figure 2-5. Configuring the zone port



3. Select Singlezone or Multizone for the Port mode.

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

5. Click **Submit**.

Next, you need to obtain the IP addresses for the in-path interface and gateway from SCM so that you can configure WAN optimization on the virtual SteelHead.

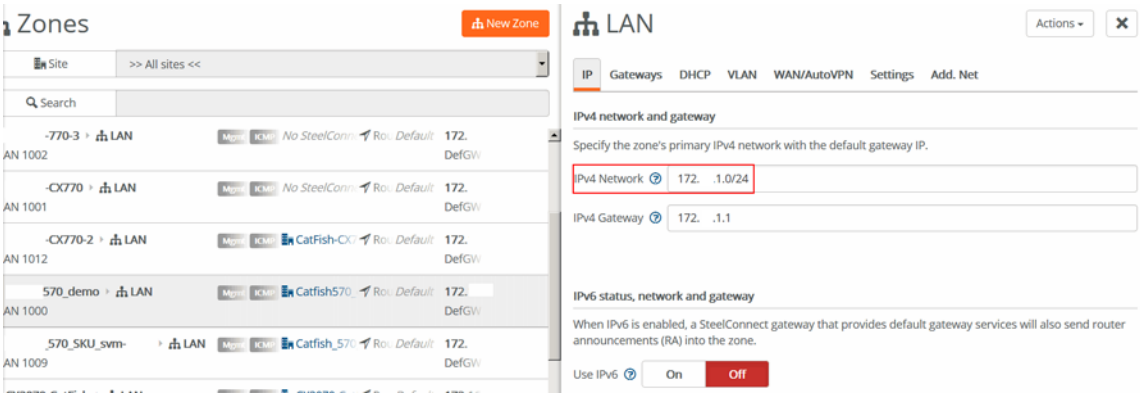
Obtaining the in-path interface IP address

You use the LAN-zone network IP address in SCM to configure the in-path interface on the virtual SteelHead.

To obtain the in-path interface IP address

1. In SCM, choose Network Design > Zones and select the device to expand the page.

Figure 2-6. Obtaining the LAN IP address for the in-path interface



   The LAN zone of the network is displayed under the IP tab. If the network IP address is 172.12.1.0/24, you can assign any IP address from 172.12.1.1 to 172.12.1.254 for the SteelHead in-path interface.

2. Write down the IP address. You will use this address when you configure the inpath0_0 interface for WAN optimization.

Next, you obtain the LAN-zone gateway IP address to configure the in-path gateway on the virtual SteelHead.

Obtaining the in-path gateway IP address

You use the LAN-zone gateway IP address in SCM to configure the in-path gateway on the SteelHead.

To obtain the in-path gateway IP address

1. To obtain the IP address for the default gateway, choose Appliances and select the device to expand the page.

2. Click the IPs tab.

Figure 2-7. Obtaining the IP address for the gateway

The in-path gateway IP address for the SteelHead is listed under the Zone gateway.

3. Write down the IP address. You will use address this when you configure the in-path gateway for the inpath0_0 interface for WAN optimization.

Cabling the SteelHead SD appliance

With the SteelHead SD, it is helpful to think of LAN ports as applying to virtual SteelHead optimization and WAN ports as applying to the SteelConnect virtual gateway. This framework will help you as you go forward in configuring the SteelHead SD.

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

- On the 570-SD or 770-SD, use a straight-through cable to connect either the WAN0_0 or WAN0_1 ports a WAN router with an internet uplink or an MPLS uplink for back-hauled internet traffic.
- On the 3070-SD, 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 break-out or via a data center over MPLS—whichever you prefer.

You cable the primary port to a DHCP reachable port on the switch.

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

WAN ports require an IP address as they will represent the uplink configuration. The SteelHead in-path interface must have an IP address and VLAN ID for the zone it is on.

Port definitions

For port locations see, Appendix A, “Appliance Technical Specifications.”

Port	Description
Primary	Preferably the primary port connects to a DHCP reachable port on a switch. The primary port is the management interface that enables you to connect to the SteelHead Management Console.
AUX	When the AUX port functions as an uplink, it is mapped to the virtual gateway. The AUX port can also be enabled as an additional WAN uplink in SCM for instances where a WAN port goes down. SteelHead services, such as datastore synchronization, aren’t supported on the AUX port. The AUX port can be used for parallel HA deployments, where the AUX port is an HA port. In HA deployments, the port is mapped to virtual SteelHead.
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 570-SD and 770-SDs, the default internet access port is WAN0_0 or WAN0_1. For 3070-SD, the default internet access port is WAN3_0 or WAN3_1. For details on 3070-SD NIC interface names, see “SteelHead SD 3070-SD specifications” on page 37.
LANX_X	Connect the LAN port to the LAN switch using a straight-through cable. For 570-SD and 770-SDs, the default port is LAN0_0 and LAN0_1. For 3070-SD, the default port is LAN3_0 or LAN3_1. For details on 3070-SD NIC interface names, see “SteelHead SD 3070-SD specifications” on page 37.
Console	Connects you to the controller virtual machine (CVM) using a serial cable. the 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 the SCM, but if necessary, you can troubleshoot the SteelHead and SteelConnect gateway locally. For details, see *SteelHead SD In-Field Upgrade Guide*.

Port mappings

For detailed information on port mappings, see Appendix B, “Port Mappings.”

Port mappings 570, 770

SteelHead SD	Interface
lan0_0 <-> wan0_0	inpath0_0
lan0_1 <-> wan0_1	inpath1_0

Port mappings 3070

The 3070-SDI has three NIC slots. The 3070-SDI ships with the NIC in slot three. If there are no NICs in slot 2, lan3_0 becomes inpath0_0 and the numbering starts from there. The port naming auto-adjusts depending on the interfaces present as the 3070 supports either 2-port or 4-port NICs in slot 2 and slot 3. The in-path naming always starts from inpath0_0.

SteelHead SD	Interface
lan2_0 <-> wan2_0	inpath0_0
lan2_1 <-> wan2_1	inpath1_0
lan3_0 <-> wan3_0	inpath2_0
lan3_1 <-> wan3_1	inpath4-0

Cabling the appliance

This section describes how to cable the appliance.

To cable the SteelHead SD

1. Plug the straight-through cable into the primary port to a DHCP reachable port on the switch. This must be a DHCP port that connects to a DHCP server.

Figure 2-8. Connecting the Primary port to the LAN switch

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

Figure 2-9. 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 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 connect either the WAN3_0 or WAN3_1 port to a WAN router. Internet reachability can be via a local break-out or via a data center over MPLS.

Figure 2-10. Connecting the WAN port to the WAN router

Identifying the primary IP address for the SteelHead

There are three ways to identify the primary IP address of the SteelHead:

- **When SteelConnect acts as the DHCP server** - You can set the SteelConnect virtual gateway to act as a DHCP server and identify the primary IP address for the SteelHead in the SCM. With no DHCP server, the SteelHead primary IP address gets preserved through the conversion process to be used by the SteelHead SD default uplink to connect to SCM.
- **When the SCC is used to manage SteelHeads** - If you're using the SCC to manage the WAN optimization service, you can obtain the primary IP address for each device in your network. SCC automatically registers all SteelHeads it detects in your network and provides the IP address for each in the Appliances page. For details on connecting to SCC, see the *SteelCentral Controller for SteelHead User's Guide*.
- **When an external server acts as the DHCP server** - Obtain the MAC address from the appliance and search for the primary IP address on the DHCP server console. You can find the MAC address on the appliance label (see Figure 2-2) or you can view it in SCM. To view the MAC address in SCM, choose Ports and select the Primary port for the device. The MAC address is listed under the Info-Mode tab.

Configuring SteelConnect to act as DHCP server

In this example the SteelHead LAN and primary ports are connected to same switch and the SteelConnect gateway acts as the DHCP server providing the primary IP address to of SteelHead.

To configure SteelConnect to act as a DHCP server

1. When you cable the SteelHead appliance, make sure you connect the LAN port and Primary port to the same switch.

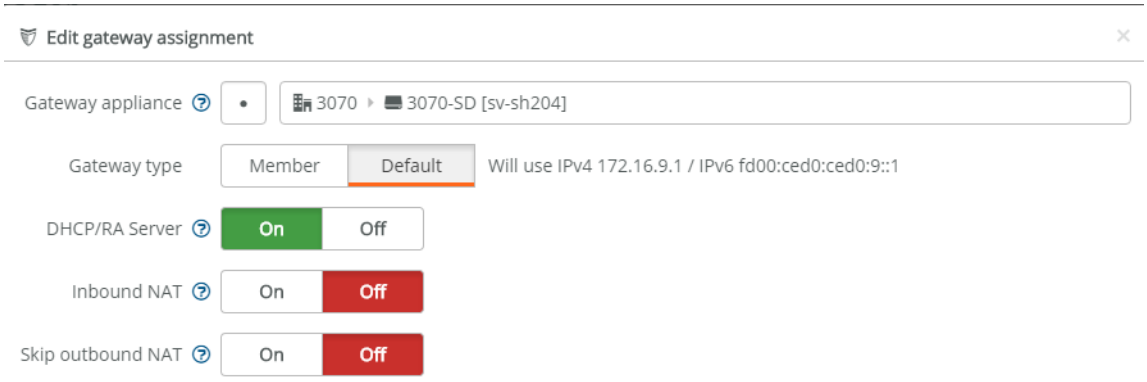
2. To set the gateway to act as a DHCP server, choose Networks Design > Zones and click the Gateways tab.

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

Figure 2-11. Editing the gateway to act as the DHCP server

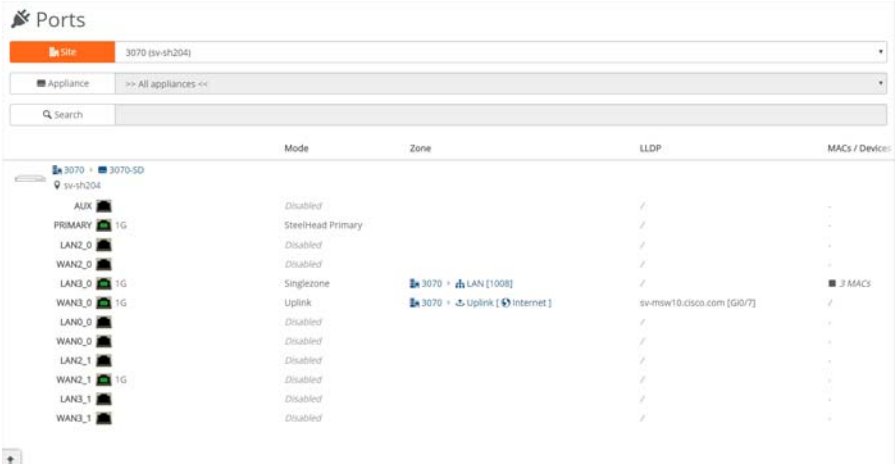
4. Make sure the DHCP/RA Server is on. (It will be green.)

Figure 2-12. DHCP/RA server is on



5. Choose Network Design > Ports to associate the LAN port to the appropriate Zone.

Figure 2-13. Associating the LAN port



6. There are two ways to connect: one is through the switch and other is back-to-back:
   - **Through the switch** - Connect the LAN port and Primary port to the switch port and configure in the same VLAN.
   - **Back-Back** - Connect the LAN port directly to the Primary port.

7. To identify the primary IP address for the SteelHead, choose Visibility > DHCP Leases:
   - The MAC address/IP address will be available for the Primary port.
   - In the figure below, the primary IP address is 172.16.9.254.

Figure 2-14. DHCP leases showing the primary IP address

Configuring the WAN optimization service in the SteelHead

Next, you configure the WAN optimization service in the SteelHead. To enable the WAN optimization service in the virtual SteelHead, you need to configure the in-path interface and the default gateway.

You will need the following information to configure the in-path interface and default gateway so that you can optimize traffic:

- **MAC address** - If you are not using the SteelCentral Controller for SteelHead (SCC) to manage your appliances, you will need the MAC address to find the primary IP address of the SteelHead on a DHCP server.
- **SCM LAN-zone IP address** - The LAN-zone IP address provides you with the IP address for the in-path interface. For details, see “To obtain the in-path interface IP address” on page 22.

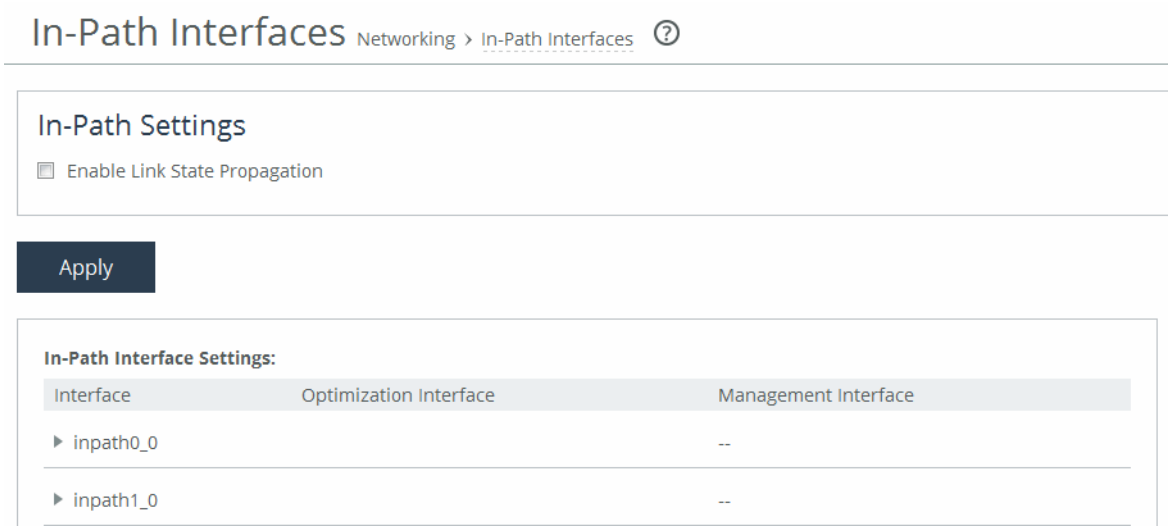
- **SCM zone gateway IP address** - The zone gateway for the device provides you with the IP address for the default gateway for the in-path interface. For details, see "To obtain the in-path gateway IP address" on page 22.

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

1. Using the Primary IP address you obtained from SCC or the DHCP server, enter it in the location box of your web browser using HTTPS. The sign in page for the SteelHead Management Console is displayed.
2. Specify the default user login (*admin*) and password (*password*).

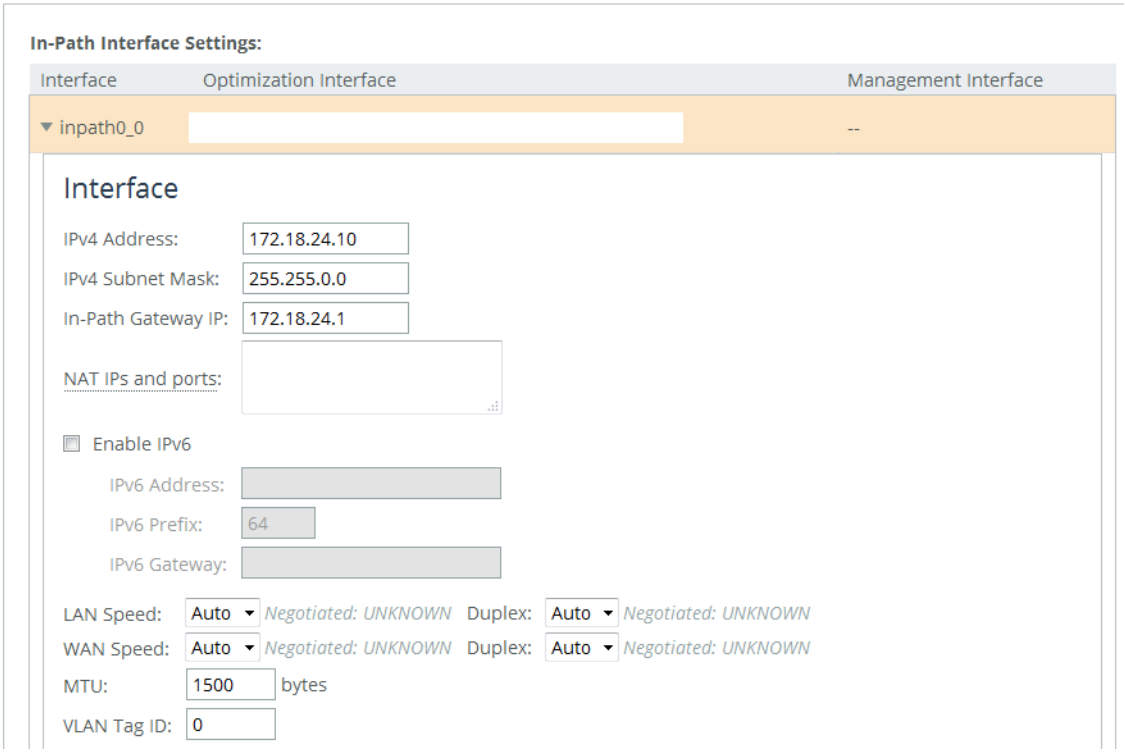
   For detailed information about monitor users and role-based management users, see the *SteelHead Management Console User's Guide*.
3. Click **Sign In** to display the Dashboard.
4. Choose Networks > Networking: In-Path Interfaces.

Figure 2-15. In-Path Interfaces page



5. Select the interface to expand the page.

Figure 2-16. Configuring the in-path interface



6. Type the IP address that you obtained from SCC. For details, see “Obtaining the in-path gateway IP address” on page 22.

7. Type the subnet mask address. The subnet mask on the in-path, must match the subnet mask on the zone (typically, /24, but it can be whatever you specified in the zone settings).

8. Type the IP address that you obtained in SCM for the default gateway. For details, see “Obtaining the in-path gateway IP address” on page 22.

9. Click **Apply**.

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

11. If you have not already done so, return to SCM and complete your gateway configuration. For details, see the *SteelConnect Manager User Guide*.

Provisioning a SteelHead SD without a DHCP server using a USB drive

Adding SteelHead SD to your network requires the appliance to contact the SteelConnect Manager, which provides the initial configuration. In a scenario where no DHCP server is available in the existing network, you can use offline provisioning.

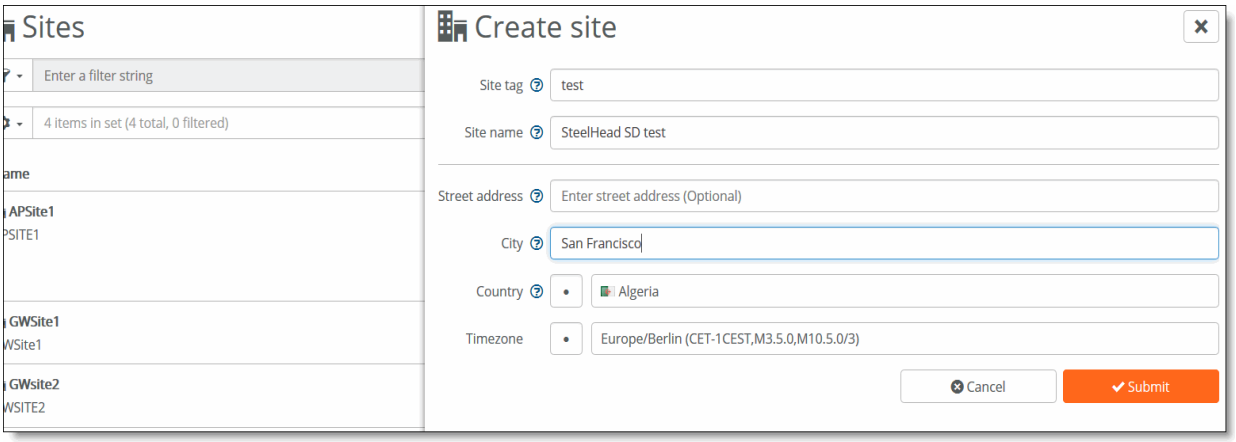
You can set up the configuration on SCM, even if the SteelHead SD is currently not present at the related site.

You'll need the serial number of the SteelHead SD to create an offline provisioning configuration file.

To provision a SteelHead SD without a DHCP server

1. Log in to SteelConnect Manager.
2. Choose Network Design > Sites > Add Site(s) > New site.
3. Specify at least the site tag, name, and city.
4. Click **Submit**.

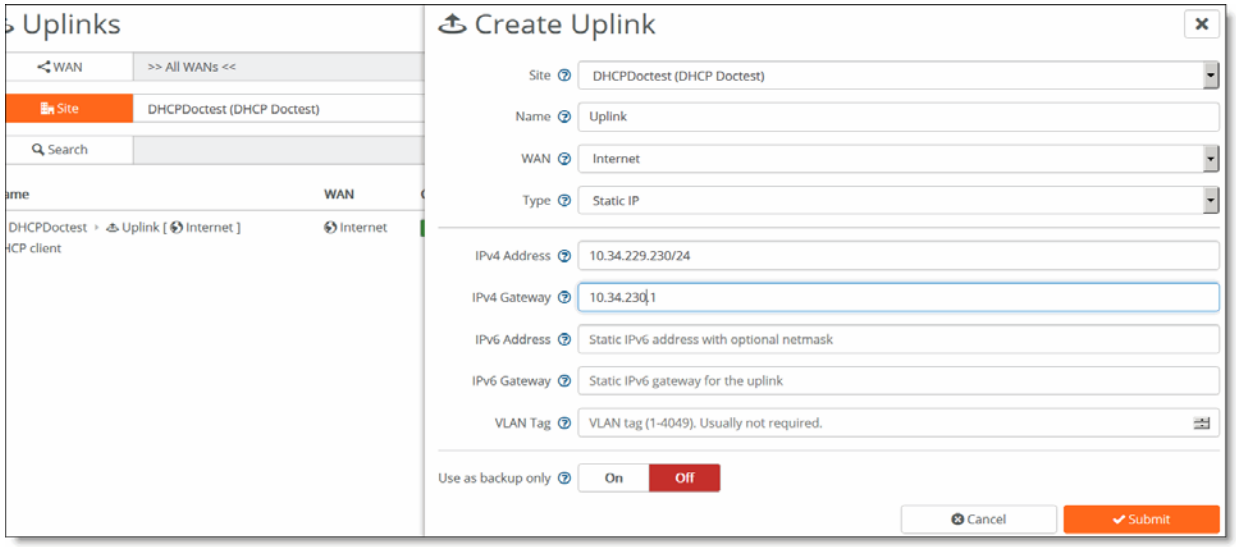
Figure 2-17. Creating a site



5. Choose Network Design > Uplinks and click **New Uplink**.
6. Select the uplink for the new site to expand the page.
7. Select Type and select Static IP from the drop-down list.
8. Specify the IP address using this format x.x.x.x/xx.
9. Specify a valid gateway address for the static IP uplink.

10. Click **Submit**. Repeat these steps for additional uplinks.

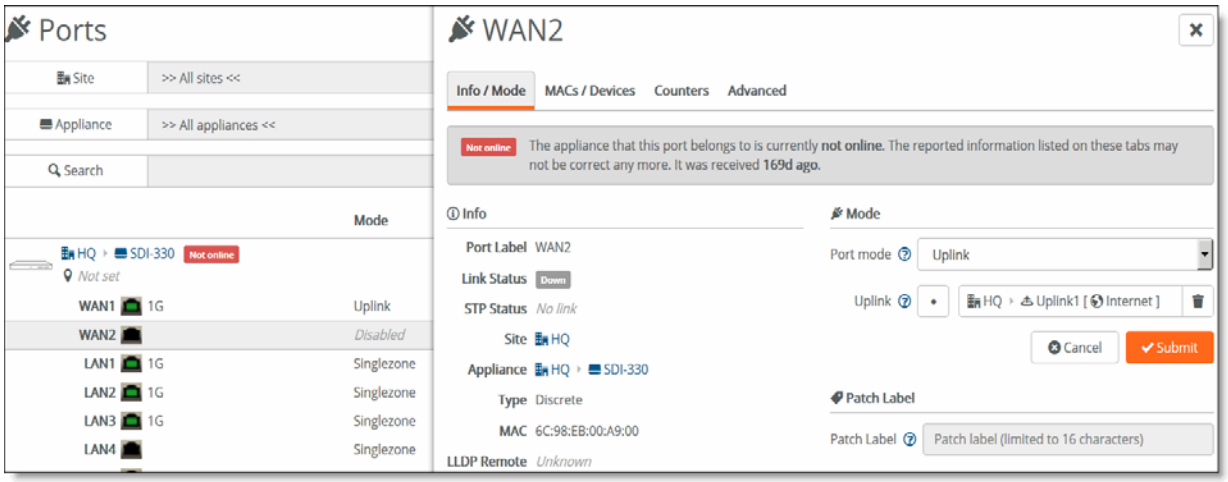
Figure 2-18. Creating a static IP uplink



To assign uplinks to the WAN ports of the appliance

1. Choose Ports > Sites and select the site you just created.
2. Under Appliances, select the SteelHead SD appliance to display the ports.
3. Select the WAN port you want to assign the uplink to. The page expands to display the port information.
4. Under Info/Mode tab, select Port Mode > Uplink and select the Static IP uplink from the drop-down list.
5. Click **Submit**. The WAN port will display the uplink you assigned to it.

Figure 2-19. Assigning the uplink to the WAN port



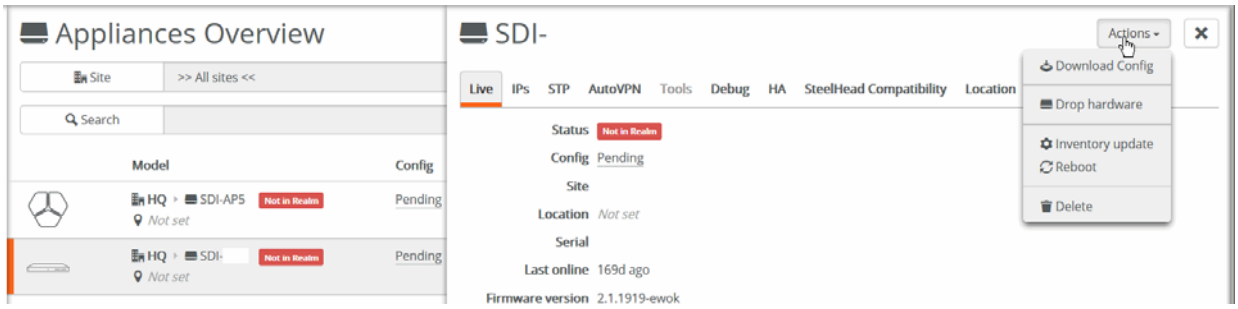
Now you are ready to download the configuration file (config file). Adhere to these guidelines:

- Wait for at least five minutes before downloading the config file to ensure that you are downloading the updated configuration.
- Do not modify the config filename.
- The USB stick must be in the ext3 or ext4 format, and starting in v2.11 can be in FAT32 format. If your USB has a different format, there are numerous instructions on the internet describing how to format a USB with ext3.
- Make sure you have all the sites and LAN/WAN ports configured with the appropriate sites, zones, and uplinks before you download the config file from the SCM.

To download the config file to the USB stick

1. Choose Appliances > Add Appliances > Register Hardware Appliance.
2. Enter the serial number of the SteelHead SD and select the site you want to deploy the appliance.
3. Select the new SteelHead SD, and click **Actions**, and select Download config from the drop-down list.

Figure 2-20. Downloading the config file



The system downloads a configuration file (config file) named with the SteelHead SD serial number. The config file is downloaded to your laptop or computer, the default location will be depend on your browser settings.

4. Copy the config file to the root directory of the first partition on a FAT32 or ext3 formatted USB drive. If your USB has a different format, there are numerous instructions on the internet describing how to format a USB.
5. Deploy the SteelHead SD on the site and power on the appliance. Wait at least 30 seconds until the new appliance powers up correctly before plugging in the USB stick.
6. Plug in the USB stick to install the configuration setting in the config file. The SteelHead SD connects to SCM with the configuration.
7. Perform a factory_reset.sh on the hypervisor after putting in the USB drive.
8. Reboot the SteelHead SD.

Next steps

After you have configured and installed the SteelHead SD appliance, refer to the *SteelConnect Manager User Guide* and the *SteelHead Management Console User's Guide* to fine tune your SD-WAN and WAN optimization features.

A

Appliance Technical Specifications

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

SteelHead SD 570-SD and 770-SD specifications

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

Status lights and ports

Figure A-1. Front panel

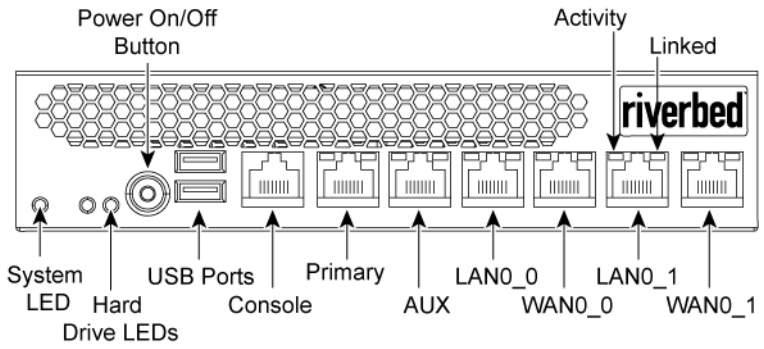
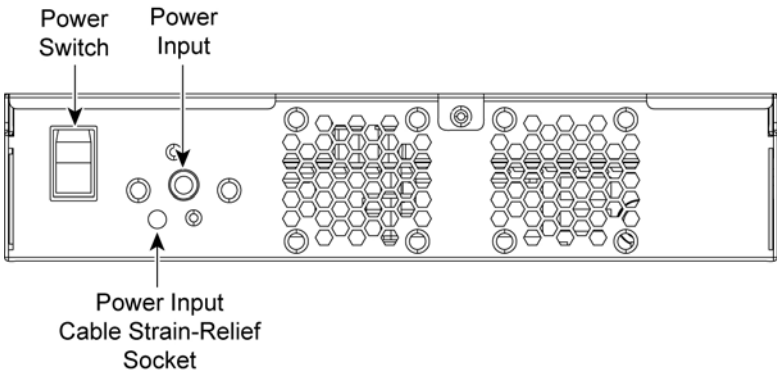


Figure A-2. Back panel



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. The SteelHead SD supports all available network interface cards (NICs) for the 570-SD and 770-SD. For details, see the *Network and Storage Card Installation Guide*.

Specification	570-SD desktop L-M-H	770-SD desktop L-M-H
Power (typical)	45 W	50 W
VA (max)	63.8	66.8
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 8x 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	100-240V 50-60 Hz	100-240V 50-60 Hz
PSU	Single 84 W External 100-240Vac, 50/60Hz, 2-1 A	Single 84 W External 100-240Vac, 50/60Hz, 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-45º C 32º-113º F	0º-45º C 32º—113º F
Temperature (storage)	-40º-65º C -40º-149º F	-40º-65º C -40º—149º F
Relative humidity	20%-80% noncondensing	20%-80% noncondensing
Storage humidity	5%-95% noncondensing	5%-95% noncondensing

SteelHead SD 3070-SD specifications

This section describes the status lights, ports, technical and environmental specifications. The SteelHead SD supports all available network interface cards (NICs) for the 3070-SD. For details, see the *Network and Storage Card Installation Guide*.

Status lights and ports

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

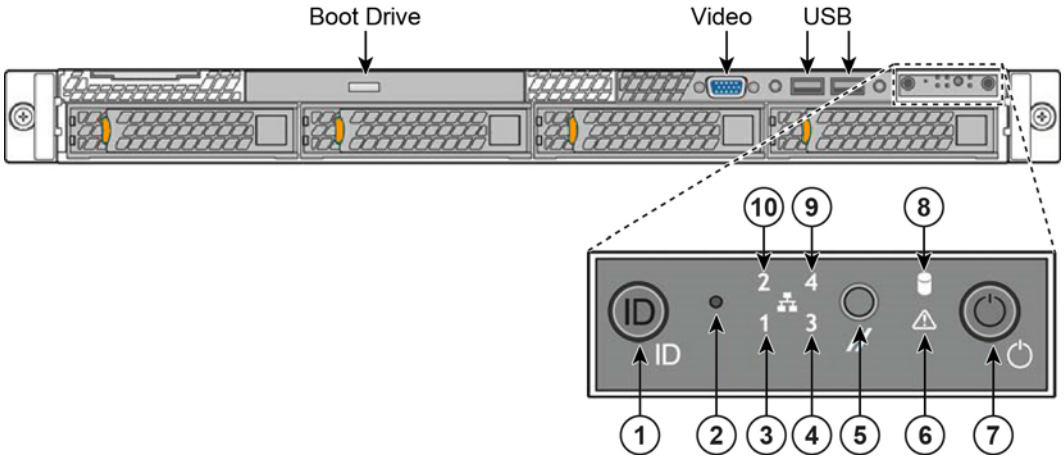
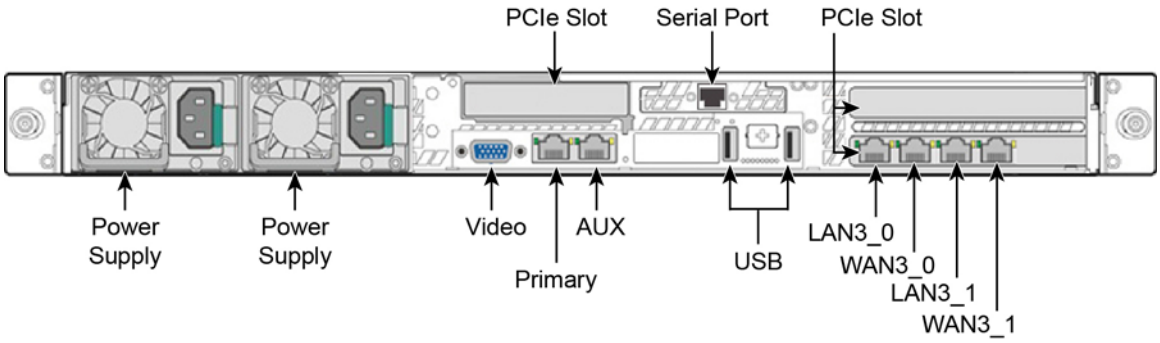


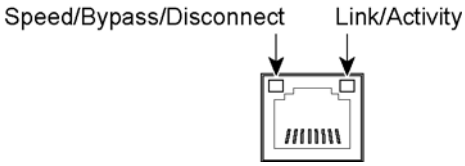
Figure A-4. 3070-SD back panel



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

This table summarizes the appliance LEDs and buttons.

Reference	LED/button	Description
1	System ID Button with Integrated LED	Maintenance = Blue Toggles the integrated ID LED and the blue server board ID LED on and off. The System ID LED identifies the system for maintenance when installed in a rack of similar server systems. You can also remotely turn on and turn off the System ID LED using the IPMI "Chassis Identify" command, which causes the LED to blink for 15 seconds. A duplicate System ID LED is on the back of the appliance to the left of the video port.
2	NMI Button	Pressing the NMI button puts the appliance in a halt state and issues a nonmaskable interrupt (NMI). This helps when performing diagnostics for a given issue where a memory download is necessary to determine the cause of the problem. To prevent an inadvertent system halt, the NMI button is located behind the front control panel faceplate and is only accessible with the use of a small tipped tool such as a pin or paper clip.
3 10	Network Activity LED Primary Auxiliary	Link = Green Activity = Blinks Green. The blink rate is consistent with the amount of network activity. The appliance doesn't use the LEDs 4 and 9.
5	System Cold Reset Button	Pressing this button reboots the appliance.
6	System Status LED	The System Status LED shows the current health of the server system. Healthy = Green Degraded = Yellow Critical = Blinks Yellow A duplicate System ID LED is on the back of the appliance to the right of the AUX port.
7	Power Button with Integrated LED	System On = Green System Off = No Light
8	Drive Activity	Activity = Blinks Green
	LEDs on Disk Drives	**Activity LED** Read/Write Activity = Blinks Green **Disk Fault LED** Failed Disk = Orange RAID Rebuild = Blinks Orange
	LEDs on Primary and AUX Ports	**Left LED** Link = Green Activity = Blinks Green **Right LED** 10 MB/sec data rate = No Light (with link on left LED) 100 MB/sec data rate = Green 1000 MB/sec 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** 1000Mbit/s = Yellow 100Mbit/s = Green 10Mbit/s = 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	100-127V, 200-240V
PSU	2 x 450 W 100-127Vac/8A, 50/60Hz 200-240Vac/4A, 50/60Hz
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	.76
Max. watts	152.8	145.4
Typical watts	122	116
Max VA	154	147
Power factor	98.96	99.16
BTU (typical)	417	397

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)	10º-35º C (50°-95 F
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

Port Mappings

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

Models 570-SD and 770-SD

Physical ports

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

- Aux, Primary, lan0_0, wan0_0, lan0_1, wan0_1

Controller virtual machine (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

Virtual SteelHead (VSH) ports

The VSH has these ports:

- Primary, Aux, lan0_0, wan0_0, inpath0_0, lan1_0, wan1_0, inpath1_0

VSH external port to VSH internal port to flows port mapping

VSH internal port	Primary	AUX	LAN0_0	WAN0_0	LAN1_0	WAN1_0
VSH external port (as seen in hypervisor)	tap1_0	tap1_1	tap1_2	tap1_3	tap1_4	tap1_5
Flows port	14	15	16	17	18	19

Virtual gateway (VGW) ports

The VGW has these ports:

- eth0, eth1, eth2, eth3, eth4

VGW external port to VGW internal port to flows port mapping:

VGW internal port	eth0	eth1	eth2	eth3	eth4
VGW external port (as seen in hypervisor)	tap2_0	tap2_1	tap2_2	tap2_3	tap2_4
Flows port	N/A	20	21	22	23

Note: tap2_0 is added linklocal_br which connects to CVM. This contains the IP 169.254.0.5 in the VGW and it is used for sending core and SCM through the CVM proxy.

Port mapping

These port mappings apply only if you have installed an add-on NIC.

Port mapping	Flows port mapping	Comments
VSH Primary <---> Physical Primary	14 <---> 9	Default filter 15
VSH AUX <---> N/A		Not connected externally
VSH lan0_0 <---> Physical lan0_0	16 <---> 10	Default filter 15
VSH lan1_0 <---> Physical lan0_1	18 <---> 12	Default filter 15
VSH wan0_0 <---> VGW eth1	17 <---> 20	Default filter 15
VSH wan1_0 <---> VGW eth2	19 <---> 21	Default filter 15
(knet5, VGW eth3 <---> Physical wan0_0	(5,22) <---> 11	Diverter
(knet7, VGW eth4) <---> Physical wan0_1	(7, 23) <---> 13	Diverter

Model 3070-SD

Physical ports

The 3070-SD has these physical ports:

- Aux, Primary, lan3_0, wan3_0, lan3_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

VSH ports

The VSH has these ports:

- Primary, Aux, lan0_0, wan0_0, inpath0_0, lan1_0, wan1_0, inpath1_0, lan2_0, wan2_0, inpath2_0, lan3_0, wan3_0, inpath3_0

VGW ports

The VGW has these ports:

- eth0, eth1, eth2, eth3, eth4, eth5, eth6, eth7, eth8

Port name to flows port mapping

Port mapping	Flows port mapping	Comments
Aux	12	
Primary	13	
LAN2_0	14	Present with an add-on NIC only.
WAN2_0	15	Present with an add-on NIC only.
LAN2_1	16	Present with an add-on NIC only.
WAN2_1	17	Present with an add-on NIC only.
LAN3_0	18	
WAN3_0	19	
LAN3_1	20	
WAN3_1	21	
VSH Primary <----> tap1_0	22	All tap ports are VM port projects in the hypervisor
VSH Aux <----> tap1_1	23	
VSH lan0_0 <----> tap1_2	24	
VSH wan0_0 <----> tap1_3	25	
VSH lan1_0 <----> tap1_4	26	
VSH wan1_0 <----> tap1_5	27	
VSH lan2_0 <----> tap1_6	28	
VSH wan2_0 <----> tap1_7	29	
VSH lan3_0 <----> tap1_8	30	
VSH wan3_0 <----> tap1_9	31	
VGW eth0 <----> tap2_0	N/A	This is added into linklocal_br in the hypervisor
VGW eth1 <----> tap2_1	32	
VGW eth2 <----> tap2_2	33	
VGW eth3 <----> tap2_3	34	
VGW eth4 <----> tap2_4	35	
VGW eth5 <----> tap2_5	36	
VGW eth6 <----> tap2_6	37	

Port mapping	Flows port mapping	Comments
VGW eth7 <----> tap2_7	38	
VGW eth8 <----> tap2_8	39	

Note: tap2_0 is added linklocal_br which connects to CVM. This contains the IP 169.254.0.5 in the VGW and it is used for sending core and SCM through the CVM proxy.

Port mapping

These port mappings apply only if you have installed an add-on NIC.

Port mapping	Flows port mapping	Comments
VSH Primary <---> Physical Primary	22 <---> 13	Default filter 15
VSH AUX <---> N/A		Not connected externally
VSH lan0_0 <---> Physical lan2_0	24 <---> 14	Default filter 15
VSH lan1_0 <---> Physical lan2_1	26 <---> 16	Default filter 15
VSH lan2_0 <---> Physical lan3_0	28 <---> 18	Default filter 15
VSH lan3_0 <---> Physical lan3_1	30 <---> 20	Default filter 15
VSH wan0_0 <---> VGW eth1	25 <---> 32	Default filter 15
VSH wan1_0 <---> VGW eth2	27 <---> 33	Default filter 15
VSH wan2_0 <---> VGW eth3	29 <---> 34	Default filter 15
VSH wan3_0 <---> VGW eth4	31 <---> 35	Default filter 15
(knet5, VGW eth5) <---> Physical wan2_0	(5,36) <---> 15	Diverter
(knet7, VGW eth6) <---> Physical wan2_1	(7, 37) <---> 17	Diverter
(knet9, VGW eth7) <---> Physical wan3_0	(9, 38) <---> 19	Diverter
(knet11, VGW eth8) <---> Physical wan3_1	(11, 39) <---> 21	Diverter

C

SteelConnect Connection Ports

Ports used by SteelConnect for inbound, outbound, and SSH 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

Service	Protocol	Default port	Destination
SteelHead SD and SDI-5030 Firmware Download	TCP	80/443	download.riverbed.com
FTP	TCP	20/21	ftp.riverbed.com

Inbound/outbound connections

Service	Protocol	Default port	Destination
AutoVPN	UDP	500/4500	Any

Tunneled SSH client connections

Service	Protocol	Default port	Destination
SSH proxy	TCP	3903	<hostname>.riverbed.cc -or- <hostname>.ocedo.cc
Workstation	TCP	3903	<hostname>.riverbed.cc -or- <hostname>.ocedo.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.