SteelHead® Installation and Configuration Guide

SteelHead® DX Appliance

Version 9.0

November 2014

riverbed®

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: http://www.riverbed.com

Part Number
712-00207-02

Contents

Preface

Welcome to the *SteelHead Installation and Configuration Guide*. Read this preface for an overview of the information provided in this guide and for an understanding of the documentation conventions used throughout. This preface includes the following sections:

About This Guide

The *SteelHead Installation and Configuration Guide* describes how to install and configure the SteelHead DX. It also describes the status lights and specifications for the system.

This guide is intended to be used with the following documentation:

- *SteelHead Management Console User's Guide* for SteelHead EXs (includes RiOS, Granite Edge, and VSP information)
- *SteelHead Deployment Guide* (for SteelHead EX deployment scenarios)
- *Granite Core Installation and Configuration Guide*
- *Granite Core and Edge Deployment Guide* (for Granite Core and Granite Edge deployment scenarios)
- *Granite Core Getting Started Guide*
- *Granite Core Management Console User's Guide*

Audience

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

Document Conventions

This manual uses the following standard set of typographical conventions to introduce new terms, illustrate screen displays, describe command syntax, and so forth.

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

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

< >	Values that you specify appear in angle brackets: **interface <ip-address>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]**
{ }	Elements that are part of a required choice appear in braces: **{<interface-name> | ascii <string> | hex <string>}**
|	The pipe symbol represents a choice to select one keyword or variable to the left or right of the symbol. The keyword or variable can be either optional or required: **{delete <filename> | upload <filename>}**

Documentation and Release Notes

To obtain the most current version of all Riverbed documentation, go to the Riverbed Support site at https://support.riverbed.com.

If you need more information, 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 identify new features in the software as well as known 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.

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 do not clearly understand the safety information provided in the product documentation.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - If you have 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** - Riverbed has a staff of professionals who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services, email proserve@riverbed.com or go to http://www.riverbed.com/services-training/Services-Training.html.
- **Documentation** - The Riverbed Technical Publications team continually strives to improve the quality and usability of Riverbed documentation. Riverbed appreciates any suggestions you might have about its online documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

CHAPTER 1 Product Overview

This chapter provides an overview of common terms, new features, upgrade instructions, technical and environmental specifications, and a description of the status lights for the system. It includes the following sections:

New Features in Version 9.0

This section provides an overview of the new features available in RiOS v9.0. For details, see the *SteelHead Management Console User's Guide*, the *SteelHead Deployment Guide*, the *SteelHead Deployment Guide - Protocols*, the *Riverbed Command-Line Interface Reference Manual*, the *SteelCentral Controller for SteelHead User's Guide*, and the *SteelCentral Controller for SteelHead Deployment Guide*.

- **Hybrid Network Topology, Application, and Site Definitions** - Changes the way you define and interact with applications and traffic by introducing the concept of network topology and applications to facilitate SteelHead configuration. The criteria used to identify traffic flows into networks, sites, and applications are now reusable. For example, you define a network topology once and then reuse it as needed on other SteelHeads. The network, site, and application definitions provide important building blocks for path selection, QoS, and secure transport, as these features have site-dependent rules.
- **Streamlined QoS Configuration** - Simplifies QoS configuration and leverages the previous basic QoS model with the added ability to create custom QoS profiles and classes on a per-site exception basis. This improved QoS user interface includes an easy-to-use QoS class hierarchy editor.
- **Enhanced Inbound QoS** - Enables configuration of path selection for inbound QoS as well as outbound QoS, and sets the same level of policies for both. Inbound QoS now supports QoS classes.
- **Automatic QoS Migration** - Automatically migrates a v8.x or v8.6.x QoS configuration to the v9.0 configuration model. The migration helps streamline upgrades to a new RiOS version. The v9.0 configuration model includes some notable changes compared to previous RiOS versions.

- **Redesigned User Experience, New Dashboard, and Streamlined Work Flows** - Improves configuration work flows, usability, and readability. The new design refreshes the SteelHead Management Console with these changes and more:
  - The Home page is now called the Dashboard. The new Dashboard highlights the product name, appliance name, and appliance health status along with the optimized throughput and bandwidth optimization statistics.
  - The previous cascading, hierarchical menu structure is now flat to provide easier navigation. This new structure also makes specific content more accessible.
  - The new UI design focuses on the minimalist use of common controls, typography, and flat colors for better readability and attractiveness.
- **Improved User Permissions Page** - Includes permission for all other RBM roles and permission to perform appliance administration, minimizing the need to assign an administrator role that grants full read-write access to all areas of the appliance. The page now merges the capability-based and role-based user tables into one Accounts table. In addition, the default user setting has been relocated from the General Security Settings page to the User Permissions page.
- **Improved TCP Dump Diagnostic Tool** - Includes a more resilient SNAP length configuration from the Management Console.
- **Management Console Configuration of the NAT IP and Port Per Interface** - Uniquely identifies different SteelHeads using the same public-facing destination addresses to support secure transport in the case of UDP encapsulation with NAT. You can now specify a NAT IPv4 address paired with a specific port opened on the NAT.
- **Merged SteelHead CX and SteelHead DX** - Merges the CX and DX SteelHead models into one image; the appliance is automatically configured to the correct product model during installation.

Prerequisites

This section provides information about product dependencies and compatibility.

Hardware and Software Dependencies

The following table summarizes the hardware and software requirements for the SteelHead.

Riverbed Component	Hardware and Software Requirements
SteelHead	19-inch (483 mm) two or four-post rack.
SteelHead Management Console	Any computer that supports a Web browser with a color image display. The Management Console has been tested with Mozilla Firefox Extended Support Release version 17.0 and Microsoft Internet Explorer v7.0 and v8.0. JavaScript and cookies must be enabled in your Web browser. Internet Explorer v7.0 and v8.0 must refresh reports every 4 minutes due to performance issues. Consider using a different browser to view reports.

Firewall Requirements

Riverbed recommends that you deploy the SteelHead behind your firewall. The following firewall settings are required for the SteelHead:

- Ports 7800 and 7810 must be open.
- Make sure your firewall does not strip TCP options.

Ethernet Network Compatibility

The SteelHead supports the following Ethernet networking standards:

- Ethernet Logical Link Control (LLC) (IEEE 802.2 - 1998)
- Fast Ethernet 100 Base-TX (IEEE 802.3 - 2008)
- Gigabit Ethernet over Copper 1000 Base-T and Fiber 1000 Base-SX (LC connector) and Fiber 1000 Base LX (IEEE 802.3 - 2008)
- 10 Gigabit Ethernet over Fiber 10GBase-LR Single Mode and 10GBase-SR Multimode (IEEE 802.3 - 2008)

The SteelHead ports support the following connection types and speeds:

- **Primary** - 10/100/1000 Base-T, auto-negotiating
- **Auxiliary** - 10/100/1000 Base-T, auto-negotiating
- **LAN** - 10/100/1000 Base-TX or 1000 Base-SX or 1000 Base-LX or 10GBase-LR or 10GBase-SR, depending on configuration
- **WAN** - 10/100/1000 Base-TX or 1000 Base-SX or 1000 Base-LX or 10GBase-LR or 10GBase-SR, depending on configuration

The SteelHead supports VLAN Tagging (IEEE 802.3 - 2008). It does not support the ISL protocol.

All copper interfaces are auto-sensing for speed and duplex (IEEE 802.3 - 2008).

The SteelHead auto-negotiates speed and duplex mode for all data rates and supports full duplex mode and flow control (IEEE 802.3 - 2008).

The SteelHead with a Gigabit Ethernet card supports jumbo frames on in-path and primary ports.

SNMP-Based Management Compatibility

The SteelHead supports a proprietary Riverbed MIB accessible through SNMP. SNMP v1 (RFCs 1155, 1157, 1212, and 1215) and SNMP v2c (RFCs 1901, 2578, 2579, 2580, 3416, 3417, and 3418) are supported, even though some MIB items can only be accessible through SNMPv2.

SNMP support allows the SteelHead to be integrated into network management systems such as Hewlett Packard OpenView Network Node Manager, BMC Patrol, and other SNMP-based network management tools.

Overview of the SteelHead

Riverbed Technology expands its market-leading SteelHead WAN optimization product family with SteelHead DX 8000. SteelHead DX appliances are purpose-built to address the unique demands of data center-to-data center disaster recovery and business continuity over WANs with up to 60x faster acceleration of data and data replication workloads, such as NetApp SnapMirror, EMC SRDF and EMC RecoverPoint, and up to 99% bandwidth reduction.

The causes for slow throughput in WANs are well known: high delay (round-trip time or latency), limited bandwidth, chatty application protocols, congestion and packet-loss. Large enterprises spend a significant portion of their information technology budgets on storage and networks, much of it spent to compensate for slow throughput, by deploying redundant servers and storage, and the required backup equipment. SteelHead DX appliances enable you to accelerate WAN performance between data centers, providing higher levels of data protection, faster data transfers, easier consolidation and centralization of key IT resources.

With the SteelHead appliance, you can solve a range of problems affecting WANs and application performance, including:

- Insufficient WAN bandwidth
- Inefficient transport protocols in high-latency environments
- Inefficient application protocols in high-latency environments

The Riverbed Optimization System (RiOS) intercepts client-server connections without interfering with normal client-server interactions, file semantics, or protocols. All client requests are passed through to the server normally, while relevant traffic is optimized to improve performance.

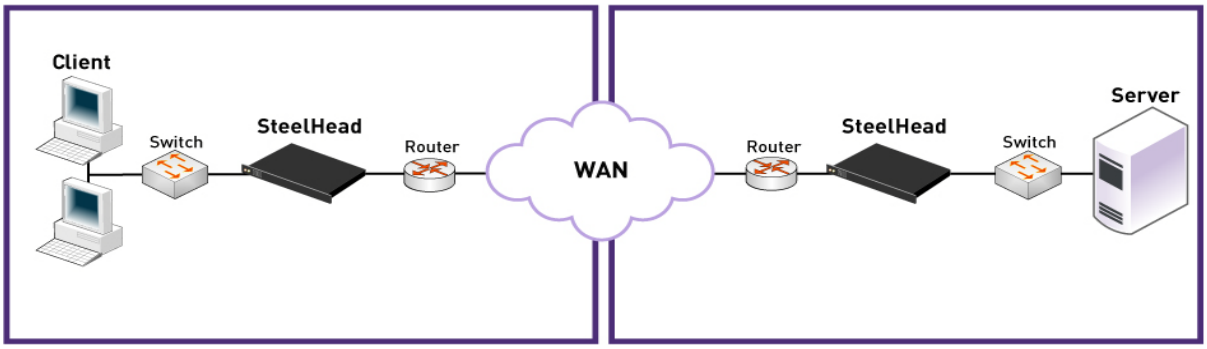
The optimization techniques RiOS utilizes are:

- **Data Streamlining** - SteelHeads can reduce WAN bandwidth utilization by 65% to 98% for TCP-based applications using Data Streamlining. In addition to traditional techniques like data compression, RiOS also uses a Riverbed proprietary algorithm called Scalable Data Referencing (SDR). SDR breaks up TCP data streams into unique *data chunks* that are indexed and stored on the device. Each data chunk is assigned a unique integer label (*reference)* before it is sent to a peer RiOS device across the WAN. When the same byte sequence is seen again in future transmissions from clients or servers, the reference is sent across the WAN instead of the raw data chunk. The peer RiOS device uses this reference to find the original data chunk on its RiOS data store, and reconstruct the original TCP data stream.
  - Turbo Data Streamlining – SteelHead DX8000 appliances offer two modes for Data Streamlining: Classic and Turbo. Classic mode is based on the same Data Streamlining techniques leveraged across the SteelHead CX and EX families. The new Turbo mode, available only in DX8000 appliances, is designed to deliver increased performance across for Data Center-to-Data Center WAN environments.
  - Storage-optimized Data Streamlining – Riverbed SteelHead solutions provide advanced data streamlining capabilities for data replication applications such as EMC SRDF/A & NetApp SnapMirror. SteelHead DXs intelligently identify and partition data sequences from headers within EMC SRDF/A to identify longer repetitive data sequences. Additionally, SteelHead solutions allow administrators to fine-tune the data streamlining techniques applied to individual storage elements, such as individual volumes for NetApp SnapMirror or individual RDF groups for EMC SRDF/A. This fine-grain control enables administrators to maximize the effectiveness of the SteelHead appliance to deliver higher levels of performance and bandwidth optimization.

- **Transport Streamlining** - SteelHeads use a generic latency optimization technique called Transport Streamlining. Transport Streamlining uses a set of standards and proprietary techniques to optimize TCP traffic between SteelHeads. These techniques:
  - ensure that efficient retransmission methods, such as TCP selective acknowledgments, are used.
  - negotiate optimal TCP window sizes to minimize the impact of latency on throughput.
  - maximize throughput across a wide range of WAN links.
- **Application Streamlining** - In addition to Data and Transport Streamlining optimizations, RiOS can apply application-specific optimizations. Application streamlining in SteelHead DXs focuses on disaster recovery application protocols such as NetApp SnapMirror, EMC SRDF/A, and FCIP.
- **Management Streamlining** - Management Streamlining refers to the methods that Riverbed has developed to simplify the deployment and management of RiOS devices. These methods include:
  - Auto-Discovery Process - Auto-discovery enables SteelHead DXs to automatically find remote SteelHead DXs, and to then optimize traffic between them. Auto-discovery relieves you from having to manually configure large amounts of network information. The auto-discovery process enables administrators to control and secure connections, specify which traffic is to be optimized, and specify peers for optimization. SteelHead DXs peer only with other SteelHead DXs.

The SteelHead is typically deployed on a LAN, with communication between appliances taking place over a private WAN or VPN. Because optimization between SteelHeads typically takes place over a secure WAN, it is not necessary to configure company firewalls to support SteelHead specific ports.

Figure 1-1. Typical Deployment



For detailed information about how the SteelHead works and deployment design principles, see the *SteelHead Deployment Guide*.

Auto-Discovery Process

Auto-discovery enables SteelHeads to automatically find remote SteelHeads and to optimize traffic to them. Auto-discovery relieves you of having to manually configure the SteelHeads with large amounts of network information. The auto-discovery process enables you to control and secure connections, specify which traffic is optimized, and specify how remote peers are selected for optimization. There are two types of auto-discoveries, original and enhanced.

Enhanced auto-discovery automatically discovers the last SteelHead in the network path of the TCP connection. In contrast, the original auto-discovery protocol automatically discovers the first SteelHead in the path. The difference is only seen in environments where there are three or more SteelHeads in the network path for connections to be optimized. Enhanced auto-discovery works with SteelHeads running the original auto-discovery protocol.

Note: SteelHead DXs peer only with other SteelHead DXs.

Configuring Optimization

You configure optimization of traffic using the Management Console or the Riverbed CLI. You configure the type of traffic a SteelHead optimizes and specify the type of action it performs using:

- In-Path rules - In-path rules determine the action a SteelHead takes when a connection is initiated, usually by a client. In-path rules are used only when a connection is initiated. Because connections are usually initiated by clients, in-path rules are configured for the initiating, or client-side SteelHead. You configure one of the following types of in-path rule actions:
  - Auto Discover - Use the auto-discovery process to determine if a remote SteelHead is able to optimize the connection attempting to be created by this SYN packet.
  - Fixed-Target - Skip the auto-discovery process and use a specified remote SteelHead as an optimization peer. Fixed-target rules require the input of at least one remote target SteelHead; an optional backup SteelHead might also be specified.
  - Fixed-Target (Packet Mode Optimization) - Skip the auto-discovery process and uses a specified remote SteelHead as an optimization peer to perform bandwidth optimization on TCPv4, TCPv6, UDPv4, or UDPv6 connections. Packet-mode optimization rules support both physical in-path and master/backup SteelHead configurations. For details, see the *SteelHead Management Console User's Guide*.
  - Pass-Through - Allow the SYN packet to pass through the SteelHead. No optimization is performed on the TCP connection initiated by this SYN packet.
  - Discard - Drop the SYN packet silently.
  - Deny - Drop the SYN packet and send a message back to its source.
- Peering rules - Peering rules determine how a SteelHead reacts when it sees a probe query. Peering rules are an ordered list of fields a SteelHead uses to match with incoming SYN packet fields: for example, source or destination subnet, IP address, VLAN, or TCP port, as well as the IP address of the probing SteelHead. This is especially useful in complex networks. There are the following types of peering rule are available:
  - Auto - If the receiving SteelHead is not using enhanced auto-discovery, this has the same effect as the Accept peering rule action. If enhanced auto-discovery is enabled, the SteelHead only becomes the optimization peer if it is the last SteelHead in the path to the server.
  - Accept - The receiving SteelHead responds to the probing SteelHead and becomes the remote-side SteelHead (that is, the peer SteelHead) for the optimized connection.
  - Passthrough - The receiving SteelHead does not respond to the probing SteelHead, and allows the SYN+ probe packet to continue through the network.

For detailed information about in-path and peering rules and how to configure them, see the *SteelHead Management Console User's Guide*.

Fail-to-Wire (Bypass) Mode

All SteelHead models and in-path network interface cards support a fail-to-wire mode. In the event of a failure or loss of power, the SteelHead goes into bypass mode and the traffic passes through uninterrupted.

Many in-path network interface cards (NICs) also support a fail-to-block mode in which case if there is a failure or loss of power, the SteelHead LAN and WAN interfaces power down and stop bridging traffic. The default failure mode is fail-to-wire mode.

If there is a serious problem with the SteelHead or it is not powered on, it goes into bypass mode to prevent a single point of failure. If the SteelHead is in bypass mode, you are notified in the following ways:

- The Intercept/Bypass status light on the bypass card is triggered. For detailed information about bypass card status lights, see the appendices that follow.
- The Dashboard page of the Management Console displays **Critical** in the Status bar.
- SNMP traps are sent (if you have set this option).
- The event is logged to system logs (syslog).
- Email notifications are sent (if you have set this option).

When the fault is corrected, new connections that are made receive optimization; however, connections made during the fault are not. To force all connections to be optimized, enable the *kickoff* feature. Generally, connections are short-lived and kickoff is not necessary. For detailed information about enabling the kickoff feature, see the *SteelHead Management Console User's Guide* and the *SteelHead Deployment Guide*.

When the SteelHead is in bypass mode the traffic passes through uninterrupted. Traffic that was optimized might be interrupted, depending on the behavior of the application-layer protocols. When connections are restored, they succeed, although without optimization.

In an out-of-path deployment, if the server-side SteelHead fails, the first connection from the client fails. After detecting that the appliance is not functioning, a ping channel is setup from the client-side SteelHead to the server-side SteelHead. Subsequent connections are passed through unoptimized. When the ping succeeds, processing is restored and subsequent connections are intercepted and optimized.

For detailed information about the **ping** command, see the *Riverbed Command-Line Interface Reference Manual*.

Fail-to-Block (Disconnect) Mode

In fail-to-block mode, if the SteelHead has an internal software failure or power loss, the SteelHead LAN and WAN interfaces power down and stop bridging traffic.

When fail-to-block is enabled, a failed SteelHead blocks traffic along its path, forcing traffic to be re-routed onto other paths (where the remaining SteelHeads are deployed). This is only useful if the network has a routing or switching infrastructure that can automatically divert traffic off of the link once the failed SteelHead blocks it.

You set fail-to-block mode in the SteelHead CLI. For detailed information, see the *SteelHead Deployment Guide*.

Note: You can use this with connection-forwarding, the allow-failure CLI command, and an additional SteelHead on another path to the WAN to achieve redundancy. For more information, see the *Riverbed Command-Line Interface Reference Manual*.

CHAPTER 2 Managing Riverbed Licenses

This chapter describes the Riverbed licensing methods and how to manage Riverbed licenses. It includes the following sections:

Riverbed Licensing Methods

A license is a string issued by Riverbed that embeds information that ties the license to data to prevent tampering. After you install the license, the system saves it in the configuration database and enables the functionality associated with the license. Riverbed employs the following licensing methods:

- **Automatic Licensing** - After you connect your SteelHead to the network, the SteelHead automatically contacts the Riverbed Licensing Portal and downloads and installs the licenses.
- **Manual Licensing** - You can manually fetch and activate licenses for Riverbed products using the Riverbed Licensing Portal. Go to https://licensing.riverbed.com/index.htm and follow the instructions to retrieve and activate license keys.
- **Factory Licensing** - You can have all your Riverbed licenses installed at the factory for a small fee.
- **Token Method** - You use tokens to activate Riverbed software, such as the Virtual SteelCentral Controller for SteelHead Mobile, Virtual SteelStore, SteelHead (virtual edition), and HP ProCurve. For detailed information, see the respective installation guides for these products.

Automatic Licensing

Automatic licensing allows the SteelHead, once connected to the network, to automatically contact the Riverbed Licensing Portal to retrieve and install license keys onto the appliance. Automatic licensing simplifies inventory management and provides an automated mechanism of fetching licenses for Riverbed products without having to manually activate individual appliances and licenses.

If you are behind a firewall you can retrieve licenses at the Riverbed Licensing Portal using the email option. For detailed information, see "Retrieving Licenses Using the Riverbed Licensing Portal" on page 14.

Automatic licensing also works over a web proxy. For details on setting up a web proxy, see the *SteelHead Management Console User's Guide*.

Tip: If automatic licensing fails, an error message appears in the Management Console. Go to the Riverbed Licensing Portal and follow the instructions for retrieving your licenses.

To view licenses on a new SteelHead

- Connect the new SteelHead to the network.

  The SteelHead automatically contacts the Riverbed Licensing Portal which downloads and installs the licenses. The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message.

To replace expired licenses

- Purchase new downloadable licenses to replace the expired license.

  At the time of the next scheduled automatic license fetch, the SteelHead automatically contacts the Riverbed License Portal and downloads the new licenses. The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message. You do not need to delete the expired license. The system uses the license with the latest expiration date.

To fetch a license on demand

1. In the Management Console choose Administration > Maintenance: Licenses to display the Licenses page.
2. Click **Fetch Updates Now**.

   The Management Console Licensing page displays a success message or the Alarm Status page reports an actionable error message.

Note: Only administrator users can fetch and install licenses. For detailed information on administrator and monitor users, see the *SteelHead Management Console User's Guide*.

Manual Licensing Using the Riverbed Licensing Portal

You can retrieve and manage Riverbed licenses using the Riverbed Licensing Portal. Once you retrieve a license from the Riverbed Licensing Portal, you need to install it.

Retrieving Licenses Using the Riverbed Licensing Portal

The licensing portal requires a unique product identifier to retrieve a license. Depending on the product, the identifier can be a serial number, a license request key (activation code), or a token. The steps to retrieve a license vary based on the product identifier. Online instructions guide you through the process.

To retrieve your licenses for an appliance using a serial number

1. Go to the License Activation page in the Riverbed Licensing Portal at https://licensing.riverbed.com/index.htm
2. Enter your appliance serial number as your unique product identifier.

   The serial number is on a label located on your appliance and it also appears in the Support tab of the Management Console.
3. Click **Next**.
4. Provide the contact information for the license, including your name and email.
5. Click **Submit**.

   The Licensing Portal displays license information for all the products purchased with the serial number you specified.
6. Click a serial number to see license details.
7. Optionally, if you are behind a firewall, type the email address in the Email address text box and click **Email Keys** to have the license keys emailed to you.

Tip: Click **New Search** to look for additional license records.

Installing Your License Keys

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

To install a license using the CLI

1. Connect to the CLI of the appliance and enter configuration mode.

   For details see the *Riverbed Command-Line Interface Reference Manual*.
2. At the system prompt, enter the following commands:

```
license install <the license key you retrieved from Riverbed Licensing Portal>
write memory
```

To install a license using the Management Console

1. Connect to the Management Console of the appliance.

   For details, see the *SteelHead Management Console User's Guide*.
2. Choose Administration > Maintenance: Licenses to display the Licenses Page.
3. Copy and paste the license key provided by Riverbed Licensing Portal into the text box. Separate multiple license keys with a space, Tab, or Enter.

CHAPTER 3 Installing and Configuring the SteelHead

This chapter describes how to install and configure the SteelHead in an in-path and out-of-path network deployment. This chapter includes the following sections:

Important: Read and follow the safety guidelines described in the *Safety and Compliance Guide*. Failure to follow these safety guidelines can result in damage to the equipment.

Choosing a Network Deployment

Typically, you deploy the SteelHead on a LAN, with communication between appliances taking place over a private WAN or VPN. Because optimization between SteelHeads typically takes place over a secure WAN, you do not need to configure company firewalls to support SteelHead-specific ports.

Note: If there are one or more firewalls between two SteelHeads, ports 7800 and 7810 must be passed through firewall devices located between the pair of SteelHeads. Also, SYN and SYN/ACK packets with the TCP option 76 must be passed through firewalls for auto-discovery to function properly.

For optimal performance, you should minimize latency between SteelHeads and their respective clients and servers. SteelHeads should be as close as possible to your network end points (client-side SteelHeads should be as close to your clients as possible and server-side SteelHeads should be as close to your servers as possible).

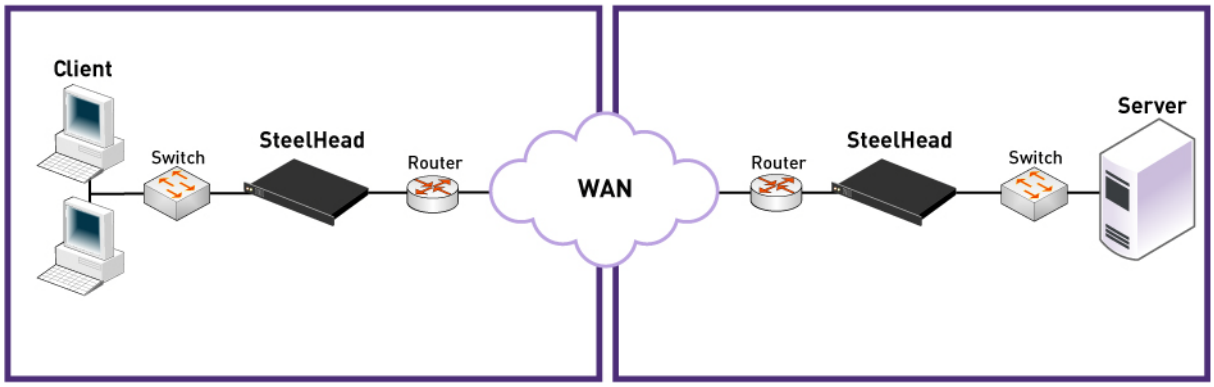
Ideally, SteelHeads optimize only traffic that is initiated or terminated at their local site. The best and easiest way to achieve this is to deploy the SteelHeads where the LAN connects to the WAN, and not where any LAN-to-LAN or WAN-to-WAN traffic can pass through (or be redirected to) the SteelHead.

For detailed information about your deployment options and best practices for deploying SteelHeads, see the *SteelHead Deployment Guide*.

Before you begin the installation and configuration process, you must select a network deployment:

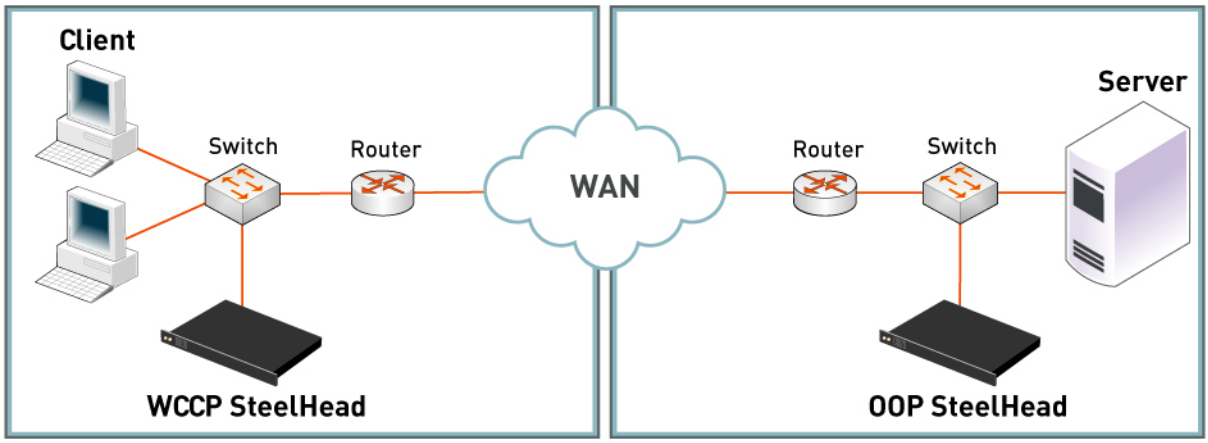
- **Physical In-Path** - In a physical in-path deployment, the SteelHead is *physically* in the direct path between clients and servers. The clients and servers continue to see client and server Internet Protocol (IP) addresses. In-path designs are the simplest to configure and manage, and the most common type of SteelHead deployment, even for large sites.

Figure 3-1. Physical In-Path Deployment



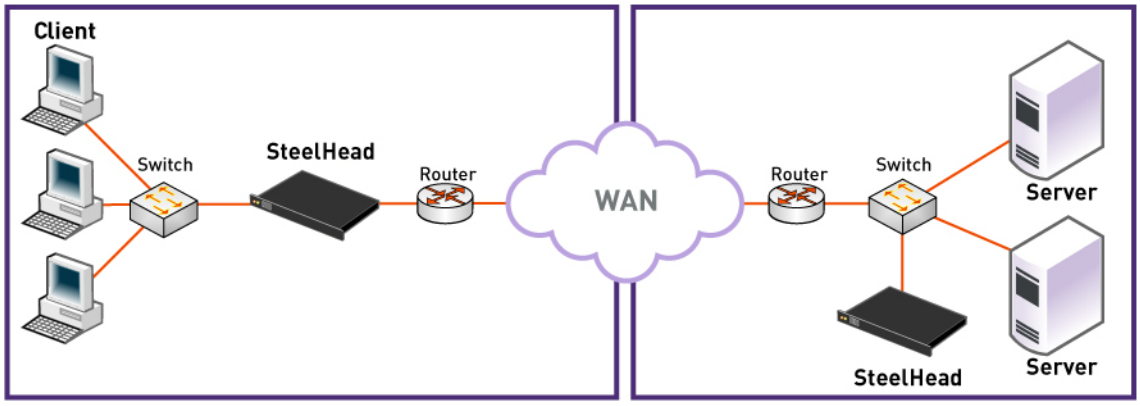
- **Virtual In-Path** - In a virtual in-path deployment, a redirection mechanism (such as WCCP, PBR, or Layer-4 switching) is used to place the SteelHead virtually in the path between clients and servers.

Figure 3-2. Virtual In-Path: WCCP Deployment



- **Out-of-Path** - In an out-of-path deployment, the server-side SteelHead is not in the direct path between the client and the server. In an out-of-path deployment, the SteelHead acts as a proxy. This type of deployment might be suitable for locations where physical in-path or virtual in-path configurations are not possible.

Figure 3-3. Out-of-Path Deployment



Checking Your Inventory

Your shipping carton contains the following items:

- The SteelHead
- One standard Ethernet straight-through cable
- One standard Ethernet crossover cable
- One serial null-modem cable
- One or two power cables (depending on your order)

  Aside from country-specific requirements, all systems ship with the same power cable. The power cable has a IEC 60320 C13 plug on one end (to connect to the SteelHead) and a country-specific plug that fits the wall socket for that country. If a system has two power supplies, it ships with two suitable cables.

  You must always connect the SteelHead using either the cable in the accessories box or another cable that is approved for use by the IEC in the country in which the appliance is connected.

  You cannot connect a SteelHead directly to multiphase outlets. You must use a rack PDU or power strip that provides the appropriate three-prong outlet (hot/neutral/ground). For details, see the Knowledge Base solution number 1301.
- One Phillips screwdriver
- Rails are preinstalled on the DX8000 platforms
- One mounting kit
- Documentation kit

If any items are damaged or missing, notify Riverbed Support at https://support.riverbed.com for replacement or repair.

Preparing Your Site for Installation

The SteelHead is shipped completely assembled, with all the equipment parts in place and securely fastened.

Site Requirements

Before you install the SteelHead, make sure that your site meets the following requirements:

- It is a standard electronic environment where the ambient temperature does not exceed 40º C (104º F) and the relative humidity does not exceed 80% (noncondensing). For detailed information, see the appendices that follow.
- Ethernet connections are available within the standard Ethernet limit.
- There is available space on a two-post or four-post 19-inch rack. For details about installing the SteelHead to a rack, see the *Rack Installation Guide* or the printed instructions that were shipped with the system.
- A clean power source is available, dedicated to computer devices and other electronic equipment.
- The rack is a standard 19-inch Telco-type mounting rack.

Note: Riverbed recommends that you use a four-post mounting rack for 2U systems.

Note: If your rack requires special mounting screws, contact your rack manufacturer.

SteelHead Ports

The following table summarizes the ports used to connect the SteelHead to your network.

Port	Description
Console	Connects the serial cable to a terminal device. You establish a serial connection to a terminal emulation program for console access to the configuration wizard and the SteelHead CLI.
Primary (PRI)	The management interface that connects the SteelHead to a LAN switch. This management interface enables you to connect to the Management Console and the SteelHead CLI. **Tip**: The primary and auxiliary ports cannot share the same network subnet. **Tip**: The primary and in-path interfaces can share the same subnet. **Tip**: You must use the primary port on the server-side for out-of-path deployments.
Auxiliary (AUX)	An optional port that provides an additional management interface for a secondary network. You cannot have the primary and auxiliary ports on the same subnet. **Tip**: The auxiliary and in-path interfaces cannot share the same network subnet. **Tip**: You cannot use the auxiliary port for out-of-path SteelHeads.

Port	Description
WAN	Connects the WAN port of the SteelHead and the WAN router using a crossover cable.
LAN	Connects the LAN port of the SteelHead and the LAN switch using a straight-through cable. **Note**: If the SteelHead is deployed between two switches, both the LAN and WAN ports must be connected with straight-through cables.

Avoiding Duplex Mismatch

Before you begin the configuration process, ensure that your LAN and WAN interfaces have the same duplex settings.

The SteelHead automatically negotiates duplex settings. If one end of the link is set to auto-negotiate and the other end of the link is not set to auto-negotiate, the duplex settings on the network device default to half-duplex. This duplex mismatch passes traffic, but it causes late collisions and results in degraded optimization. To achieve maximum optimization, set your network devices to 100 and **full**.

To avoid duplex mismatches, manually configure the duplex settings on your:

- router.
- switch.
- SteelHead WAN interface.
- SteelHead LAN interface.
- SteelHead primary interface.

The following can be signs of a duplex mismatch:

- On the Reports > Diagnostics: System Logs page you see errors for sends, receives, CRC, and short sends.
- You cannot connect to an attached device.
- You can connect to a device when you choose auto-negotiation, but you cannot connect to that same device when you manually set the speed or duplex.
- Slow performance across the network.

For detailed information about checking for duplex mismatches, see Chapter 4, "Troubleshooting."

Bypass Card Interface Naming Conventions

The interface names for the bypass cards are a combination of the slot number and the port pairs (<slot>_<pair>, <slot>_<pair>). For example, if a four-port bypass card is located in slot 0 of your appliance, the interface names are lan0_0, wan0_0, lan0_1, and wan0_1, respectively. Alternatively, if the bypass card is located in slot 1 of your appliance, the interface names are lan1_0, wan1_0, lan1_1, and wan1_1, respectively.

For detailed information about installing additional bypass cards, see the *Network Interface Card Installation Guide*.

Completing the Configuration Checklist

Before you begin, consult the *Rack Installation Guide* for detailed information about how to install your model to a rack.

The following checklist lists the parameters you specify to complete the initial configuration of the SteelHead. Be prepared to provide values for these parameters.

Appliance	Parameter	Your Value
SteelHead (the Primary Interface)	Host name	
	IP address	
	Netmask	
	Default gateway (the WAN gateway)	
	DNS IP address	
	Domain name for the system	
	Administrator password	
	SMTP server IP address	
	Events and failures notification email address	
	Primary interface speed	
	Primary interface duplex	
In-Path Deployments	In-path interface IP address	
	In-path netmask	
	In-path gateway	
	In-path: LAN interface speed	
	In-path: LAN interface duplex	
	In-path: WAN interface speed	
	In-path: WAN interface duplex	

Note: The SteelHead automatically negotiates duplex settings. If one end of the link is set to auto-negotiate and the other end of the link is not set to auto-negotiate, the duplex settings on the network device default to half-duplex. This duplex mismatch passes traffic, but it causes late collisions and results in degraded optimization. To achieve maximum optimization, set the network devices to 100 and **full**.

Powering On the System

The following section describes how to connect the AC power and how to power on the system.

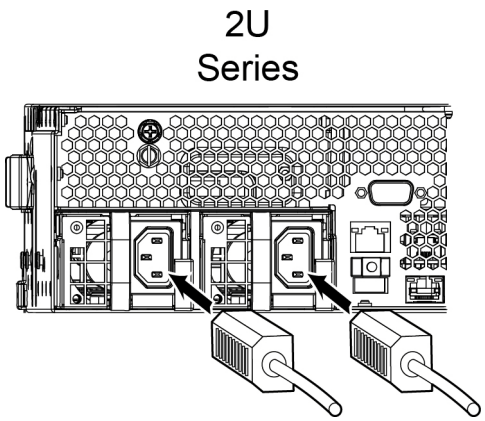
Caution: In European electrical environments you must ground (earth) the Green/Yellow tab on the power cord, or risk electrical shock.

To power on the system

1. If your system has a master power switch, ensure that the system and master power switch is in the off position on the rear of the SteelHead.
2. Plug the AC power cord into the SteelHead.

Note: If your model has multiple power supplies, you must plug in all the power cords or you will hear an alarm.

Figure 3-4. Connecting the AC Power



3. Plug the AC power cord into an uninterrupted AC power source.
4. Press the system power switch on. If the SteelHead does not immediately power on, press the power switch off, then press the power switch on again.
5. Check the status lights on the SteelHead. For detailed information about the status lights, see Appendix A, "SteelHead DX8000 Specifications."

Note: The SteelHead DX takes approximately 10 minutes to boot.

Configuring In-Path SteelHead Appliances

In a physical in-path deployment, the SteelHead is physically in the direct path between clients and servers. The clients and servers continue to see client and server IP addresses. Physical in-path configurations are suitable for any location where the total bandwidth is within the limits of the installed SteelHead. For a detailed figure, see "Choosing a Network Deployment" on page 17.

For detailed information about in-path deployments, see the *SteelHead Deployment Guide*.

You use standard Ethernet straight-through and crossover cables to connect to your network in an in-path configuration. Make sure that you use the correct cables to establish your network connections:

- **Straight-through cables** - Primary and LAN ports on the appliance to the LAN switch.
- **Crossover cable** - WAN port on the appliance to the WAN router.

Connecting the SteelHead to Your Network

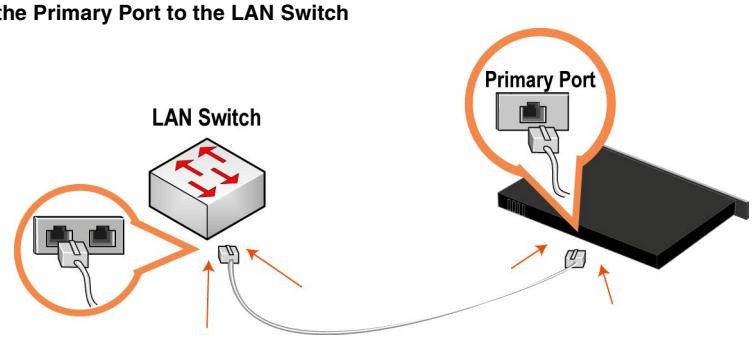
You use standard Ethernet straight-through and crossover cables to connect to your network in an in-path configuration. Make sure that you use the correct cables to establish your network connections:

- **Straight-through cables** - Primary and LAN ports on the appliance to the LAN switch.
- **Crossover cable** - WAN port on the appliance to the WAN router.

To connect to the SteelHead to your network

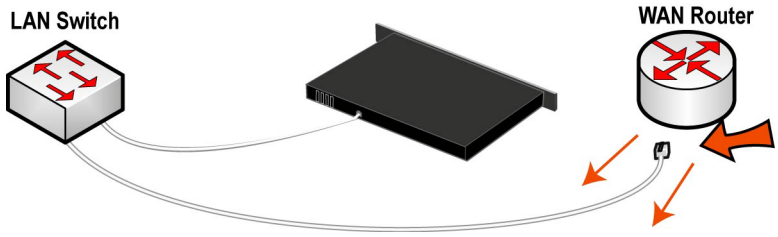
1. Plug the straight-through cable into the primary port of the SteelHead and the LAN switch. This can be any port on your LAN switch configured to connect to a host.

Figure 3-5. Connecting the Primary Port to the LAN Switch



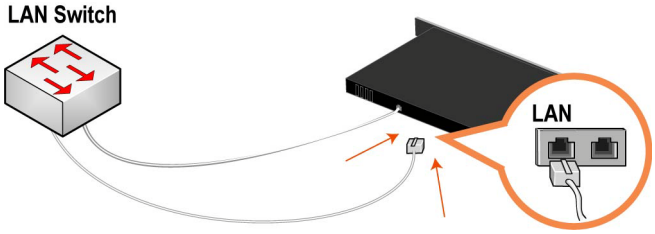
2. Identify the straight-through cable that connects your LAN switch to your WAN router. Unplug the end connected to the WAN router.

Figure 3-6. Disconnecting the WAN Router



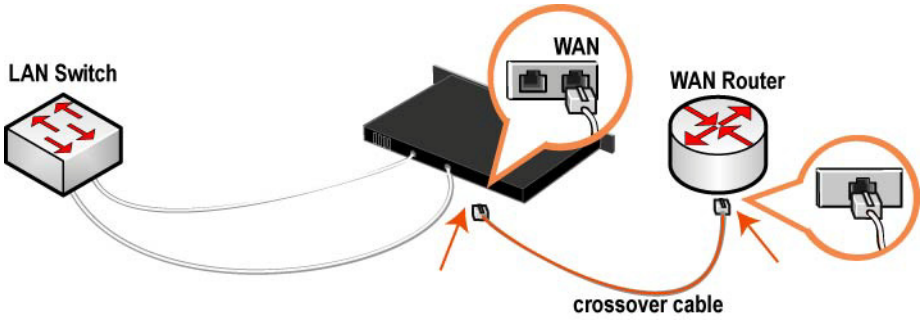
3. Plug the straight-through cable that you disconnected from the WAN router into the LAN port of the SteelHead.

Figure 3-7. Connecting the LAN Switch to the LAN Port



4. Using the provided crossover cable, plug the cable into the WAN port of the SteelHead and the WAN router. This must be a crossover cable.

Figure 3-8. Connecting the WAN Port to the WAN Router



Note: If you have a four-port or six-port bypass card, repeat Step 1 through Step 4. For detailed information about installing additional bypass cards, see the *Network Interface Card Installation Guide*.

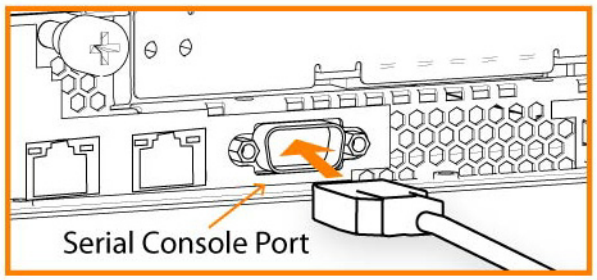
Running the Configuration Wizard

To access the configuration wizard and the SteelHead CLI, you establish a serial connection using a terminal emulator program.

To run the configuration wizard

1. Plug the serial cable into the Serial/Console port and a terminal.

Figure 3-9. Connecting to the SteelHead



2. Start your terminal emulation program, such as Tera Term Pro. The terminal device must have the following settings:

- Baud rate: 9600 bps
- Data bits: 8
- Parity: none
- Stop bits: 1
- vt100 emulation
- No flow control

If you are using the SteelHead with a terminal server, the terminal server must use hardware flow control for the port connected to the SteelHead.

Riverbed recommends that you connect the console port to a device that logs output. Even though this is not a requirement, it can help you to identify problems with the system.

3. Log in as administrator user (`admin`) and enter the default password (`password`). For example,

```
login as: admin
Sent username "admin"
password: password
```

The configuration wizard automatically starts after you have entered the login and default password. After you have established a connection, you configure the SteelHead using the configuration wizard.

4. If you are prompted to auto-configure using a SteelCentral Controller for SteelHead (Controller) appliance, answer **no**.

```
Do you want to auto-configure using a Controller? no
```

Tip: If you mistakenly answer **yes**, return to the wizard from the CLI by entering the **configuration jump-start** command from configuration mode. For detailed information, see the "To restart the configuration wizard" on page 29.

---

5. To start the configuration wizard, enter **yes** at the system prompt.

```
Do you want to use the configuration wizard for initial configuration? yes
```

Press **Enter** to enter the default value; press **?** for help; press **Ctrl-B** to go back to the previous step.

6. Complete the configuration wizard steps on the client-side and the server-side SteelHeads as described in the following table.

Wizard Prompt	Description	Example
Step 1: Host name?	Enter the host name for the SteelHead.	`hostname? amnesiac`
Step 2: Use DHCP on the primary interface?	You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SteelHead. Riverbed recommends that you do not set DHCP. The default value is no.	`Use DHCP? no`
Step 3: Primary IP address?	Enter the IP address for the SteelHead.	`Primary IP address? 10.10.10.6`

Wizard Prompt	Description	Example
Step 4: Netmask?	Enter the netmask address.	`Netmask? 255.255.0.0`
Step 5: Default gateway?	Enter the default gateway for the SteelHead.	`Default gateway? 10.0.0.1`
Step 6: Primary DNS server?	Enter the primary DNS server IP address.	`Primary DNS server? 10.0.0.2`
Step 7: Domain name?	Enter the domain name for the network where the SteelHead is to reside. If you set a domain name, you can enter host names in the system without the domain name.	`Domain name? example.com`
Step 8: Admin password?	Riverbed strongly recommends that you change the default administrator password at this time. The password must be a minimum of six characters. The default administrator password is password.	`Admin password? xxxyyy`
Step 9: SMTP server?	Enter the name of the SMTP server. External DNS and external access for SMTP traffic is required for email notification of events and failures to function. Important: Make sure that you provide a valid SMTP server to ensure that the email notifications for events and failures.	`SMTP server? natoma`
Step 10: Notification email address?	Enter a valid email address to which notification of events and failures are to be sent.	`Notification email address? example@xample.com`
Step 11: Set the primary interface speed?	Enter the speed on the primary interface (that is, the SteelHead). Make sure that this value matches the settings on your router or switch. The default value is auto.	`Set the primary interface speed? [auto] auto`
Step 12: Set the primary interface duplex?	Enter the duplex mode on the primary interface. Make sure that this value matches the settings on your router or switch. The default value is `auto`.	`Set the primary interface duplex? [auto] auto`
Step 13: Would you like to activate the in-path configuration?	Enter `yes` at the system prompt to configure in-path support. An in-path configuration is a configuration in which the SteelHead is in the direct path of the client and server. For detailed information about in-path configurations, see the *SteelHead Deployment Guide*.	`Would you like to activate the in-path configuration? yes`
Step 14: In-Path IP address?	Enter the in-path IP address for the SteelHead.	`In-Path IP address? 10.11.11.6`
Step 15: In-Path Netmask?	Enter the in-path netmask address.	`In-Path Netmask? 255.255.0.0`

Wizard Prompt	Description	Example
Step 16: In-Path Default gateway?	Enter the in-path default gateway (the WAN gateway).	`In-Path Default Gateway? 10.11.11.16`
Step 17: Set the in-path: LAN interface speed?	Enter the in-path, LAN interface speed. Make sure that this value matches the settings on your router or switch. The default value is auto.	`Set the in-path: LAN interface speed? [auto] auto`
Step 18: Set the in-path: LAN interface duplex?	Enter the in-path, LAN duplex value. Make sure that this value matches the settings on your router or switch. The default value is auto.	`Set the in-path: LAN interface duplex? [auto] auto`
Step 19: Set the in-path: WAN interface speed?	Enter the in-path, WAN interface speed. Make sure that this value matches the settings on your router or switch. The default value is auto.	`Set the in-path: WAN interface speed? [auto] auto`
Step 20: Set the in-path: WAN interface duplex?	Enter the in-path, WAN duplex speed. Make sure that this value matches the setting on your router or switch. The default value is auto.	`Set the in-path: WAN interface duplex? [auto] auto`

7. The system confirms your settings.

```
   You have entered the following information:
   1. Hostname: amnesiac
   2. Use DHCP on primary interface: no
   3. Primary IP address: 10.10.10.6
   4. Netmask: 255.255.0.0
   5. Default gateway: 10.0.0.1
   6. Primary DNS server: 10.0.0.2
   7. Domain name: example.com
   8. Admin password: xxxyyy
   9. SMTP server: natoma
   10. Notification email address: example@example.com
   11. Set the primary interface speed: auto
   12. Set the primary interface duplex: auto
   13. Would you like to activate the in-path configuration: yes
   14. In-Path IP address: 10.11.11.6
   15. In-Path Netmask: 255.255.0.0
   16. In-Path Default gateway: 10.11.11.16
   17. Set the in-path:LAN interface speed: auto
   18. Set the in-path:LAN interface duplex: auto
   19. Set the in-path:WAN interface speed: auto
   20. Set the in-path:WAN interface duplex: auto
To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.
Choice:
```

   The SteelHead configuration wizard automatically saves your configuration settings.

8. To log out of the system, enter the following command at the system prompt:

```
amnesiac> exit
```

To restart the configuration wizard

- Enter the following set of commands at the system prompt:

```
> enable
# configure terminal
(config) # configuration jump-start
```

For detailed information about the CLI, see the *Riverbed Command-Line Interface Reference Manual*.

Verifying You Are Connected to the SteelHead

Perform the following tasks to verify that you have properly connected the SteelHead.

To verify you are connected to the SteelHead

1. Verify that you can connect to the CLI using one of the following devices:

- An ASCII terminal or emulator that can connect to the serial console. It must have the following settings: 9600 baud, 8 bits, no parity, 1 stop bit, vt100, and no flow control.
- A computer with a Secure Shell (SSH) client that is connected to the SteelHead primary port.

2. At the system prompt, enter the following command:

```
ssh admin@host.domain
```

or

```
ssh admin@ipaddress
```

3. You are prompted for the administrator password. This is the password you set in the configuration wizard.

4. At the system prompt, ping from the management interface:

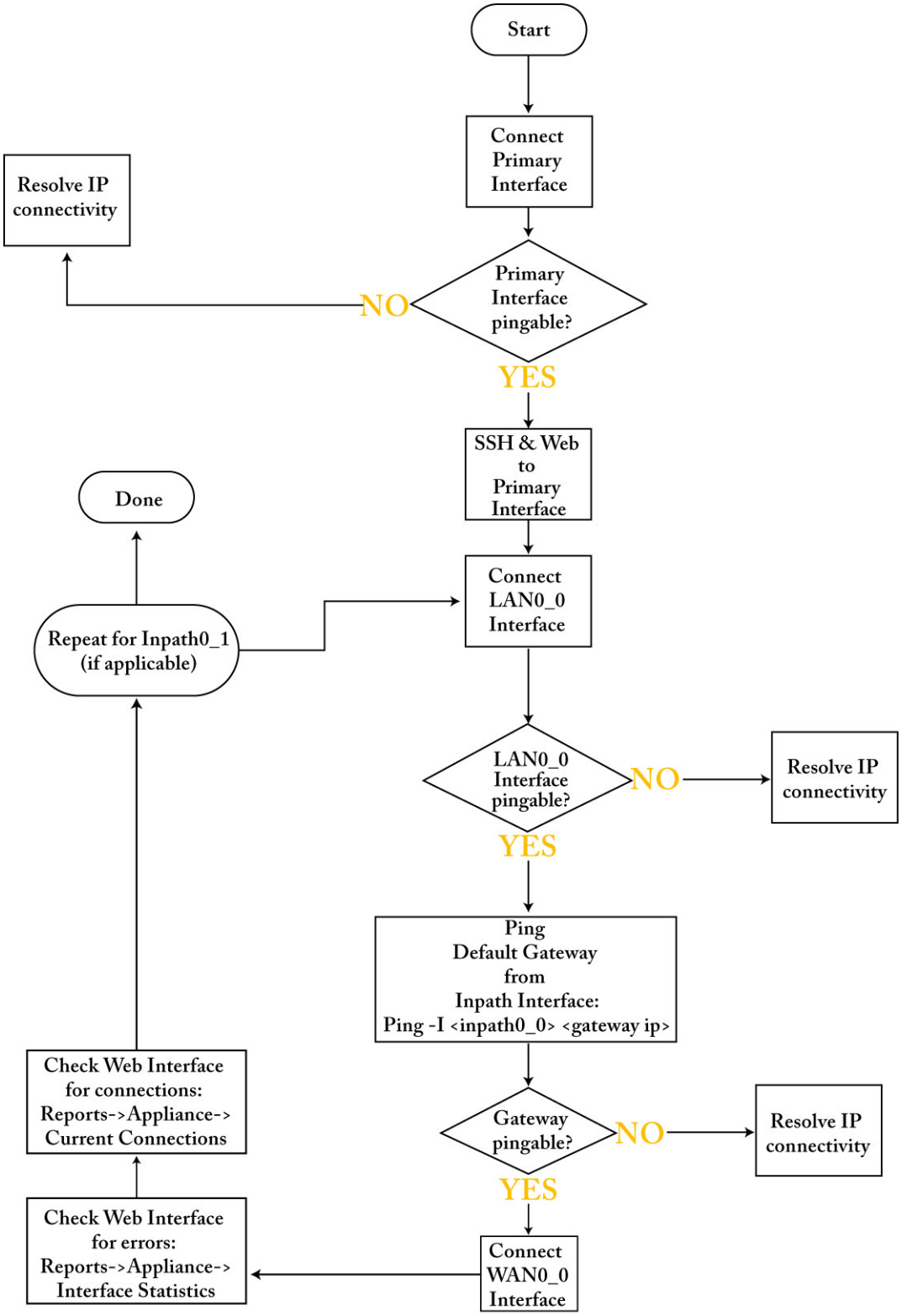
```
ping -I <primary-IP-address> <primary-default-gateway>
```

5. At the system prompt, ping from the in-path default gateway:

```
ping -I <in-path-IP-address> <in-path-default-gateway>
```

If you have problems connecting to the SteelHead, use the following flow chart to trouble shoot issues.

Figure 3-10. Resolving IP Connectivity



Connecting to the Management Console

After you configure the SteelHead, you can check and modify your configuration settings and view performance reports and system logs in the Management Console. You can connect to the Management Console through any supported Web browser.

To connect to the Management Console, you must know the host, domain, and administrator password that you assigned in the configuration wizard.

Note: Cookies and JavaScript must be enabled in your Web browser.

To connect to the Management Console

1. Specify the URL for the Management Console in the location box of your Web browser:

   `protocol://host.domain`

   - *protocol* is http or https. HTTPS uses the SSL protocol to ensure that a secure environment. If you use HTTPS to connect, you are prompted to inspect and verify the SSL key.
   - *host* is the host name you assigned to the SteelHead during initial configuration. If your DNS server maps that IP address to a name, you can specify the DNS name.
   - *domain* is the full domain name for the SteelHead.

Note: Alternatively, you can specify the IP address instead of the host and domain.

   The Management Console appears, displaying the Login page.

2. In the Username text box, type the user login: admin, monitor, a login from a RADIUS or TACACS+ database, or any local accounts created using the Role-Based Accounts feature. The default login is admin.

   Users with administrator privileges can configure and administer the SteelHead. Users with monitor privileges can view the SteelHead reports, user logs, and change their own password. A monitor user cannot make configuration changes.

3. In the Password text box, type the password you assigned in the configuration wizard of the SteelHead. (The SteelHead is shipped with the default password: password.)

4. Click **Log In** to display the Dashboard page.

   The Dashboard page summarizes the current status of your system.

Verifying WAN Optimization

Perform the following tasks to verify that you have properly configured the SteelHead.

To verify optimization

1. Go to the Reports > Optimization: Bandwidth Optimization in the Management Console to verify optimization.
2. Map a remote drive on a client machine.
3. Drag and drop a 1 MB file from the client to the remote server.

   Ensure that the server is located across the WAN.
4. Drag and drop the 1 MB file again.

   Performance improves significantly.

Checking for Speed and Duplex Errors

If you selected auto-negotiation (auto) for your in-path and primary interfaces, you must ensure that the SteelHead negotiated the speed and duplex at the rate your devices expect. For example, ensure settings are auto on the LAN and WAN and 100 FULL on the LAN and WAN. You can verify your speed and duplex settings in the Networking > Networking: In-path Interfaces page and the Networking > Networking: Base Interfaces page of the Management Console.

To check for speed and duplex errors

1. In the Management Console, go to the Reports > Diagnostics: System Logs page.
2. Check the system logs for duplex or speed errors.
3. Go to the Reports > Networking: Current Connections page.
4. Check for duplex and speed errors.

   If you find errors, change the speed and duplex settings on your LAN and WAN interface in the Networking > Networking: In-path Interfaces page.

Configuring Out-of-Path Steelhead Appliances

In an out-of-path deployment, the SteelHead is not in the direct path between the client and the server. Servers see the IP address of the server-side SteelHead rather than the client-side IP address.

An out-of-path configuration is suitable for data center locations where physical in-path or logical in-path configurations are not possible. For a detailed figure, see "Choosing a Network Deployment" on page 17.

For detailed information about out-of-path deployments, see the *SteelHead Deployment Guide*.

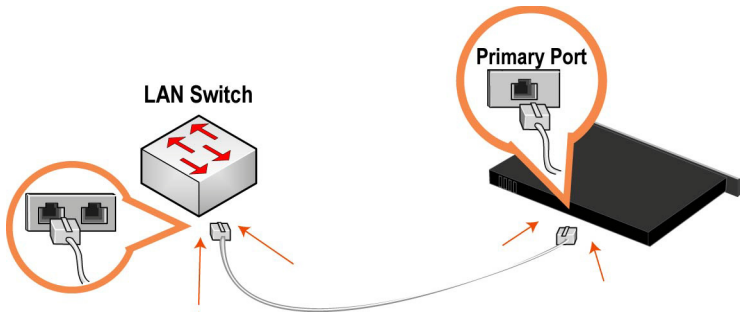
Connecting Out-of-Path Steelhead Appliances to Your Network

You use a standard Ethernet straight-through cable to connect the primary port of the SteelHead to the LAN switch in an out-of-path configuration.

To connect an out-of-path SteelHead to your network

- Plug the straight-through cable into the primary port of the SteelHead and the LAN switch. This can be any port on your LAN switch that is configured to connect to a host.

Figure 3-11. Connecting the primary Port and LAN Switch



Configuring the Server-Side SteelHead

The configuration wizard automatically starts when you log in to the SteelHead CLI for the first time. For detailed information about the configuration wizard and how to start it, see "To run the configuration wizard" on page 25.

In an out-of-path configuration, the client-side SteelHead is configured as an in-path device and the server-side SteelHead is configured as an out-of-path device.

To configure the server-side SteelHead

1. Check the duplex and speed settings on the router and switch that connects to your SteelHead. Make sure that the settings on the router, switch, and the SteelHead match. For example, ensure that settings are auto speed and duplex on the LAN and WAN or 100 FULL on the LAN and WAN. If the settings do not match, optimization might be degraded.

2. Connect to the CLI.

3. If you are prompted to auto-configure the SteelHead using the CMC, enter **No**.

```
Do you want to auto-configure using a Controller? no
```

4. To start the configuration wizard, enter **yes** at the system prompt.

```
Do you want to use the configuration wizard for initial configuration? yes
```

Tip: If you mistakenly answer **no**, to return to the wizard from the CLI, enter the **configuration jump-start** command from configuration mode. For detailed information, see the "To restart the configuration wizard" on page 29.

---

5. Complete the configuration wizard steps on the client side and server side.

Wizard Prompt	Description	Example
Step 1: Host name?	Enter the host name for the SteelHead.	`Hostname? amnesiac`
Step 2: Use DHCP on the primary interface?	You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SteelHead. Riverbed recommends that you do not set DHCP. The default value is **no**.	`Use DHCP? no`
Step 3: Primary IP address?	Enter the IP address for the SteelHead.	`Primary IP address? 10.10.10.6`
Step 4: Netmask?	Enter the netmask address.	`Netmask? 255.255.0.0`
Step 5: Default gateway?	Enter the default gateway for the SteelHead.	`Default gateway? 10.0.0.1`
Step 6: Primary DNS server?	Enter the primary DNS server IP address.	`Primary DNS server? 10.0.0.2`
Step 7: Domain name?	Enter the domain name for the network where the SteelHead is to reside. If you set a domain name, you can enter host names in the system without the domain name.	`Domain name? example.com`
Step 8: Admin password?	Riverbed strongly recommends that you change the default administrator password at this time. The password must be a minimum of 6 characters. The default administrator password is **password**.	`Admin password? xxxyyy`
Step 9: SMTP server?	Enter the SMTP server. External DNS and external access for SMTP traffic is required for email notification of events and failures to function. Important: Make sure that you provide a valid SMTP server to ensure that the email notifications for events and failures.	`SMTP server? natoma`
Step 10: Notification email address?	Enter a valid email address to receive email notification of events and failures.	`Notification email address? example@example.com`
Step 11: Set the primary interface speed?	Enter the speed on the primary interface (that is, the SteelHead). Make sure that this value matches the settings on your router or switch. The default value is auto.	`Set the primary interface speed? [auto] auto`

Wizard Prompt	Description	Example
Step 12: Set the primary interface duplex?	Enter the duplex mode on the primary interface, and type a value at the system prompt. Make sure that this value matches the settings on your router or switch. The default value is auto.	`Set the primary interface duplex? [auto] auto`
Step 13: Would you like to activate the in-path configuration?	Enter `no` at the system prompt to configure in-path support. An in-path configuration is a configuration in which the SteelHead is in the direct path of the client and server. For detailed information about in-path configurations, see the *SteelHead Deployment Guide*.	`Would you like to activate the in path configuration? no`
Step 14: Would you like to activate the out-of-path configuration?	Enter `yes` at the system prompt to configure out-of-path support. An out-of-path configuration is a configuration in which the SteelHead is not in the direct path of the client and server. For detailed information about in-path configurations, see the *SteelHead Deployment Guide*.	`Would you like to activate the out-of-path configuration? [no] yes`

The system confirms your settings:

```
You have entered the following information:
Step 1: Hostname? amnesiac
Step 2: Use DHCP on primary interface? no
Step 3: Primary IP address? 10.10.10.6
Step 4: Netmask? 255.255.0.0
Step 5: Default gateway? 10.0.0.1
Step 6: Primary DNS server? 10.0.0.2
Step 7: Domain name? example.com
Step 8: Admin password? xxxyyyy
Step 9: SMTP server? natoma
Step 10: Notification email address? example@example.com
Step 11: Set the primary interface speed? auto
Step 12: Set the primary interface duplex? auto
Step 13. Would you like to activate the in-path configuration: no
Step 14: Would you like to activate the out-of-path configuration? yes

To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.
```

The SteelHead configuration wizard automatically saves your settings.

6. To log out of the system, enter the following command at the system prompt:

```
amnesiac> exit
```

For details on restarting the configuration wizard, see "To restart the configuration wizard" on page 29.

Configuring the Client-Side SteelHead

In an out-of-path configuration, you configure the client-side SteelHead in the same way as in an in-path configuration. For optimization to occur, you must define a fixed-target rule on the client-side SteelHead that points to the out-of-path, server-side SteelHead. You can define fixed-target rules using the Management Console or the CLI.

For detailed information about the Management Console, see the *SteelHead Management Console User's Guide*.

For detailed information about the CLI, see the *Riverbed Command-Line Interface Reference Manual*.

The following procedures describe how to configure in-path rules using the Management Console.

To configure the client-side SteelHead

1. Follow the procedures for an in-path configuration.

   For details, see "Configuring In-Path SteelHead Appliances" on page 24.

2. Connect to the Management Console.

   For details, see "Connecting to the Management Console" on page 31.

3. Choose Optimization > Network Services: In-Path Rules page.

4. Under In-Path Rules, click **Add a New In-Path Rule** to display the in-path rule configuration options.

5. For Type, select **Fixed-Target** from the drop-down list.

6. For Target Appliance IP Address, specify the IP address and port number for the peer SteelHead.

   Use one of these formats:

   XXX.XXX.XXX.XXX/XX (IPv4)

   X:X:X::X/XXX (IPv6)

   The IP address must be the primary Port IP address on the target SteelHead. The default port is 7810.

7. Optionally, if you have a backup, out-of-path SteelHead in your system (that is, failover support), for Backup Appliance IP Address, specify the IP address and port for the backup appliance in the Backup IP and Port text boxes.

   Use one of these formats:

   XXX.XXX.XXX.XXX/XX (IPv4)

   X:X:X::X/XXX (IPv6)

   The default port is 7810.

8. Click **Add** to apply the rule to the running configuration.

9. Click **Save** to write your settings to memory.

   For detailed information, see "Verifying You Are Connected to the SteelHead" on page 29 and "Verifying WAN Optimization" on page 32.

You can now optimize WAN traffic using the SteelHead.

CHAPTER 4 Troubleshooting

This chapter describes how to troubleshoot the SteelHead installation. This chapter describes how to troubleshoot the following issues:

Cables

Improper cabling prevents smooth traffic flows between the SteelHead and the router or switch.

Solution

To ensure that the traffic flows when the SteelHead is optimizing traffic, and when the SteelHead transitions to bypass mode, use the appropriate crossover or straight-through cable to connect the SteelHead to a router or switch. Verify the cable selection by removing the power cable from the appliance, and then test connectivity through it. Make sure that you have connected your cables as follows:

- SteelHead to router: crossover cable

- SteelHead to switch: straight-through cable
- SteelHead to SteelHead: crossover cable
- SteelHead to a host: crossover cable

Duplex Mismatch

The following symptoms occur due to a duplex mismatch:

- Access is not faster after configuring the SteelHead.
- The interface counters display error messages. An alarm or log message about error counts appears.
- The pass-through rule is ineffective. (This is a definite indication of duplex mismatch.)
- There are many retransmissions in packet traces.
- You cannot connect to an attached device.
- You can connect with a device when you choose auto-negotiation, but you cannot connect with the same device when you manually set the speed or duplex.
- Good performance for one direction of data flow, but poor performance in the opposite direction.

Possible Cause

- You have probably set the duplex value for your router to 100Full (fixed) and for the SteelHead to Auto.

Example

The following example shows applications that appear slower with SteelHeads configured in an in-path deployment. The timed performance numbers to transfer a 20-MB file over FTP are:

- no SteelHead – 3:16
- cold SteelHead – 5:08
- warm SteelHead – 3:46

Adding a pass-through rule for an application does not help. Slow connections appear as optimized in the Management Console on the Current Connections report page. However, stopping the SteelHead service while leaving the system powered on and an in-path configuration returns performance to original levels.

Solutions

To resolve the duplex mismatch error:

- Connect to the SteelHead CLI and enter the flood-ping command to check the duplex mismatch:

  ```
  ping -f -I >in-path-ip> -s 1400 <clientIP>
  ```

- Change the interface speed and duplex to match.
- Ensure there is a speed and duplex match between each in-path interface and its peer network interface. If they do not match, you might have a large number of errors on the interface when it is in the bypass mode, because the switch and the router are not set with the same duplex settings. Also, ensure connectivity when service is down.

If matching speed and duplex do not reduce collisions or errors, try hard-setting one end and auto-setting the other. Try the half-duplex mode.

- If all combinations fail, as a last resort, add an intermediary hub or switch that is more compatible with both network interfaces.

In-Path SteelHeads Connection

When there are SteelHeads with in-path connection issues, the two sites are connected in-path and you can ping them, but they cannot connect to each other to optimize data.

Possible Cause

The firewall is running port filtering and drops your probe packets. The firewall is filtering the IP and port address of the source and destination (bandwidth limitation) systems.

Solutions

To resolve the SteelHead connection issue:

- open port 7800 on both firewalls.
- use the port visibility mode.
- if there is no encryption, place the SteelHead after the firewall.

IP Address Configuration

If you have not configured IP addresses correctly, the SteelHeads cannot connect to each other or to your network.

Solutions

To verify the IP address has been configured correctly:

- Ensure the SteelHeads are reachable through the IP address, by pinging their primary and in-path interfaces.
- Ensure that the SteelHeads in the network can reach each other through their own interfaces.

  Connect to the SteelHead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*. Enter the following command to ping from a specific in-path interface on a SteelHead to another in-path interface:

  ```
  ping -f -I {Local-SteelHead-Inpath-IP} -s 1400 {Remote-SteelHead-Inpath-IP}
  ```

- Ensure that the default gateways, both for the SteelHead and for its in-path interfaces, are correct.
- For physical or virtual in-path installations, verify that the server-side SteelHead can be auto-discovered by the client-side SteelHead.

  Connect to the SteelHead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*. Enter the command:

  ```
  tproxytrace -i inpath0_0 <example-server-IP-address>:<example-server-TCP-port>
  ```

This causes the SteelHead to generate a fake TCP SYN packet, destined for the specified IP address and TCP port, and send it to the specified in-path interface. A remote SteelHead should respond if it sees the SYN packet.

- Verify that the client-side SteelHead is visible to the server-side SteelHead.

  Connect to the SteelHead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*. Enter the command:

  ```
  tproxytrace -i inpath0_0 <example-client-IP-address>: <example-client-TCP-port>
  ```

Asymmetric Routing

If there is an asymmetric routing issue, many connections fail during data transfer or they fail to start.

Possible Cause

Asymmetric routing occurs when a TCP connection takes one path to the destination and another when returning to the source. If the SteelHead sees only the LAN to WAN or only the WAN to LAN packets, it cannot optimize the data.

Solutions

To resolve the asymmetric routing issue, do one of the following:

- Rank the following solutions from most to least preferable with respect to complexity and cost and select one:
  - configure a fixed-target rule.
  - use a logical in-path configuration such as WCCP or PBR.
  - use four-port or six-port SteelHead.
  - configure connection-forwarding with two SteelHeads.
- Remove the asymmetry.

Packet Ricochet

The following symptoms occur due to packet ricochet:

- Performance is less than expected
- The following log message appears:

  ```
  » [fionr taelrcreeapdt/y lnoactaltekde rnceoln/neiccotireo.n c:119426.316]
  8.n7a3t._1c5h:e1c6k1: 1 SYN ==> packet 192.168.208.12:80 ==> 192.168.72.9:7801
  ```

Possible Cause

Traffic to the LAN is travelling to the WAN router on the way to the LAN.

Solutions

To resolve packet ricochet issues:

- Change the in-path gateway to the LAN router.
- Add static routes to LAN subnets through the LAN router.
- Enable in-path simplified routing.

Packet Ricochet: ICMP Redirects

The following symptoms occur due to packet ricochet Internet Control Messaging Protocol (ICMP) redirects:

- Connections fail on first attempt, but succeed on second attempt.
- On one or both sites, the in-path interface on the SteelHead is on a different network than the local host.
- There are no in-path routes defined.

Possible Causes

- Traffic to the LAN is traveling to the WAN router on the way to the LAN, but the router drops the packet.
- Outer connections to clients or servers are routed through the WAN interface to the WAN gateway, and then routed through the SteelHead to the next hop LAN gateway.
- The WAN router is probably dropping the SYN from the SteelHead before issuing an ICMP redirect.

Solutions

To resolve the packet ricochet ICMP redirects issue, do one of the following:

- Change the router ICMP configuration to forward the packet or turn off ICMP redirect.
- Change the in-path gateway to the LAN router.
- Add static routes to LAN subnets through the LAN router.
- Enable in-path simplified routing. For details, see "Simplified Routing" on page 41.
- Add in-path routes to local destinations to prevent the ICMP redirect and subsequent drop.

Simplified Routing

Simplified routing changes the process used to select the destination Ethernet address for packets transmitted from in-path interfaces.

Simplified routing collects the IP address for the next hop MAC address from each packet it receives to address traffic. With simplified routing, you can use either the WAN or LAN-side device as a default gateway. The SteelHead learns the right gateway to use by watching where the switch or router sends the traffic, and by associating the next-hop Ethernet addresses with IP addresses. Enabling simplified routing eliminates the need to add static routes when the SteelHead is in a different subnet from the client and the server.

Without simplified routing, if a SteelHead is installed in a different subnet from the client or server, you must define one router as the default gateway and static routes for the other routers so that traffic is not redirected back through the SteelHead. In some cases, even with the static routes defined, the Access Control List (ACL) on the default gateway can still drop traffic that should have gone through the other router. Enabling simplified routing eliminates this issue.

Simplified routing has the following constraints:

- You cannot enable WCCP.
- The default route must exist on each SteelHead in your network.

Tip: For detailed information, see the *SteelHead Deployment Guide*.

To enable simplified routing

1. Choose Networking > Network Integration: Simplified Routing to display the Simplified Routing page.
2. Under Mapping Data Collection Setting, complete the configuration as described in the following table.

Control	Description
Collect Mappings From	Select one of the following options from the drop-down list: • **None** - Do not collect mappings. • **Destination Only** - Collects destination MAC data. Use this option in connection-forwarding deployments. This is the default setting. • **Destination and Source** - Collect mappings from destination and source MAC data. Use this option in connection-forwarding deployments. • **All** - Collect mappings for destination, source, and inner MAC data. Also collect data for connections that are *un-natted* (connections that are not translated using NAT). You cannot enable this option in connection-forwarding deployments. Riverbed recommends that you use this option to maximize the effects of simplified routing.

3. Click **Apply** to save your settings to the running configuration.
4. Click **Save** to save your settings permanently.

Auto-Discovery Failure

When auto-discovery fails, all traffic passes through with the SteelHead in-path (physically or logically).

Possible Causes

- Cisco PIX 7.x or Raptor firewalls
- Satellite
- Intrusion Detection System (IDS) or Intrusion Prevention System (IPS)

Solutions

- Create a fixed-target rule on the client-side SteelHead.
  - Specify the **Target Appliance IP Address** and its port as 7800 on the opposite SteelHead (in-path without auto-discovery).
- Configure end nodes (firewalls) to allow your probe to pass through.
- Configure the SteelHead IP address as the friendly IP address for IDS or IPS.
- Cisco PIX Firewall IOS v7.0 might block the auto-discovery probe. Some firewall configurations strip TCP options or drop packets with these options. You can keep this configuration and switch to fixed-target rules or change the configuration on the firewall.

Protocol Optimization Errors

When there are protocol optimization errors, the SteelHead does not optimize expected protocols.

Solutions

To resolve protocol optimization errors, check:

- that connections have been successfully established.
- that SteelHeads on the other side of a connection are turned on.
- for secure or interactive ports that are preventing protocol optimization.
- for any pass-through rules that could be causing some protocols to pass through the SteelHeads unoptimized.
- that the LAN and WAN cables are not inadvertently swapped.

Server-Side Out-of-Path Connection Caveats

The following are the caveats for a server-side out-of-path (OOP) SteelHead connection:

- OOP configuration does not support auto-discovery. You must create a fixed-target rule on the client-side SteelHead.
- You must create an OOP connection from an in-path or logical in-path SteelHead and direct it to port 7810 on the primary interface of the server-side SteelHead. This setting is mandatory.
- Interception is not supported on the primary interface.
- An OOP configuration provides non-transparent optimization from the server perspective. Clients connect to servers, but servers treat it like a server-side SteelHead connection. This affects:

  - log files.
  - server-side ACLs.
  - bi-directional applications such as rsh.
- You can use OOP configurations along with in-path or logical in-path configurations.

Specific Problems

The following section describes specific problems you might encounter in the SteelHead.

Problem	Solution
The **show interfaces** CLI command displays 4294967295 as the number of errors on an interface.	The bypass card is not properly installed; reinstall it. For details, see the *Network Interface Card Installation Guide*.
The SteelHead blocks traffic when going into bypass mode.	If a SteelHead blocks traffic when going into bypass mode, verify that connections to its neighboring devices are correctly configured. Ensure that the cable from the SteelHead to the switch is a straight-through cable and the cable from the SteelHead to the router is a crossover cable. Also, ensure that there are no network speed or duplex mismatches.

The SteelHead does not come out of bypass mode when the network connection is restored.	If a SteelHead does not come out of bypass mode, verify that:
	• The in-path interface has an IP address. For example, at the system prompt, enter the **show interfaces** CLI command.
	• In-path interception is enabled. For example, at the system prompt, enter the **show in-path** CLI command. Expected results are:
	`Enabled: yes`
	`Optimizations Enabled On: inpath0_0`
	• The bypass service is running. For example, at the system prompt, enter the **show service** CLI command. To enable the SteelHead service if it is not running, use the CLI command **service enable**.
	• You have a valid and active SH10BASE license. Your license file should also contain entries for SH10CIFS and SH10EXCH licenses, even if they have not been activated. For example, at the system prompt, enter the **show licenses** CLI command. For questions about licenses, contact Riverbed Support at https://support.riverbed.com.

The SteelHead fails to boot.	Ensure that: • The power strip or the uninterruptable power supply (UPS) the SteelHead is plugged into is turned on and is functioning properly. • The rocker switch on the back of the SteelHead (Series xx20) is turned on. (When on, the rocker switch is in the depressed, or **1** position.)

Resetting a Lost Password

To reset your password, you must have access to the serial console or monitor and must be able to see the entire boot process to perform these steps:

1. Start, or reboot the appliance.
2. When prompted, press any key to continue.
3. Immediately press E. A GNU GRUB menu appears.
4. Press V or ^ to select the disk image to boot.
5. Press E.

   A GRUB menu appears, with options similar to the following:

```
-----------------
0: root (hd0,1)
1: kernel /vmlinuz ro root=/dev/sda5 console=tty0 console=ttyS0,9600n8
-----------------
```

6. Press V or ^ to select the kernel boot parameters entry.
7. Press E to edit the kernel boot parameters. The CLI displays a partially completed line of text similar to the following:

```
kernel /vmlinuz ro root=/dev/sda5 console=tty0 console=ttyS0,9600n8
```

8. The line of text contains two console= entries. Modify this line as follows:
   - If you are accessing the SteelHead remotely, delete

```
console=tty0
```

   - If you are accessing the SteelHead directly (through a keyboard and monitor connected to the appliance), delete

```
console=ttyS0
```

   - At the end of the line, type a space and append the line with

```
 single fastboot
```

   - You must include a space before the word **single**.

Tip: Use the arrow keys to access the entire command line.

9. Press Enter.
10. Press B to continue booting.
11. At the command prompt, enter `/sbin/resetpw.sh`.

    The password is blank.
12. Type **reboot** and press Enter to reboot the appliance.

Network Integration Checklist

Before you begin configuring the SteelHead, check the following configuration settings:

- Speed and duplex.
- QoS integration.
- Multi-hop optimization.
- Packet ricochet.
- VPN: Ensure the encryption is on the WAN side of the SteelHead.
- Firewall: Ensure probes are passed, especially Cisco PIX and Raptor. If inside the SteelHead, try probe caching for src IP rules; if outside, check firewall performance.
- In-path: Is it a VLAN trunk? (Configure trunking).
- Incorrectly designed load balancing implementations.
- Remove or manage asymmetry.
- Fail-to-wire or fail-to-block, you need Link State Protocol (LSP) for quicker convergence.
- WCCP or VLAN bridge: Router model and IOS revision.
- Does the network use Network Address Translation (NAT) or Port Address Translation (PAT).

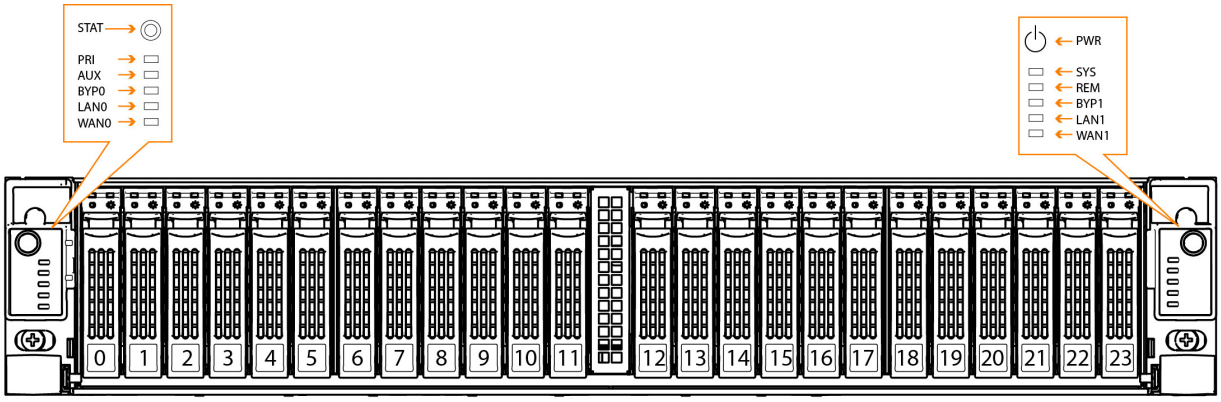
APPENDIX A SteelHead DX8000 Specifications

This appendix describes the status lights, ports, and the technical and environmental specifications for the SteelHead DX.

Status Lights and Ports

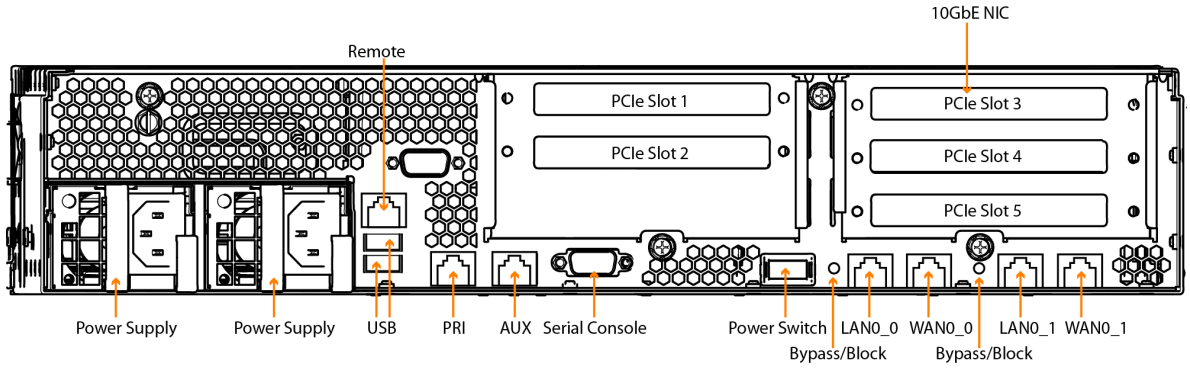
The following figure illustrates the status light and port locations.

Figure A-1. Front Panel



Disks 0 and 1 are HDD.

Figure A-2. Back Panel



The following table summarizes the system LEDs. For information about SteelHead DX NICs, see the *Network Interface Card Installation Guide*.

LED	Status
SYSTEM	Normal = Blue System Boot = Yellow
PRI = Primary **AUX = Auxiliary** **REM = Remote**	Link and Traffic = Blinks Blue
LAN-WAN	Link and Traffic = Blinks Blue
BYP/BLK **BYP = Bypass** **BLK = Block (Disconnect)**	Normal = No Light Bypass or Block (Disconnect) = Orange
HDDs	**Activity LED** Disk Connected = Blue Read/Write Activity = Blinks Blue **Disk Fault LED** Failed Disk = Orange
Back Panel **PRI = Primary** **AUX = Auxiliary** **REM = Remote**	**Left LED** Link = Green Activity = Blinks Green **Right LED** GB = Orange 100 MB = Green (REM only at 100 MB) 10 MB = No Light
Back Panel **LAN-WAN**	**Left LED** Link = Green Activity = Blinks Green **Right LED** GB = Orange 100 MB = Green 10 MB = No Light **BYP/BLK** Normal = No Light Bypass or Block (Disconnect) = Orange

Technical Specifications

The following table summarizes the technical specifications for the systems.

	DX8000
Form Factor	2 U
Hard Disk	2 x 500 GB HDD
RAM	128 GB
Dimensions (LxWxH)	25.4x17.2x3.43 in 645.4x436x87.1 mm
Weight (without packaging)	54 lbs/ 4.5 kg
Voltage Frequency	100-127V, 200-240V
PSU	2 x 770W 100-127Vac/8A, 50/60Hz 200-240Vac/4A, 50/60Hz
PCI Slots	3
Included Bypass Ports (GigE Copper)	4
Included Bypass Ports (10 GbE SR Fibre)	2
Max # Ports	18

Power Requirements and Consumption

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

System	**DX8000**
PSU Type	**2 x 770W**
AC Input	**230V**
Max. Amps.	2.8
Max. Watts	510
Typical Watts	410

System	DX8000
PSU Type	2 x 770W
AC Input	230V
Max VA	525
Power Factor	97
BTU (Typical)	1390

Environmental Specifications

The following table summarizes the environmental requirements for the systems.

	DX8000
Operating Acoustic	65.5 dBa Sound Pressure (Typical)
Temperature (Operating)	10º - 40º C 50° - 104º F
Temperature (Storage)	-40º - 65º C -40º - 149º F
Relative Humidity	20% - 80% non-condensing
Storage Humidity	5% - 95% non-condensing

Index