SteelHead™ Installation and Configuration Guide

SteelHead CX (x70), (xx70), (xx55)

Version 9.2

May 2016
Contents

Preface.....................................................................................................................................................7
  About This Guide .................................................................................................................................7
  Audience ...............................................................................................................................................7
  Document Conventions ......................................................................................................................8
  Documentation and Release Notes ...................................................................................................8
  Safety Guidelines ...............................................................................................................................8
  Contacting Riverbed ..........................................................................................................................9

Chapter 1 - Product Overview ...........................................................................................................11
  Prerequisites ......................................................................................................................................11
    Hardware and Software Dependencies ...........................................................................................11
    SCC Compatibility ............................................................................................................................12
    Virtual Services Platform (VSP) Support .........................................................................................12
    Firewall Requirements .....................................................................................................................12
    Ethernet Network Compatibility .......................................................................................................12
    SNMP-Based Management Compatibility ......................................................................................13
  Overview of the SteelHead ................................................................................................................13
    Configuring Optimization .................................................................................................................16
    Fail-to-Wire (Bypass) Mode ..............................................................................................................17
    Fail-to-Block (Disconnect) Mode ......................................................................................................18
  New Features in Version 9.2 ..............................................................................................................19
    Hostname-Based Interception Policy ............................................................................................19
    Hybrid Networking ..........................................................................................................................19
    Web Proxy .........................................................................................................................................20
    Applications ......................................................................................................................................20
    SSL ...................................................................................................................................................20
    Platforms .........................................................................................................................................21
  Upgrading RiOS to 9.2 .......................................................................................................................21
    User Permissions .............................................................................................................................21
    Upgrade Considerations ...................................................................................................................22
    Recommended Upgrade Paths ..........................................................................................................22
    Upgrading the RiOS Software Version ...........................................................................................23
Contents

Downgrading the RiOS Software Version.................................................................24

Chapter 2 - Managing Riverbed Licenses .................................................................25
  Riverbed Licensing Methods ..............................................................................25
  Automatic Licensing ..........................................................................................25
  Manual Licensing Using the Riverbed Licensing Portal ...........................................26
    Retrieving Licenses Using the Riverbed Licensing Portal .....................................27
  Installing Your License Keys ..............................................................................27

Chapter 3 - Installing and Configuring the SteelHead ..............................................29
  Choosing a Network Deployment .........................................................................29
  Checking Your Inventory ....................................................................................31
  Preparing Your Site for Installation ..................................................................33
    Site Requirements ..........................................................................................33
    SteelHead Ports ............................................................................................33
    Avoiding Duplex Mismatch ............................................................................34
    Bypass Card Interface Naming Conventions ....................................................35
    Completing the Configuration Checklist ........................................................35
  Powering On the System ....................................................................................36
    Securing the Power Cord on Desktop Systems ..................................................36
  Configuring In-Path SteelHeads .........................................................................37
    Connecting the SteelHead to Your Network ......................................................38
    Running the Configuration Wizard ..................................................................39
    Verifying You Are Connected to the SteelHead .................................................43
    Connecting to the Management Console ........................................................45
    Verifying WAN Optimization ..........................................................................46
    Checking for Speed and Duplex Errors ............................................................46
  Configuring Out-of-Path SteelHeads .................................................................47
    Connecting Out-of-Path SteelHeads to Your Network .......................................47
    Configuring the Server-Side SteelHead ............................................................47
    Configuring the Client-Side SteelHead .............................................................50

Chapter 4 - Troubleshooting ..................................................................................53
  Cables .................................................................................................................53
    Solution ............................................................................................................54
  Duplex Mismatch ...............................................................................................54
    Possible Cause .................................................................................................54
  In-Path SteelHeads Connection ..........................................................................55
    Possible Cause .................................................................................................55
  Oplock Issues .....................................................................................................55
    Possible Causes ...............................................................................................56
  CIFS Overlapping Open Optimization Denies Multi-User Access ............................56
Appendix C - SteelHead CX xx55 Appliance Specifications.................................................................81
Appendix B - SteelHead CX x70 Desktop Appliance Specifications ...................................................77
Appendix A - SteelHead CX xx70 Appliance Specifications.................................................................67
SteelHead Installation and Configuration Guide

Solution ..........................................................................................................................................................57
IP Address Configuration ..........................................................................................................................58
   Solutions .................................................................................................................................................58
Asymmetric Routing ................................................................................................................................59
   Possible Cause .......................................................................................................................................59
Packet Ricochet .......................................................................................................................................59
   Possible Cause .......................................................................................................................................60
Packet Ricochet: ICMP Redirects .............................................................................................................60
   Possible Causes .......................................................................................................................................60
Simplified Routing .....................................................................................................................................60
Autodiscovery Failure ...............................................................................................................................61
   Possible Causes .......................................................................................................................................61
Protocol Optimization Errors ....................................................................................................................62
   Solutions .................................................................................................................................................62
Server-Side Out-of-Path Connection Caveats ..........................................................................................62
Specific Problems ......................................................................................................................................63
Resetting a Lost Password .........................................................................................................................63
Network Integration Checklist ..................................................................................................................65

Appendix A - SteelHead CX xx70 Appliance Specifications.......................................................................67
CX3070 Specifications ...............................................................................................................................67
   Status Lights and Ports ...........................................................................................................................68
   Technical Specifications .........................................................................................................................70
   Power Requirements and Consumption ...............................................................................................71
   Environmental Specifications .................................................................................................................71
CX5070 and CX7070 Specifications .........................................................................................................71
   Status Lights and Ports ...........................................................................................................................72
   Technical Specifications .........................................................................................................................75
   Power Requirements and Consumption ...............................................................................................75
   Environmental Specifications .................................................................................................................76

Appendix B - SteelHead CX x70 Desktop Appliance Specifications .....................................................77
CX570 and CX770 Specifications ..............................................................................................................77
   Status Lights and Ports ...........................................................................................................................77
   Technical Specifications .........................................................................................................................79
   Environmental Specifications .................................................................................................................79

Appendix C - SteelHead CX xx55 Appliance Specifications.......................................................................81
CX255 Specifications ...............................................................................................................................81
   Status Lights and Ports ...........................................................................................................................81
   Technical Specifications .........................................................................................................................83
   Environmental Specifications .................................................................................................................83
Preface

Welcome to the *SteelHead Installation and Configuration Guide* for SteelHead CX. 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 these sections:

- “About This Guide” on page 7
- “Safety Guidelines” on page 8
- “Contacting Riverbed” on page 9

---

About This Guide

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

This guide includes information relevant to these products:

- Riverbed Optimization System (RiOS)
- Riverbed SteelHead (SteelHead)
- Riverbed SteelHead CX (SteelHead CX)
- Riverbed SteelHead (Virtual Appliance) (SteelHead-v)
- Riverbed SteelHead SaaS
- Riverbed command-line interface (CLI)

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.

This guide is also for users who are using the Riverbed command-line interface as described in the *Riverbed Command-Line Interface Reference Manual*. 
Document Conventions

This guide uses this standard set of typographical conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>italics</em></td>
<td>Within text, new terms and emphasized words appear in <em>italic</em> typeface.</td>
</tr>
<tr>
<td><strong>boldface</strong></td>
<td>Within text, CLI commands, CLI parameters, and REST API properties appear in <strong>bold</strong> typeface.</td>
</tr>
<tr>
<td>Courier</td>
<td>Code examples appear in Courier font:</td>
</tr>
<tr>
<td></td>
<td>amnesiac &gt; enable</td>
</tr>
<tr>
<td></td>
<td>amnesiac # configure terminal</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Values that you specify appear in angle brackets: <strong>interface <code>&lt;ip-address&gt;</code></strong></td>
</tr>
<tr>
<td><code>[ ]</code></td>
<td>Optional keywords or variables appear in brackets: <code>ntp peer </code>&lt;ip-address&gt;<code>&gt;</code> <code>[version </code>&lt;number&gt;<code>]</code></td>
</tr>
<tr>
<td><code>{ }</code></td>
<td>Elements that are part of a required choice appear in braces: `{&lt;interface-name&gt;</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
</tbody>
</table>

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.

**Note:** 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.

---

## 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. This chapter includes these sections:

- “Prerequisites” on page 11
- “Overview of the SteelHead” on page 13
- “New Features in Version 9.2” on page 19
- “Upgrading RiOS to 9.2” on page 21

Prerequisites

This section provides information about product dependencies and compatibility.

Hardware and Software Dependencies

This table summarizes the hardware and software requirements for the SteelHead.

<table>
<thead>
<tr>
<th>Riverbed Component</th>
<th>Hardware and Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteelHead</td>
<td>19-inch (483 mm) two-post or four-post rack.</td>
</tr>
<tr>
<td>SteelHead Management Console</td>
<td>Any computer that supports a Web browser with a color image display.</td>
</tr>
<tr>
<td></td>
<td>The Management Console has been tested with all versions of Chrome, Mozilla Firefox Extended Support</td>
</tr>
<tr>
<td></td>
<td>Release version 38, and Microsoft Internet Explorer 11.</td>
</tr>
<tr>
<td></td>
<td>The SteelCentral Controller for SteelHead has been tested with Mozilla Firefox Extended Support</td>
</tr>
<tr>
<td></td>
<td>Release version 38, and Microsoft Internet Explorer 11.</td>
</tr>
<tr>
<td></td>
<td>JavaScript and cookies must be enabled in your Web browser.</td>
</tr>
</tbody>
</table>


**SCC Compatibility**

To manage SteelHead 9.2 appliances, you need to use SCC 9.2. Earlier versions of the SCC do not support 9.2 SteelHeads. For details about SCC compatibility across versions, see the *SteelCentral Controller for SteelHead Installation Guide*.

**Virtual Services Platform (VSP) Support**

VSP is not supported on the Series xx55 hardware platforms. VSP is supported only on the EX Series xx60 hardware platforms. For detailed information about the SteelHead EX systems, see the *SteelHead EX Installation and Configuration Guide*.

**Firewall Requirements**

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

- Ports 7800 and 7810 must be open.
- Make sure your firewall doesn’t strip TCP options.

Secure transport requires communication on the management plane, control plane, and data plane. Consider the following port usage:

- The management plane requires communication between the SteelHead and the SCC on TCP port 9443 and TCP port 22.
- The control plane between the SteelHead acting as the controller and the SteelHeads acting as group members is over TCP port 9443.
- Encryption service flows over ESP (IP protocol 50). Or, if the network is public, over UDP port 4500.

**Ethernet Network Compatibility**

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

<table>
<thead>
<tr>
<th>Ethernet Standard</th>
<th>IEEE Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Logical Link Control (LLC)</td>
<td>IEEE 802.2 - 1998</td>
</tr>
<tr>
<td>Fast Ethernet 100BASE-TX</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Copper 1000BASE-T</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Fiber 1000BASE-SX (LC connector)</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Fiber 1000BASE-LX</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over Fiber 10GBASE-LR Single Mode</td>
<td>IEEE 802.3 - 2008</td>
</tr>
<tr>
<td>Gigabit Ethernet over 10GBASE-SR Multimode</td>
<td>IEEE 802.3 - 2008</td>
</tr>
</tbody>
</table>
The SteelHead ports support these connection types and speeds:

<table>
<thead>
<tr>
<th>Port</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary (PRI)</td>
<td>10/100/1000BASE-T, autonegotiating</td>
</tr>
<tr>
<td>Auxiliary (AUX)</td>
<td>10/100/1000BASE-T, autonegotiating</td>
</tr>
<tr>
<td>LAN</td>
<td>10/100/1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBase-LR, 10GBase-SR (depending on configuration)</td>
</tr>
<tr>
<td>WAN</td>
<td>10/100/1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBase-LR, 10GBase-SR (depending on configuration)</td>
</tr>
</tbody>
</table>

The SteelHead supports VLAN Tagging (IEEE 802.3 - 2008). It doesn’t support the ISL protocol.

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

**SNMP-Based Management Compatibility**

This product supports a proprietary Riverbed MIB accessible through SNMP. SNMPv1 (RFCs 1155, 1157, 1212, and 1215), SNMPv2c (RFCs 1901, 2578, 2579, 2580, 3416, 3417, and 3418), and SNMPv3 are supported, although some MIB items might only be accessible through SNMPv2 and SNMPv3.

SNMP support enables the product 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**

The causes for slow throughput in WANs are well known: high delay (round-trip time or latency), limited bandwidth, and chatty application protocols. 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. SteelHeads enable you to consolidate and centralize key IT resources to save money, reduce capital expenditures, simplify key business processes, and improve productivity.

With the SteelHead, 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.

RiOS uses these optimization techniques:
- **Data Streamlining** - SteelHeads and SteelHead Mobile 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 stored in the hard disk (RiOS data store) of the device running RiOS (a SteelHead or SteelHead Mobile host system). Each data chunk is assigned a unique integer label (reference) before it’s 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 (a SteelHead or SteelHead Mobile host system) uses this reference to find the original data chunk on its RiOS data store, and reconstruct the original TCP data stream.

- **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 acknowledgements, 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 supports a rich set of application protocols that includes but is not limited to Microsoft Exchange, CIFS, SMB, SharePoint, HTTP/HTTPS, Lotus Notes, FCIP, SRDF, and SnapMirror.
Path Selection for Hybrid Networking - These solutions maximize multiple WAN services based on business needs, service quality, and costs. Path selection redirects specific traffic or applications through one of three alternate paths determined by destination availability in cascading order. The path selection technology deterministically redirects select traffic and application flows through alternate networks based on service metrics, such as path availability, application priority, and policies you create.

- Traffic Classification - The SteelHead application flow engine, which covers more than 1,300 individual applications and processes, uses information to understand where data is coming from, which application sent it, and what function that application is trying to accomplish. The application flow engine utilizes a variety of techniques, often in combination, such as port-based classification, application signature matching, protocol dissection, behavioral classification, and others. Path selection classifies traffic using the full assortment of packet rules including IP addresses, 5-tuple, differentiated services code point (DSCP), TCP, user datagram protocol (UDP) port numbers, and so on. In this way, operators can instruct SteelHead solutions to precisely associate applications to networks based on their nature, performance requirements, and business criticality.

- Packet Forwarding - After the SteelHead has selected the right path, the next step is for it to steer traffic to the newly selected path. This operation is transparent to the client, server, and any networking devices such as routers or switches. RiOS forwards packets either directly using distinct SteelHead physical interfaces, or indirectly using (MAC) address rewriting. When these forwarding methods aren’t possible; for example, with virtual in-path deployments or where the SteelHead solution is not in the same Layer-2 domain, RiOS uses DSCP marking with upstream policy-based routing.

- Availability Monitoring - The SteelHead monitors end-to-end path availability and quality. You define the endpoint IP address for every path, and the SteelHead sends an Internet control message protocol (ICMP) ping every two seconds. To validate availability, each path can have a different remote host.

- Failover Management - If three consecutive pings are missed, the system considers the path to be unavailable, and selects the backup path. Every application has a default and a prioritized set of backup paths. Should the default path be unavailable, the higher-priority backup is instantly used (and then the lower one if needed). Operators can block certain types of applications when the primary path becomes unavailable, with a goal of reserving the remaining available bandwidth for more critical applications. As soon as the default path becomes available, traffic is routed back to it.
Management Streamlining - Management streamlining refers to the methods that Riverbed has developed to simplify the deployment and management of RiOS devices. These methods include:

- **Autodiscovery Process**, which enables SteelHeads and SteelHead Mobile to automatically find remote SteelHeads, and to then optimize traffic using them. Enhanced autodiscovery automatically discovers the last SteelHead in the network path of the TCP connection. Autodiscovery relieves you from having to manually configure large amounts of network information. The autodiscovery process enables administrators to control and secure connections, specify which traffic is to be optimized, and specify peers for optimization.

- **SteelCentral Controller for SteelHead (SCC)**, which automatically configures and monitors remote SteelHeads. It also gives you a single view of the overall benefit and health of the SteelHead network. SteelCentral Controller for SteelHead’s central management console dramatically improves the management and usability of control capabilities. The SCC features an intuitive interface and management plane based on high-level abstractions such as applications, sites, uplinks, or networks that match the way you view your IT environment. With SCC, you can implement new, more efficient configuration and change management workflows that make hybrid-networking capabilities truly usable at scale.

- **SteelCentral Controller for SteelHead Mobile (SCCM)**, which tracks the individual health and performance of each deployed software client, and manages enterprise client licensing. The SCCM enables you to see who is connected, view their data reduction statistics, and perform support operations such as resetting connections, pulling logs, and automatically generating traces for troubleshooting. You can perform all of these management tasks without end user input.

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

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 these types of in-path rule actions:

  - **Auto Discover** - Use the autodiscovery 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 autodiscovery 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 autodiscovery process and use 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. These types of peering rule are available:

- **Auto** - If the receiving SteelHead is not using enhanced autodiscovery, this has the same effect as the Accept peering rule action. If enhanced autodiscovery is enabled, the SteelHead only becomes the optimization peer if it’s 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 doesn’t 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’s 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’s a serious problem with the SteelHead or it’s 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 these 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 of the Management Console displays the Critical health icon next to the appliance name.
- 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 receive optimization; however, connections made during the fault aren’t optimized. 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 SteelHead 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 rerouted 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.

**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.

You set fail-to-block mode in the SteelHead CLI. For detailed information, see the SteelHead Deployment Guide.
New Features in Version 9.2

These new features are available in RiOS 9.2.

Hostname-Based Interception Policy

- **Logical Groups of Domain Names and Hostnames in In-Path Rules** - In-path rules recognize and process logical groups of domain names and hostnames using a single label that resolves to several IP addresses. This ability to group domain names and hostnames simplifies in-path rule management. One in-path rule replaces many. You can specify an Internet domain with wildcards to define a wider group. For example, a domain label called Office365 can be configured to match *.microsoftonline.com, *.office365.com, or *.office.com in a single in-path rule.

  A single rule can target a specific service such as SharePoint—even when the same IP address serves content for both SharePoint and Lync.

  You can also use host labels to populate the in-path destination with a set of IP addresses and subnets to the service.

Hybrid Networking

- **Performance and Scale Improvements** - You can define up to 500 sites for increased scale and configuration responsiveness. QoS, path selection, and secure transport can now handle up to 25 percent more optimized connections per second without classification errors.

- **Uplink Probe Enhancements** - The uplink probing techniques have been improved to:
  - leverage the SteelHead’s traffic awareness to accelerate probing to sites that are seeing traffic, while backing off probing for sites that are not seeing traffic. If an uplink isn’t currently in use, it isn’t probed.
  - avoid redundancy by probing only a subset of peers instead of probing all peers. For example, if there are four peers on a path that is up and actively seeing traffic, the probe monitors two peers instead of four. Also, the probes monitor only the uplinks referenced in a path selection rule. Subset probing is helpful with secure uplinks where both secure and nonsecure uplinks are created but aren’t referenced by a path selection rule.
  - enforce a rate limit on all probes the SteelHead sends, up to a maximum of 128 kilobits per second for each uplink by default. You can reduce the default maximum rate limit using the CLI or the SteelCentral Controller (SCC).

- **Path Selection Support for Transit Site Traffic** - Transit traffic is traffic that is not sourced or destined locally. For example, in a hub-and-spoke configuration with a static VPN setup, the SteelHead does not recognize traffic as being initiated by an external site and applies path selection rules for LAN-side traffic. The transit site path selection rules route return traffic outside the VPN tunnel, causing the firewall to drop packets. A new CLI command, `path-selection-transit-bypass`, pushes general path selection rules but selectively turns off path selection for transit site traffic. RiOS identifies transit traffic by checking subnets to determine whether the traffic is sourced or destined locally. This feature maintains the original path selection intent, including failure conditions, even when the traffic is routed through a transit site.
Path Selection with Interceptor (PSIC) Automatic Channel Configuration - To communicate efficiently, PSIC requires cluster channels between the SteelHead and SteelHead Interceptor appliances. Cluster channels are traditionally configured on the SteelHead. You can enable the PSIC automatic channel configuration feature using the SteelCentral Controller (SCC) to configure the cluster channels and then push the configuration to the appliances. No additional configuration tasks are required.

Web Proxy

Virtual In-Path Deployment - You can now use the Web proxy with virtual in-path deployments such as Web Cache Communication Protocol (WCCP) and policy-based routing (PBR).

Caching Enhancements:
- The cache content is persistent after reboots and service restarts.
- The individual object size limitation has been removed.
- An expanded cache storage space. The CX 555 and CX 755 models can use up to 50 GB of cache space for Web Proxy storage.

Host Label and Domain Label Integration with Web Proxy – You can use host labels and domain labels to define more granular traffic with the Web proxy service.

Additional Log Formats Support – An expanded request logging format improves visibility, debugging, and diagnostics.

Applications

SMB 3.1.1 Optimization - This feature includes Server Message Block (SMB) v3.1.1 dialect support when enabling SMBv3 on a SteelHead. SMBv3.1.1 was introduced by Microsoft in Windows 10 and Windows 2016. SMB v3.1.1 is only negotiated when systems of these operating system versions are directly connected. RiOS 9.2 supports SMB file sharing as well as Windows domain integration.


SMB Latency Optimization Support for MAC OS X 10.9 and 10.10 Client - RiOS provides SMBv2 and SMBv3 latency optimization support for Mac OS X clients.

Full MAPI over HTTP Optimization - RiOS includes application-level latency optimization for MAPI over HTTP in addition to the bandwidth optimization introduced in RiOS 9.1. This feature accelerates and reduces the data consumption across Microsoft Outlook and supports both cached exchange and online modes.

Expanded Exchange Server 2016 and Outlook 2016 Qualifications

SSL

TLS 1.2 Support - Transport Layer Security (TLS) 1.2 is enabled by default and upon upgrade for client-side and server-side SteelHeads for improved security.

OpenSSL 1.0.2 Support - The SteelHead support for the SSL protocol stack is based on OpenSSL 1.0.2. This version includes support for camillia ciphers, krb5 ciphers, and ECDHE cipher negotiation.

SafeNet Hardware Security Module (HSM) Support for SSL Certificates - You can store proxy private keys and certificates on SafeNet Luna HSM devices for SSL optimization.
SHA2 Support for Proxy Certificate - The SteelHead uses SHA-512 for proxy certificate signature hash.

Subject Alternative Name (SAN) with SSL Proxy Certificate - Includes Subject Alternative Name field checking when the SteelHead returns a proxy certificate.

Platforms

SteelHead (Virtual Edition) KVM Image - You can deploy a SteelHead (virtual edition) using a kernel-based virtual machine (KVM) image format. A KVM consists of a loadable kernel module that provides the core virtualization infrastructure and a processor-specific module that provides virtualization extensions running on a Linux kernel as a host. The support includes models up to and including VCX 1555H and requires no licensing changes.

New Microsoft Azure-Based Larger CCX Models - An Azure cloud CCX-SUB-PERF-TIER4 license can optimize Azure workloads up to 400 Mbps to Cloud IaaS while supporting a connection count of up to 30,000 connections per SteelHead. The SteelHead-c CCX runs as a virtual machine hosted in Azure infrastructure services.

Upgrading RiOS to 9.2

RiOS 9.2 is backward compatible with previous RiOS versions. However, to obtain the full benefits of the new features in RiOS 9.2, you must upgrade the client-side and server-side SteelHeads on any given WAN link. After you have upgraded all appliances, all the benefits of the 9.2 features and enhancements are available.

User Permissions

Upgrading from RiOS 8.6 to 9.0 and later requires additional user permissions for path selection and QoS. For example, a user with QoS read/write permission in a previous version will no longer have permission to configure a QoS rule. In 9.0 and later, a user needs read/write permission for Network Settings in addition to read/write permission for QoS.

This table summarizes the changes to the user permission requirements for RiOS 9.0 and later.

<table>
<thead>
<tr>
<th>Management Console Page</th>
<th>To Configure This Feature or Change This Section</th>
<th>Required Read Permission</th>
<th>Required Read/Write Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking &gt; Topology: Sites &amp; Networks</td>
<td>Networks</td>
<td>Network Settings Read-Only</td>
<td>Network Settings Read/Write</td>
</tr>
<tr>
<td></td>
<td>Sites</td>
<td>Network Settings Read-Only</td>
<td>QoS Read/Write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QoS Read-Only</td>
<td>QoS Read/Write</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Path Selection Read-Only</td>
<td>Path Selection Read/Write</td>
</tr>
<tr>
<td>Networking &gt; App Definitions: Applications</td>
<td>Applications</td>
<td>Network Settings Read-Only</td>
<td>Network Settings Read/Write</td>
</tr>
<tr>
<td>Networking &gt; Network Services: Quality of Service</td>
<td>Enable QoS</td>
<td>QoS Read-Only</td>
<td>QoS Read/Write</td>
</tr>
</tbody>
</table>
Product Overview

Upgrade Considerations

Consider the following before upgrading RiOS:

- You can’t upgrade Series x50 or xx50 hardware to RiOS version 9.2.
- If you mix RiOS software versions in your network, the releases might support different optimization features and you can’t take full advantage of the features that aren’t part of the older software versions.

Recommended Upgrade Paths

To find allowed upgrades between RiOS versions and recommended upgrade paths, use the Software Upgrade tool on the Riverbed Support site at https://support.riverbed.com. The tool includes all of the recommended intermediate RiOS versions.
Upgrading the RiOS Software Version

Follow these steps to upgrade your RiOS software. These instructions assume you are familiar with the SteelHead, the CLI, and the Management Console.

To upgrade the RiOS software version

1. Download the software image from the Riverbed Support site to a location such as your desktop. Optionally, in RiOS version 9.2, you can download a delta image directly from the Riverbed Support site to the SteelHead. The downloaded image includes only the incremental changes. The smaller file size means a faster download and less load on the network. To download a delta image, skip to step 2.

2. Log in to the Management Console using the Administrator account (admin).

3. Choose Administration > Maintenance: Software Upgrade page and choose one of these options:
   - **From URL** - Type the URL that points to the software image. Use one of these formats:
     http://host/path/to/file
     https://host/path/to/file
     ftp://user:password@host/path/to/file
     scp://user:password@host/path/to/file
   - **From Riverbed Support Site** - Select the target release number from the drop-down list to download a delta image directly to the appliance from the Riverbed Support site. The downloaded image includes only the incremental changes. You don’t need to download the entire image. The system downloads and installs the new image immediately after you click **Install**. To download and install the image later, schedule another date or time before you click **Install**.
   - **From Local File** - Browse your file system and select the software image.
   - **Schedule Upgrade for Later** - Select this check box to schedule an upgrade for a later time. Type the date and time in the Date and Time text boxes using these formats: YYYY/MM/DD and HH:MM:SS.

4. Click **Install** to immediately upload and install the software upgrade on your system, unless you schedule it for later.

   The software image can be quite large; uploading the image to the system can take a few minutes. Downloading a delta image directly from the Riverbed Support site is faster because the downloaded image includes only the incremental changes and is downloaded directly to the appliance.

   As the upgrade progresses, status messages appear.

   After the installation is complete, you are reminded to reboot the system to switch to the new version of the software.

5. Choose Administration > Maintenance: Reboot/Shutdown and click **Reboot**.

   The appliance can take a few minutes to reboot. This is normal behavior as the software is configuring the recovery flash device. Don’t press Ctrl-C, unplug, or otherwise shut down the system during this first boot. There’s no indication displayed during the system boot that the recovery flash device is being configured.

   After the reboot, the Dashboard, Software Upgrade, and Help pages of the Management Console display the RiOS version upgrade.
Downgrading the RiOS Software Version

If you are downgrading to a previous version of the RiOS software, you must downgrade to a version of the software that has previously run on your system.

**Note:** When downgrading from an image that supports four 10 GigE cards to an older image that doesn’t, the message `Updating BIOS. Do not interrupt or reboot till the command completes` appears. This message indicates that the appropriate BIOS for your software image is being installed.
This chapter describes the Riverbed licensing methods and how to manage Riverbed licenses. It includes these sections:

- “Riverbed Licensing Methods” on page 25
- “Automatic Licensing” on page 25
- “Retrieving Licenses Using the Riverbed Licensing Portal” on page 27
- “Installing Your License Keys” on page 27

### 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 these 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. For detailed information, see the respective installation guides for your 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 or by downloading and XML file to the SteelCentral Controller for SteelHead. For detailed information, see “Retrieving Licenses Using the Riverbed Licensing Portal” on page 27.

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

Note: 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 must have access to the Internet.

  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 don’t 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

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.
8. Optionally, if you are behind a firewall, click Download XML to download an XML file. The XML file can be imported by the SteelCentral Controller for SteelHead.

Note: 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 these 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 these sections:

- “Choosing a Network Deployment” on page 29
- “Checking Your Inventory” on page 31
- “Preparing Your Site for Installation” on page 33
- “Powering On the System” on page 36
- “Configuring In-Path SteelHeads” on page 37
- “Configuring Out-of-Path SteelHeads” on page 47

Note: 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 don’t 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.

![Physical In-Path Deployment](image1)

- **Virtual In-Path** - In a virtual in-path deployment, the SteelHead is virtually in the path between clients and servers. Traffic moves in and out of the same WAN interface, and the LAN interface is not used. This deployment differs from a physical in-path deployment in that a packet redirection mechanism, such as a SteelHead Interceptor, WCCP, policy based routing (PBR), or Layer-4 switching, directs packets to SteelHeads that aren’t in the physical path of the client or server. For details on the redirection mechanisms, see the SteelHead Deployment Guide.

![Virtual In-Path Deployment](image2)

- **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 aren’t possible. This deployment requires only a SteelHead primary interface to connect to the network. The SteelHead can be connected anywhere in the LAN.

![Out-of-Path Deployment](image3)
An out-of-path SteelHead deployment doesn’t use a redirecting mechanism. You configure fixed-target in-path rules for the client-side SteelHead. The fixed-target in-path rules point to the primary IP address of the out-of-path SteelHead. The out-of-path SteelHead uses its primary IP address when communicating to the server. The remote SteelHead must be deployed either in a physical or virtual in-path mode.

Figure 3-3. Out-of-Path Deployment

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Benefits</th>
<th>Requires</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical In-Path</td>
<td>Simple to configure and uses automatic discovery of peers.</td>
<td>In-path rules</td>
<td>Scaling, availability, cabling</td>
</tr>
<tr>
<td>Virtual In-Path</td>
<td>Limited physical disruption, routing forces traffic to WAN, automatic discovery of peers.</td>
<td>External setup to use PBR, WCCP, a SteelHead Interceptor, or Layer-4 switching</td>
<td>Dependent on the external configuration</td>
</tr>
<tr>
<td>Out-of-Path</td>
<td>The client-side SteelHead sends directly to the server-side SteelHead with no physical disruption. This configuration is typically used as a way to rapidly deploy a SteelHead in a site with very complex or numerous connections to the WAN.</td>
<td>Fixed-target rules</td>
<td>Requires explicit manual configuration. Connections initiated from the site with the out-of-path SteelHead can’t be optimized. Servers at the site detect the optimized traffic coming from the out-of-path SteelHead primary IP address instead of a client IP address.</td>
</tr>
</tbody>
</table>

Checking Your Inventory

Your shipping carton contains these 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 an 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 can’t 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 xx55
- 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 these requirements:

- It’s a standard electronic environment where the ambient temperature doesn’t exceed 40º C (104º F) and the relative humidity doesn’t exceed 80% (noncondensing). For detailed information, see the appendices that follow.
- Ethernet connections are available within the standard Ethernet limit.
- There’s 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 and 3U systems.

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

SteelHead Ports

This table summarizes the ports used to connect the SteelHead to your network.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Depending on your appliance, the Console port is either a DB9F port or an RJ45 port. (For port details for your appliance model, see the specification appendix for your product.) The appropriate console cable ships with your appliance. 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.</td>
</tr>
<tr>
<td>Primary (PRI)</td>
<td>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. The primary and auxiliary ports can’t share the same network subnet. The primary and in-path interfaces can share the same subnet. You must use the primary port on the server-side for out-of-path deployments.</td>
</tr>
</tbody>
</table>
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.

These can be signs of a duplex mismatch:
  - The Link Duplex alarm triggers.
  - On the Reports > Diagnostics: System Logs page you see errors for sends, receives, CRC, and short sends.
  - You can’t connect to an attached device.
  - You can connect to a device when you choose automatic negotiation, but you can’t 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.”

---

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auxiliary (AUX) | An optional port that provides an additional management interface for a secondary network. You can’t have the primary and auxiliary ports on the same subnet.  
The auxiliary and in-path interfaces can’t share the same network subnet.  
You can’t use the auxiliary port for out-of-path SteelHeads.  
This port is not available on the SteelHead model CX255. |
| 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.                                                                     |
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.

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

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Parameter</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteelHead (the Primary Interface)</td>
<td>Host name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Netmask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default gateway (the WAN gateway)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain name for the system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrator password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SMTP server IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events and failures notification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primary interface speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primary interface duplex</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>In-Path Deployments</th>
<th>In-path interface IP address</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In-path netmask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: LAN interface speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: LAN interface duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: WAN interface speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In-path: WAN interface duplex</td>
<td></td>
</tr>
</tbody>
</table>

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

This 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 3-5. 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 doesn’t 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 the appendices that follow.

Note: The SteelHead CX (Series xx55) takes approximately 10 minutes to boot.

Securing the Power Cord on Desktop Systems

The CX255 models include a power cord retention module. You can install this to reduce the risk of accidentally unplugging the power.
To install the power cord retention module

1. Push the retention module into the socket near the power connection.
   The socket is left of the power supply.

2. Attach the retention fastener to module and tighten around the power cable.

The retention module doesn’t prevent accidental pulls from removing the power cord, but it does provide increased protection.

Configuring In-Path SteelHeads

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 29.

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 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 3-6. Connecting the Primary Port to the LAN Switch**

   ![Diagram of connecting primary port to LAN switch](image)

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

   **Figure 3-7. Disconnecting the WAN Router**

   ![Diagram of disconnecting WAN router](image)

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

   **Figure 3-8. Connecting the LAN Switch to the LAN Port**

   ![Diagram of connecting LAN switch to LAN port](image)
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 3-9. Connecting the WAN Port to the WAN Router**

![Diagram showing WAN connection](image)

**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 Console port and a terminal.

   Depending on your appliance, the Console port is either a DB9F port or an RJ45 port. (For port details for your appliance model, see the specification appendix for your product.)

   The appropriate console cable ships with your appliance.

   **Figure 3-10. Connecting to the SteelHead**

   ![Console port types](image)

2. Start your terminal emulation program, such as Tera Term Pro. The terminal device must have these 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 have a SCC appliance installed in your network to manage multiple SteelHeads, you can use it to automatically configure them:

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

If you answer yes, you are prompted for the SCC host name or IP address. The host name or IP address is used to contact the SCC. The default value is riverbedcmc. If you enter no, the wizard continues.

**Note:** If you mistakenly answer yes, 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 42.

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 this table.

<table>
<thead>
<tr>
<th>Wizard Prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Host name?</td>
<td>Enter the host name for the SteelHead.</td>
<td>hostname? amnesiac</td>
</tr>
<tr>
<td>Step 2: Use DHCP on the primary interface?</td>
<td>You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the SteelHead.</td>
<td>Use DHCP? no</td>
</tr>
<tr>
<td></td>
<td>Riverbed recommends that you don’t set DHCP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default value is no.</td>
<td></td>
</tr>
<tr>
<td>Step 3: Primary IP address?</td>
<td>Enter the IP address for the SteelHead.</td>
<td>Primary IP address? 10.10.10.6</td>
</tr>
<tr>
<td>Step 4: Netmask?</td>
<td>Enter the netmask address.</td>
<td>Netmask? 255.255.0.0</td>
</tr>
<tr>
<td>Step 5: Default gateway?</td>
<td>Enter the default gateway for the SteelHead.</td>
<td>Default gateway? 10.0.0.1</td>
</tr>
<tr>
<td>Step 6: Primary DNS server?</td>
<td>Enter the primary DNS server IP address.</td>
<td>Primary DNS server? 10.0.0.2</td>
</tr>
<tr>
<td>Wizard Prompt</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Step 7: Domain name?</td>
<td>Enter the domain name for the network where the SteelHead is to reside.</td>
<td>Domain name? example.com</td>
</tr>
<tr>
<td></td>
<td>If you set a domain name, you can enter host names in the system without the domain name.</td>
<td></td>
</tr>
<tr>
<td>Step 8: Admin password?</td>
<td>Riverbed strongly recommends that you change the default administrator password at this time.</td>
<td>Admin password? xxyyyy</td>
</tr>
<tr>
<td></td>
<td>The default administrator password is password.</td>
<td></td>
</tr>
<tr>
<td>Step 9: SMTP server?</td>
<td>Enter the name of the SMTP server. External DNS and external access for SMTP traffic is required</td>
<td>SMTP server? natoma</td>
</tr>
<tr>
<td></td>
<td>for email notification of events and failures to function.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that you provide a valid SMTP server to ensure that the email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>notifications for events and failures.</td>
<td></td>
</tr>
<tr>
<td>Step 10: Notification email address?</td>
<td>Enter a valid email address to which notification of events and failures are to be sent.</td>
<td>Notification email address?</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:examples@example.com">examples@example.com</a></td>
<td><a href="mailto:examples@example.com">examples@example.com</a></td>
</tr>
<tr>
<td>Step 11: Set the primary interface speed?</td>
<td>Enter the speed on the primary interface (that is, the SteelHead). Make sure that this value</td>
<td>Set the primary interface</td>
</tr>
<tr>
<td></td>
<td>matches the settings on your router or switch.</td>
<td>speed? [auto] auto</td>
</tr>
<tr>
<td></td>
<td>The default value is auto.</td>
<td></td>
</tr>
<tr>
<td>Step 12: Set the primary interface duplex?</td>
<td>Enter the duplex mode on the primary interface. Make sure that this value matches the settings</td>
<td>Set the primary interface</td>
</tr>
<tr>
<td></td>
<td>on your router or switch. The default value is auto.</td>
<td>duplex? [auto] auto</td>
</tr>
<tr>
<td>Step 13: Would you like to activate the in-path</td>
<td>Enter yes at the system prompt to configure in-path support. An in-path configuration is a</td>
<td>Would you like to activate the</td>
</tr>
<tr>
<td>configuration?</td>
<td>configuration in which the SteelHead is in the direct path of the client and server. For</td>
<td>in-path configuration? yes</td>
</tr>
<tr>
<td></td>
<td>detailed information about in-path configurations, see the SteelHead Deployment Guide.</td>
<td></td>
</tr>
<tr>
<td>Step 14: In-Path IP address?</td>
<td>Enter the in-path IP address for the SteelHead.</td>
<td>In-Path IP address? 10.11.11.6</td>
</tr>
<tr>
<td>Step 15: In-Path Netmask?</td>
<td>Enter the in-path netmask address.</td>
<td>In-Path Netmask? 255.255.0.0</td>
</tr>
<tr>
<td>Step 16: In-Path Default gateway?</td>
<td>Enter the in-path default gateway (the WAN gateway).</td>
<td>In-Path Default Gateway? 10.11.11.16</td>
</tr>
</tbody>
</table>
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.

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.

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.

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.

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: xxyyy
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.

7. To log out of the system, enter this command at the system prompt:
   amnesiac> exit

To restart the configuration wizard
   Enter these 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 these 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 these devices:
   - An ASCII terminal or emulator that can connect to the serial console. It must have these 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 this command:
   
   \[
   \text{ssh admin@host.domain} \quad \text{or} \quad \text{ssh admin@ipaddress}
   \]

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:
   
   \[
   \text{ping -I <primary-IP-address> <primary-default-gateway>}
   \]

5. At the system prompt, ping from the in-path default gateway:
   
   \[
   \text{ping -I <in-path-IP-address> <in-path-default-gateway>}
   \]
If you have problems connecting to the SteelHead, use this flow chart to troubleshoot issues.

**Figure 3-11. Resolving IP Connectivity**

- **Start**
  - Connect Primary Interface
    - Primary Interface Pingable?
      - **YES**
        - SSH & Web to Primary Interface
      - **NO**
        - **Resolve IP Connectivity**
    - Repeat for Inpath0.1 (if applicable)
  - **Done**
    - **Check Cabling**
      - Check Web Interface for connections: Reports -> Networking: Current Connections
      - Connect LAN0.0 Interface
        - LAN0.0 Interface Pingable?
          - **YES**
            - Ping Default Gateway from Inpath Interface
              - Ping - 1 <inpath0_0> <gateway ip>
              - **Resolve IP Connectivity**
          - **NO**
            - **Check Web Interface for errors:** Reports -> Networking: Interface Counters
        - **NO**
          - **Resolve IP Connectivity**
    - **Gateway Pingable?**
      - **YES**
        - Connect WAN0.0 Interface
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>`

   The `<protocol>` variable is http or https. HTTPS uses the SSL protocol to ensure a secure environment. When you connect using HTTPS, the system prompts you to inspect and verify the SSL certificate. This is a self-signed certificate that provides encrypted Web connections to the Management Console. The system recreates the certificate when you change the appliance hostname or when the certificate expires.

   The secure vault doesn’t protect the self-signed certificate used with HTTPS connections.

   The `<host>` variable is the hostname you assigned to the SteelHead primary interface in the configuration wizard. If your DNS server maps that IP address to a name, you can specify the DNS name.

   The `<domain>` variable is the full domain name for the appliance.

---

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

---

The Management Console appears, displaying the Sign in page.

*Figure 3-12. Sign in Page*
2. In the Username text box, type the user login: admin, monitor, a signin from a RADIUS or TACACS+ database, or any local accounts created using the Role-Based Accounts feature. The default signin is admin.

Users with administrator (admin) privileges can configure and administer the SteelHead. Users with monitor privileges can view the SteelHead reports, view user logs, and change their own password. A monitor user can’t 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 Sign In to display the Dashboard.

The Dashboard summarizes the current status of your system.

Verifying WAN Optimization

Perform these 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 (cyclic redundancy check (CRC) or frame errors).

3. Go to the Administration > System Settings: Alarms page.

4. Check the link duplex and link I/O alarms.
If a link alarm status is degraded, choose Networking > Networking: Base Interfaces or Networking > Networking: In-path Interfaces and examine the SteelHead link configuration. Next, examine the peer switch user interface to check its link configuration. If the configuration on one side is different from the other, traffic is sent at different rates on each side, causing many collisions.

To troubleshoot, change both interfaces to automatic duplex negotiation. If the interfaces don’t support automatic duplex, configure both ends for full duplex.

You can enable or disable the alarm for a specific interface. To disable an alarm, choose Administration: System Settings > Alarms and select or clear the check box next to the link alarm.

### Configuring Out-of-Path SteelHeads

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 aren’t possible. For a detailed figure, see “Choosing a Network Deployment” on page 29. For detailed information about out-of-path deployments, see the SteelHead Deployment Guide.

#### Connecting Out-of-Path SteelHeads 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 3-13. 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 39.

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 don’t match, optimization might be degraded.

2. Connect to the CLI.

3. If you have a SteelCentral Controller for SteelHead (SCC) appliance installed in your network to manage multiple SteelHeads, you can use it to automatically configure them.

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

   If you enter yes, you are prompted for the SCC host name or IP address. The host name or IP address is used to contact the SCC. The default value is set to riverbedcontroller. If you enter no, the wizard continues.

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

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

   Note: 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 42.

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

<table>
<thead>
<tr>
<th>Wizard Prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Host name?</td>
<td>Enter the host name for the SteelHead.</td>
<td>Hostname? amnesiac</td>
</tr>
<tr>
<td>Step 2: Use DHCP on the primary interface?</td>
<td>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 don’t set DHCP. The default value is no.</td>
<td>Use DHCP? no</td>
</tr>
<tr>
<td>Step 3: Primary IP address?</td>
<td>Enter the IP address for the SteelHead.</td>
<td>Primary IP address? 10.10.10.6</td>
</tr>
<tr>
<td>Step 4: Netmask?</td>
<td>Enter the netmask address.</td>
<td>Netmask? 255.255.0.0</td>
</tr>
<tr>
<td>Step 5: Default gateway?</td>
<td>Enter the default gateway for the SteelHead.</td>
<td>Default gateway? 10.0.0.1</td>
</tr>
<tr>
<td>Step 6: Primary DNS server?</td>
<td>Enter the primary DNS server IP address.</td>
<td>Primary DNS server? 10.0.0.2</td>
</tr>
<tr>
<td>Step 7: Domain name?</td>
<td>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.</td>
<td>Domain name? example.com</td>
</tr>
<tr>
<td>Wizard Prompt</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Step 8: Admin password?</td>
<td>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 <strong>password</strong>.</td>
<td>Admin password? xxxyyy</td>
</tr>
<tr>
<td>Step 9: SMTP server?</td>
<td>Enter the SMTP server. External DNS and external access for SMTP traffic is required for email notification of events and failures to function. <strong>Note:</strong> Make sure that you provide a valid SMTP server to ensure receipt of email notifications for events and failures.</td>
<td>SMTP server? natoma</td>
</tr>
<tr>
<td>Step 10: Notification email address?</td>
<td>Enter a valid email address to receive email notification of events and failures.</td>
<td>Notification email address? <a href="mailto:example@example.com">example@example.com</a></td>
</tr>
<tr>
<td>Step 11: Set the primary interface speed?</td>
<td>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.</td>
<td>Set the primary interface speed? [auto] auto</td>
</tr>
<tr>
<td>Step 12: Set the primary interface duplex?</td>
<td>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.</td>
<td>Set the primary interface duplex? [auto] auto</td>
</tr>
<tr>
<td>Step 13: Would you like to activate the in-path configuration?</td>
<td>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.</td>
<td>Would you like to activate the in path configuration? no</td>
</tr>
<tr>
<td>Step 14: Would you like to activate the out-of-path configuration?</td>
<td>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.</td>
<td>Would you like to activate the out-of-path configuration? [no] yes</td>
</tr>
</tbody>
</table>

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 this command at the system prompt:
   amnesiac> exit

For details on restarting the configuration wizard, see “To restart the configuration wizard” on page 42.

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.

These 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 SteelHeads” on page 37.

2. Connect to the Management Console.
   For details, see “Connecting to the Management Console” on page 45.
3. Choose Optimization > Network Services: In-Path Rules.

**Figure 3-14. 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 about verifying your connections and configuration settings, see “Verifying You Are Connected to the SteelHead” on page 43 and “Verifying WAN Optimization” on page 46.

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 these issues:

- "Cables" on page 53
- "Duplex Mismatch" on page 54
- "In-Path SteelHeads Connection" on page 55
- "Oplock Issues" on page 55
- "CIFS Overlapping Open Optimization Denies Multi-User Access" on page 56
- "IP Address Configuration" on page 58
- "Asymmetric Routing" on page 59
- "Packet Ricochet" on page 59
- "Packet Ricochet: ICMP Redirects" on page 60
- "Autodiscovery Failure" on page 61
- "Protocol Optimization Errors" on page 62
- "Server-Side Out-of-Path Connection Caveats" on page 62
- "Specific Problems" on page 63
- "Resetting a Lost Password" on page 63
- "Network Integration Checklist" on page 65

---

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

For details, go to the Knowledge Base solution number S15298.

Duplex Mismatch

These symptoms occur due to a duplex mismatch:

- Access is not faster after configuring the SteelHead.
- The Link Duplex alarm triggers.
- 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 can’t connect to an attached device.
- You can connect with a device when you choose auto-negotiation, but you can’t 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 100 Full (fixed) and set the duplex value for the SteelHead to Auto.

Example

This 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 doesn’t 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’s a speed and duplex match between each in-path interface and its peer network interface. If they don’t match, you might have a large number of errors on the interface when it’s in the bypass mode, because the switch and the router aren’t set with the same duplex settings. Also, ensure connectivity when service is down.

  If matching speed and duplex don’t 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 can’t 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’s no encryption, place the SteelHead after the firewall.

---

Oplock Issues

These symptoms occur due to opportunistic lock (oplock) issues:

- File access is not faster or tasks such as drag-and-drop are fast but applications might benefit from acceleration.
- The Current Connections report page in the Management Console (select Reports > Networking: Current Connections) displays slow connections as optimized.
Possible Causes

- The client is running an old antivirus software such as McAfee v4.5, the most common type, which competes with the application for an oplock instead of opening as read-only. The antivirus causes multiple file opens.
- The server has oplocks disabled.

Example

You can open a previously-accessed file in 5 seconds on PC1, but you can’t open the same file under 24 seconds on PC2. If you close the file on PC1, you can open it in 5 seconds on PC2. However, it takes you 24 seconds to open the same file on PC1.

Solutions

Windows Common Internet File System (CIFS) uses oplock to determine the level of safety the OS or the application has in working with a file. Oplock is a lock that a client requests on a file in a remote server.

An oplock controls the consistency of optimizations such as read-ahead. Oplock levels are reduced when you make conflicting opens to a file.

To prevent any compromise to data integrity, the SteelHead only optimizes data when a client has exclusive access to the data.

When an oplock is not available, the SteelHead doesn’t perform application-level latency optimization but still performs scalable data referencing (SDR) and data compression as well as TCP optimization. Therefore, even without the benefits of latency optimization, SteelHeads still increase WAN performance, but not as effectively as when application optimizations are available.

To resolve oplock issues:

- Upgrade your antivirus software to the latest version.
- Use Filemon (sysinternals) to check for file access.
- Enable CIFS Overlapping Opens (by default, this function is enabled). For details, see “CIFS Overlapping Open Optimization Denies Multi-User Access” on page 56.
- Ensure that the server has oplock enabled by verifying registry settings on Windows servers or the Filer configuration (for NetApp or EMC servers).
- Run a network analyzer such as Riverbed SteelCentral Pilot, which is fully integrated with Wireshark, and determine that the server grants oplocks when the client opens a file.
- Check whether the client is running an antivirus software that is scanning the files over the WAN or that the antivirus software doesn’t break the oplock.

CIFS Overlapping Open Optimization Denies Multi-User Access

The CIFS overlapping open optimization issue prevents a client from accessing a file when different clients access the file at the same time.
Solution

To resolve the CIFS overlapping open optimization issue, configure CIFS overlapping open optimization on the client-side SteelHead as follows:

1. Connect to the SteelHead Management Console. For details, see “To connect to the Management Console” on page 45.

2. On the client-side SteelHead, choose Optimization: CIFS (SMB1) to display the CIFS (SMB1) page.

Figure 4-1. CIFS (SMB1) Page
3. Under Overlapping Open Optimization (Advanced), complete the configuration as described in this table.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Overlapping Open Optimization</td>
<td>Enables overlapping opens to obtain better performance with applications that perform multiple opens on the same file. For example, CAD applications. By default, this setting is disabled. Enable this setting on the client-side SteelHead. With overlapping opens enabled, the SteelHead optimizes data where exclusive access is available (when locks are granted). When an oplock is not available, the SteelHead doesn’t perform application-level latency optimizations but still performs SDR and compression on the data as well as TCP optimizations. If a remote user opens a file that is optimized using the overlapping opens feature and a second user opens the same file, they might receive an error message if it doesn’t go through a SteelHead. For example, certain applications that are sent over the LAN. If this occurs, you should disable overlapping opens for such applications. Use the radio buttons to set either an include list or exclude list of file types subject to overlapping opens optimization.</td>
</tr>
<tr>
<td>Optimize only the following extensions</td>
<td>Specify a list of extensions you want to include in overlapping opens optimization.</td>
</tr>
<tr>
<td>Optimize all except the following extensions</td>
<td>Specify a list of extensions you don’t want to include. For example, you should specify any file extensions that use Enable Applock Optimization.</td>
</tr>
</tbody>
</table>

4. Click **Apply** to apply your settings to the current configuration.

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

### IP Address Configuration

If you have not configured IP addresses correctly, the SteelHeads can’t 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 this 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.
Asymmetric Routing

If there’s 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 can’t optimize the data.

Solutions

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

- Rank these 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

These symptoms occur due to packet ricochet:

- Performance is less than expected
- This log message appears:

```bash
8.n7a3t_1c5h:e1c6k1: 1 SYN ==> packet 192.168.208.12:80 ==> 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
These 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 travelling 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 60.
- 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 these constraints:

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

For detailed information, see the SteelHead Deployment Guide.

**To enable simplified routing**


2. Under Mapping Data Collection Setting, complete the configuration as described in this table.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Mappings From</td>
<td>Select one of these options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong> - Don’t collect mappings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination Only</strong> - Collects destination MAC data. Use this option in</td>
</tr>
<tr>
<td></td>
<td>connection-forwarding deployments. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination and Source</strong> - Collect mappings from destination and source</td>
</tr>
<tr>
<td></td>
<td>MAC data. Use this option in connection-forwarding deployments.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All</strong> - Collect mappings for destination, source, and inner MAC data.</td>
</tr>
<tr>
<td></td>
<td>Also collect data for connections that are <em>un-natted</em> (connections that</td>
</tr>
<tr>
<td></td>
<td>aren’t translated using NAT). You can’t enable this option in</td>
</tr>
<tr>
<td></td>
<td>connection-forwarding deployments. Riverbed recommends that you use this</td>
</tr>
<tr>
<td></td>
<td>option to maximize the effects of simplified routing.</td>
</tr>
</tbody>
</table>

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

4. Click **Save** to save your settings permanently.

**Autodiscovery Failure**

When autodiscovery 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 autodiscovery).
- 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 7.0 might block the autodiscovery 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 doesn’t 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 aren’t inadvertently swapped.

---

**Server-Side Out-of-Path Connection Caveats**

Consider these the caveats for a server-side out-of-path (OOP) SteelHead connection:
- OOP configuration doesn’t support autodiscovery. 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.
Specific Problems

This section describes specific problems you might encounter in the SteelHead.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The show interfaces CLI command displays 4294967295 as the number of errors on an interface.</td>
<td>The bypass card is not properly installed; reinstall it. For details, see the Network Interface Card Installation Guide.</td>
</tr>
<tr>
<td>The SteelHead blocks traffic when going into bypass mode.</td>
<td>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.</td>
</tr>
</tbody>
</table>
| The SteelHead doesn’t come out of bypass mode when the network connection is restored. | If a SteelHead doesn’t 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:  
  ```
  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’s 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. |

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.
   - For a SteelHead upgraded to 4.0 from 2.0 or 3.0, the menu prompts you to select the Riverbed SteelHead, diagnostics, or a restore/recovery image. Select Riverbed SteelHead and skip to Step 5.
   - For a SteelHead manufactured with 4.0 (that has not had previous versions), the menu prompts you to select the disk image to use. Continue with Step 4.
   - For software versions prior to 4.0, the menu displays root and kernel parameters. Skip to Step 6.

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`.

```
Note: Use the arrow keys to access the entire command line.
```


10. Press B to continue booting.
    The system starts.

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 these configuration settings:

- Speed and duplex.
- QoS integration.
- Multihop 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)?
This appendix describes the status lights, ports, and the technical and environmental specifications for the xx70 appliances. It includes these sections:

- “CX3070 Specifications” on page 67
- “CX5070 and CX7070 Specifications” on page 71

CX3070 Specifications

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

Figures illustrate the status light and port locations.

**Figure A-1. CX3070 Front Panel with LEDs and Buttons**

**Figure A-2. CX3070 Back Panel**

**Note:** By default, the SteelHead CX3070 ships with a bypass card in slot 3. The default interface names are LAN3_0, WAN3_0, LAN3_1, and WAN3_1. This appliance doesn’t have an inpath0_0 interface as found on earlier appliances and by default the CX3070 uses inpath3_0 and inpath3_1.
This table summarizes the appliance LEDs and buttons.

<table>
<thead>
<tr>
<th>Reference</th>
<th>LED/Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 non-maskable 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         | Network Activity LED               | Link = Green  
Activity = Blinks Green. The blink rate is consistent with the amount of network activity.                                                                                                                                                       |
| 4         | System Cold Reset Button           | Pressing this button reboots the appliance.                                                                                                                                                              |
| 5         | 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. |
| 6         | Power Button with Integrated LED   | System On = Green  
System Off = No Light                                                                                                                                                                                |
| 7         | Drive Activity                     | Activity = Blinks Green                                                                                                                                                                                 |
| 8         | LEDs on Disk Drives               | Activity LED  
Read/Write Activity = Blinks Green  
Disk Fault LED  
Failed Disk = Orange  
RAID Rebuild = Blinks Orange                                                                                                                                                                   |
| 9         | 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                                                                                                           |
### Technical Specifications

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th>Reference</th>
<th>LED/Button</th>
<th>Description</th>
</tr>
</thead>
</table>
|           | 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  
Speed/Bypass/Disconnect Link/Activity |
|           | 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 |

<table>
<thead>
<tr>
<th></th>
<th><strong>CX3070 L/M/H</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>1U</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>2 x 1000 GB, 2 SSD x 160</td>
</tr>
<tr>
<td>Data Store</td>
<td>320 GB SSD</td>
</tr>
</tbody>
</table>
| Dimensions (LxWxH) | 25.21 x 17.24 x 1.7 in  
640.4 x 438 x 43.2 mm |
| Weight (without packaging) | 27 lbs / 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 Slots | 3 |
| Included Bypass Ports/Max # Ports | 4/12 |
Power Requirements and Consumption

This 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).

<table>
<thead>
<tr>
<th>System</th>
<th>CX3070</th>
<th>CX3070</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>All (L/M/H)</td>
<td>All (L/M/H)</td>
</tr>
<tr>
<td>PSU Type</td>
<td>2 x 450W</td>
<td>2 x 450W</td>
</tr>
<tr>
<td>AC Input</td>
<td>120V</td>
<td>230V</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>1.54</td>
<td>.76</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>152.8</td>
<td>145.4</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>122</td>
<td>116</td>
</tr>
<tr>
<td>Max VA</td>
<td>154</td>
<td>147</td>
</tr>
<tr>
<td>Power Factor</td>
<td>98.96</td>
<td>99.16</td>
</tr>
<tr>
<td>BTU (Typical)</td>
<td>417</td>
<td>397</td>
</tr>
</tbody>
</table>

Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th>CX3070</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
</tr>
<tr>
<td>Relative Humidity</td>
</tr>
</tbody>
</table>

CX5070 and CX7070 Specifications

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

These figures illustrate the status light and port locations.

**Figure A-3. CX5070 and CX7070 Front Panel with LEDs and Buttons**

Disks 0 and 23 are HDD. Disks 1 through 22 are SSD.

**Figure A-4. CX5070 and CX7070 Back Panel**

---

**Note:** By default, the SteelHead CX5070 and CX7070 ship with a bypass card in slot 1. The default interface names are LAN1_0, WAN1_0, LAN1_1, and WAN1_1. This appliance doesn’t have an inpath0_0 interface as found on earlier appliances and by default the CX5070 and CX7070 use inpath1_0 and inpath1_1.
This table summarizes the appliance LEDs and buttons.

<table>
<thead>
<tr>
<th>Reference</th>
<th>LED/Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 non-maskable 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 shown in Figure A-3. |
| 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 |
| 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 |
<table>
<thead>
<tr>
<th>Reference</th>
<th>LED/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEDs on Default 4 Port Copper Bypass Card</td>
<td>Link/Activity LED&lt;br&gt;Link = Green&lt;br&gt;Activity = Blinks Green</td>
<td>Speed/Bypass/Disconnect LED&lt;br&gt;1000Mbit/s = Yellow&lt;br&gt;100Mbit/s = Green&lt;br&gt;10Mbit/s = Off&lt;br&gt;Bypass = Blinks Green&lt;br&gt;Disconnect = Blinks Yellow</td>
</tr>
<tr>
<td>LEDs on Power Supply</td>
<td>Power On and Healthy = Green&lt;br&gt;Power Off = Off&lt;br&gt;Standby = Blinks Green&lt;br&gt;Power Lost But Second Power Supply Has Power = Amber&lt;br&gt;Power On With Warning Events (high temperature, high power, high current, slow fan) = Blinks Amber</td>
<td></td>
</tr>
</tbody>
</table>
## Technical Specifications

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX5070 M/H</th>
<th>CX7070 L</th>
<th>CX7070 M</th>
<th>CX7070 H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form Factor</strong></td>
<td>2 U</td>
<td>2 U</td>
<td>2 U</td>
<td>2 U</td>
</tr>
<tr>
<td><strong>Hard Disk/SSD</strong></td>
<td>2 x 1000 GB HDD</td>
<td>2 x 1000 GB HDD</td>
<td>2 x 1000 GB HDD</td>
<td>2 x 1000 GB HDD</td>
</tr>
<tr>
<td></td>
<td>6 x 160GB SSDs</td>
<td>6 x 300 GB SSDs</td>
<td>8 x 300 GB SSDs</td>
<td>16 x 300 GB SSDs</td>
</tr>
<tr>
<td><strong>Data Store</strong></td>
<td>960 GB SSD</td>
<td>1.8 TB SSD</td>
<td>2.4 TB SSD</td>
<td>4.8 TB SSD</td>
</tr>
<tr>
<td><strong>Dimensions (LxWxH)</strong></td>
<td>27.87 x 17.24 x 3.45 in</td>
<td>27.87 x 17.24 x 3.45 in</td>
<td>27.87 x 17.24 x 3.45 in</td>
<td>27.87 x 17.24 x 3.45 in</td>
</tr>
<tr>
<td></td>
<td>707.8 x 438 x 87.6 mm</td>
<td>707.8 x 438 x 87.6 mm</td>
<td>707.8 x 438 x 87.6 mm</td>
<td>707.8 x 438 x 87.6 mm</td>
</tr>
<tr>
<td><strong>Weight (without packaging)</strong></td>
<td>41 lbs/18.6 kg</td>
<td>41 lbs/18.6 kg</td>
<td>41 lbs/18.6 kg</td>
<td>42 lbs/19.05 kg</td>
</tr>
<tr>
<td><strong>Voltage Frequency</strong></td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
</tr>
<tr>
<td><strong>PSU</strong></td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
</tr>
<tr>
<td></td>
<td>100-127Vac/8.2A, 50/60Hz</td>
<td>100-127Vac/8.2A, 50/60Hz</td>
<td>100-127Vac/8.2A, 50/60Hz</td>
<td>100-127Vac/8.2A, 50/60Hz</td>
</tr>
<tr>
<td></td>
<td>200-240Vac/4.4A, 50/60Hz</td>
<td>200-240Vac/4.4A, 50/60Hz</td>
<td>200-240Vac/4.4A, 50/60Hz</td>
<td>200-240Vac/4.4A, 50/60Hz</td>
</tr>
<tr>
<td><strong>PCI Slots</strong></td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td><strong>Included Bypass Ports/Max # Ports</strong></td>
<td>4/20</td>
<td>4/20</td>
<td>4/20</td>
<td>4/20</td>
</tr>
</tbody>
</table>

## Power Requirements and Consumption

This 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).

<table>
<thead>
<tr>
<th>System</th>
<th>CX5070</th>
<th>CX5070</th>
<th>CX7070</th>
<th>CX7070</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td>All (M/H)</td>
<td>All (M/H)</td>
<td>All (L/M/H)</td>
<td>All (L/M/H)</td>
</tr>
<tr>
<td><strong>PSU Type</strong></td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
</tr>
<tr>
<td><strong>AC Input</strong></td>
<td>120V</td>
<td>230V</td>
<td>120V</td>
<td>230V</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>3.0</td>
<td>1.5</td>
<td>5.3</td>
<td>2.7</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>298</td>
<td>291</td>
<td>527</td>
<td>520</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>238</td>
<td>232</td>
<td>422</td>
<td>416</td>
</tr>
<tr>
<td>Max VA</td>
<td>301</td>
<td>293</td>
<td>533</td>
<td>524</td>
</tr>
<tr>
<td>Power Factor</td>
<td>98.96</td>
<td>99.16</td>
<td>98.96</td>
<td>99.16</td>
</tr>
<tr>
<td>BTU (Typical)</td>
<td>814</td>
<td>794</td>
<td>1439</td>
<td>1418</td>
</tr>
</tbody>
</table>
Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX5070</th>
<th>CX7070</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
<td>7.0 BA sound power (Typical)</td>
<td>7.0 BA sound power (Typical)</td>
</tr>
<tr>
<td></td>
<td>55 dBA sound pressure</td>
<td>55 dBA sound pressure</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
<td>10° - 35° C</td>
<td>10° - 35° C</td>
</tr>
<tr>
<td></td>
<td>50° - 95 F</td>
<td>50° - 95 F</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
<td>-40° - 70° C</td>
<td>-40° - 70° C</td>
</tr>
<tr>
<td></td>
<td>-40° - 158° F</td>
<td>-40° - 158° F</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>50% to 90%, non-condensing with a maximum wet bulb of 28 deg C (at</td>
<td>50% to 90%, non-condensing with a maximum wet bulb of 28 deg C (at</td>
</tr>
<tr>
<td></td>
<td>temperatures from 25 to 35 deg C)</td>
<td>temperatures from 25 to 35 deg C)</td>
</tr>
</tbody>
</table>
This appendix describes the status lights, ports, and the technical and environmental specifications for the x70 desktop systems.

**CX570 and CX770 Specifications**

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

**Status Lights and Ports**

This figure illustrates the status light and port locations.

*Figure B-1. Front Panel*
This table summarizes the system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>Healthy = Blue</td>
</tr>
<tr>
<td></td>
<td>Degraded = Yellow</td>
</tr>
<tr>
<td></td>
<td>Critical = Red</td>
</tr>
<tr>
<td></td>
<td>Power Off = None</td>
</tr>
<tr>
<td><strong>Power Button LED</strong></td>
<td>System Off = No Light</td>
</tr>
<tr>
<td></td>
<td>Standby Mode = Yellow</td>
</tr>
<tr>
<td></td>
<td>Power On = Blue</td>
</tr>
<tr>
<td><strong>Hard Drive LED</strong></td>
<td>Activity = Blinks Blue</td>
</tr>
<tr>
<td></td>
<td>Failed Disk = Orange</td>
</tr>
<tr>
<td><strong>Primary LED</strong></td>
<td>Left LED</td>
</tr>
<tr>
<td></td>
<td>Link = Green</td>
</tr>
<tr>
<td></td>
<td>Activity = Blinks Green</td>
</tr>
<tr>
<td></td>
<td>GB = Yellow</td>
</tr>
<tr>
<td></td>
<td>100 MB = Green</td>
</tr>
<tr>
<td></td>
<td>10 MB = No Light (with link on left LED)</td>
</tr>
<tr>
<td><strong>LAN/WAN LEDs</strong></td>
<td>Left LED</td>
</tr>
<tr>
<td></td>
<td>Link = Green</td>
</tr>
<tr>
<td></td>
<td>Activity = Blinks Green</td>
</tr>
<tr>
<td></td>
<td>Bypass/Disconnect = Yellow</td>
</tr>
<tr>
<td></td>
<td>Right LED</td>
</tr>
<tr>
<td></td>
<td>GB = Yellow</td>
</tr>
<tr>
<td></td>
<td>100 MB = Green</td>
</tr>
<tr>
<td></td>
<td>10 MB = No Light (with link on left LED)</td>
</tr>
</tbody>
</table>
# Technical Specifications

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX570 Desktop L-M-H</th>
<th>CX770 Desktop L-M-H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power (Typical)</strong></td>
<td>45 W</td>
<td>50 W</td>
</tr>
<tr>
<td><strong>VA (max)</strong></td>
<td>63.8</td>
<td>66.8</td>
</tr>
<tr>
<td><strong>BTU</strong></td>
<td>145 BTU</td>
<td>165 BTU</td>
</tr>
<tr>
<td><strong>Hard Disk</strong></td>
<td>1 x 320 GB 2.5” HDD</td>
<td>1 x 320 GB 2.5” HDD</td>
</tr>
<tr>
<td></td>
<td>1 x 80 GB SSD</td>
<td>1 x 160 GB SSD</td>
</tr>
<tr>
<td><strong>Data Store</strong></td>
<td>70 GB SSD</td>
<td>150 GB SSD</td>
</tr>
<tr>
<td><strong>Dimensions (LxWxH)</strong></td>
<td>13x8x1.73 in</td>
<td>13x8x1.73 in</td>
</tr>
<tr>
<td></td>
<td>330x204x44mm</td>
<td>330x204x44mm</td>
</tr>
<tr>
<td><strong>Weight (without packaging)</strong></td>
<td>5.5 lbs</td>
<td>5.5 lbs</td>
</tr>
<tr>
<td></td>
<td>2.4 kg</td>
<td>2.4 kg</td>
</tr>
<tr>
<td><strong>Voltage Frequency</strong></td>
<td>100-240V, 50 - 60 Hz</td>
<td>100-240V, 50 - 60 Hz</td>
</tr>
<tr>
<td><strong>PSU</strong></td>
<td>Single 84 W External 100-240Vac, 50/60Hz, 2-1 A</td>
<td>Single 84 W External 100-240Vac, 50/60Hz, 2-1 A</td>
</tr>
<tr>
<td><strong>Onboard Bypass Ports/ Max # Ports</strong></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

# Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX570 Desktop L-M-H</th>
<th>CX770 Desktop L-M-H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating Acoustic</strong></td>
<td>45 dBA Sound pressure (Typical)</td>
<td>45 dBA Sound pressure (Typical)</td>
</tr>
<tr>
<td><strong>Temperature (Operating)</strong></td>
<td>0º - 45º C, 32º - 113º F</td>
<td>0º - 45º C, 32º - 113º F</td>
</tr>
<tr>
<td><strong>Temperature (Storage)</strong></td>
<td>-40º - 65°C, -40º - 149º F</td>
<td>-40º - 65°C, -40º - 149º F</td>
</tr>
<tr>
<td><strong>Relative Humidity</strong></td>
<td>20% - 80% noncondensing</td>
<td>20% - 80% noncondensing</td>
</tr>
<tr>
<td><strong>Storage Humidity</strong></td>
<td>5% - 95% noncondensing</td>
<td>5% - 95% noncondensing</td>
</tr>
</tbody>
</table>
SteelHead CX xx55 Appliance Specifications

This appendix describes the status lights, ports, and the technical and environmental specifications for the xx55 appliances. It includes these sections:

- “CX255 Specifications” on page 81
- “CX555 and CX755 Specifications” on page 84
- “CX1555 Specifications” on page 86
- “CX5055 and CX7055 Specifications” on page 89

CX255 Specifications

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

Status Lights and Ports

This figure illustrates the status light and port locations.

Figure C-1. Front Panel
This table summarizes the system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>Healthy = Blue</td>
</tr>
<tr>
<td></td>
<td>Degraded = Yellow</td>
</tr>
<tr>
<td></td>
<td>Critical = Red</td>
</tr>
<tr>
<td></td>
<td>Power Off = None</td>
</tr>
<tr>
<td><strong>Power Button LED</strong></td>
<td>System Off = No Light</td>
</tr>
<tr>
<td></td>
<td>Standby Mode = Yellow</td>
</tr>
<tr>
<td></td>
<td>Power On = Blue</td>
</tr>
<tr>
<td><strong>Primary LED</strong></td>
<td>Left LED</td>
</tr>
<tr>
<td></td>
<td>Link = Green</td>
</tr>
<tr>
<td></td>
<td>Activity = Blinks Green</td>
</tr>
<tr>
<td></td>
<td>Right LED</td>
</tr>
<tr>
<td></td>
<td>GB = Yellow</td>
</tr>
<tr>
<td></td>
<td>100 MB = Green</td>
</tr>
<tr>
<td></td>
<td>10 MB = No Light (with link on left LED)</td>
</tr>
<tr>
<td><strong>LAN/WAN LEDs</strong></td>
<td>Left LED</td>
</tr>
<tr>
<td></td>
<td>Link = Green</td>
</tr>
<tr>
<td></td>
<td>Activity = Blinks Green</td>
</tr>
<tr>
<td></td>
<td>Bypass/Disconnect = Yellow</td>
</tr>
<tr>
<td></td>
<td>Right LED</td>
</tr>
<tr>
<td></td>
<td>GB = Yellow</td>
</tr>
<tr>
<td></td>
<td>100 MB = Green</td>
</tr>
<tr>
<td></td>
<td>10 MB = No Light (with link on left LED)</td>
</tr>
</tbody>
</table>
## Technical Specifications

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX255 Desktop P-U-L-M-H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong> (Typical)</td>
<td>30 W</td>
</tr>
<tr>
<td><strong>VA</strong> (max)</td>
<td>63.8</td>
</tr>
<tr>
<td><strong>BTU</strong></td>
<td>102 BTU</td>
</tr>
<tr>
<td><strong>Hard Disk</strong></td>
<td>320 GB</td>
</tr>
<tr>
<td><strong>Data Store</strong></td>
<td>50 GB</td>
</tr>
<tr>
<td><strong>Dimensions</strong> (LxWxH)</td>
<td>13x8x1.73 in</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weight (without packaging)</strong></td>
<td>5.5 lbs</td>
</tr>
<tr>
<td><strong>Voltage</strong> Frequency</td>
<td>100-240V</td>
</tr>
<tr>
<td><strong>PSU</strong></td>
<td>Single 84 W External</td>
</tr>
<tr>
<td></td>
<td>100-240Vac, 50/60Hz, 2-1 A</td>
</tr>
</tbody>
</table>

### Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX255</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating Acoustic</strong></td>
<td>45 dBA Sound pressure (Typical)</td>
</tr>
<tr>
<td><strong>Temperature (Operating)</strong></td>
<td>0º - 45º C</td>
</tr>
<tr>
<td><strong>Temperature (Storage)</strong></td>
<td>-40º - 65º C</td>
</tr>
<tr>
<td><strong>Relative Humidity</strong></td>
<td>20% - 80%</td>
</tr>
<tr>
<td><strong>Storage Humidity</strong></td>
<td>5% - 95%</td>
</tr>
</tbody>
</table>
CX555 and CX755 Specifications

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

Status Lights and Ports

This figure illustrates the status light and port locations.

Figure C-3. Front Panel

![Front Panel Diagram]

*Fail-to-Bypass (Bypass) and Fail-to-Block (Disconnect)

Figure C-4. Back Panel

![Back Panel Diagram]

This table summarizes the system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Healthy = Blue  Degraded = Yellow  Critical = Red System Boot = Yellow</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When the appliance is powered down with the power connected (for example, after running a <em>reload halt</em> command), the color of the system LED is undefined and carries no significance. The color can be either red, orange, or purple, depending on the state of the LED prior to shutdown.</td>
</tr>
<tr>
<td>HDD ACT</td>
<td>HDD Activity = Blinks Blue</td>
</tr>
</tbody>
</table>
### Technical Specifications

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX555 Desktop M-H</th>
<th>CX755 Desktop L-M-H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power (Typical)</strong></td>
<td>45 W</td>
<td>50 W</td>
</tr>
<tr>
<td><strong>VA (max)</strong></td>
<td>62.5</td>
<td>66.5</td>
</tr>
<tr>
<td><strong>BTU</strong></td>
<td>145 BTU</td>
<td>165 BTU</td>
</tr>
<tr>
<td><strong>Hard Disk</strong></td>
<td>2 x 250 GB</td>
<td>2 x 250 GB</td>
</tr>
<tr>
<td></td>
<td>H= 1 x 250 GB HDD + 1 x 160 SSD</td>
<td></td>
</tr>
<tr>
<td><strong>Data Store</strong></td>
<td>80 GB</td>
<td>100-160 GB</td>
</tr>
<tr>
<td><strong>Dimensions (LxWxH)</strong></td>
<td>7.1x12x1.65 in 180.3x304.8x42 mm</td>
<td>7.1x12x1.65 in 180.3x304.8x42 mm</td>
</tr>
<tr>
<td><strong>Weight (without packaging)</strong></td>
<td>4.7 lbs 2.15 kg</td>
<td>4.7 lbs 2.15 kg</td>
</tr>
<tr>
<td><strong>Voltage Frequency</strong></td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
</tr>
<tr>
<td><strong>PSU</strong></td>
<td>Single 100 W Internal 100-240Vac, 50/60Hz, 2-1 A</td>
<td>Single 100 W Internal 100-240Vac, 50/60Hz, 2-1 A</td>
</tr>
<tr>
<td><strong>Onboard Bypass Ports/Max # Ports</strong></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX555</th>
<th>CX755</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
<td>45 dBA Sound pressure</td>
<td>45 dBA Sound pressure</td>
</tr>
<tr>
<td>(Typical)</td>
<td>0º - 45º C</td>
<td>0º - 45º C</td>
</tr>
<tr>
<td></td>
<td>32º - 113º F</td>
<td>32º - 113º F</td>
</tr>
<tr>
<td>Temperature (Operating)</td>
<td>-40º - 65º C</td>
<td>-40º - 65º C</td>
</tr>
<tr>
<td></td>
<td>-40º - 149º F</td>
<td>-40º - 149º F</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>20% - 80% noncondensing</td>
<td>20% - 80% noncondensing</td>
</tr>
<tr>
<td>Storage Humidity</td>
<td>5% - 95% noncondensing</td>
<td>5% - 95% noncondensing</td>
</tr>
</tbody>
</table>

CX1555 Specifications

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

Status Lights and Ports

This figure illustrates the status light and port locations.

Figure C-5. Front Panel

Figure C-6. Back Panel
This table summarizes the system LEDs.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM</strong></td>
<td>Healthy = Blue</td>
</tr>
<tr>
<td></td>
<td>Degraded = Yellow</td>
</tr>
<tr>
<td></td>
<td>Critical = Red</td>
</tr>
<tr>
<td></td>
<td>System Boot = Yellow</td>
</tr>
<tr>
<td><strong>PRI = Primary</strong> <strong>AUX = Auxiliary</strong> <strong>REM = Remote</strong></td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td><strong>LAN-WAN</strong></td>
<td>Link and Traffic = Blinks Blue</td>
</tr>
<tr>
<td><strong>BYP/BLK</strong></td>
<td>Normal = No Light</td>
</tr>
<tr>
<td><strong>BYP = Bypass</strong></td>
<td>Bypass or Block (Disconnect) = Orange</td>
</tr>
<tr>
<td><strong>BLK = Block (Disconnect)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HDDs/SSDs</strong></td>
<td>Activity LED</td>
</tr>
<tr>
<td></td>
<td>Disk Connected = Blue</td>
</tr>
<tr>
<td></td>
<td>Read/Write Activity = Blinks Blue</td>
</tr>
<tr>
<td><strong>Back Panel</strong></td>
<td><strong>Left LED</strong></td>
</tr>
<tr>
<td><strong>PRI = Primary</strong> <strong>AUX = Auxiliary</strong> <strong>REM = Remote</strong></td>
<td><strong>Link = Green</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Activity = Blinks Green</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Right LED</strong></td>
</tr>
<tr>
<td></td>
<td><strong>GB = Orange</strong></td>
</tr>
<tr>
<td></td>
<td><strong>100 MB = Green (REM only at 100 MB)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>10 MB = No Light</strong></td>
</tr>
<tr>
<td></td>
<td><strong>BYP/BLK</strong></td>
</tr>
<tr>
<td></td>
<td>Normal = No Light</td>
</tr>
<tr>
<td></td>
<td>Bypass or Block (Disconnect) = Orange</td>
</tr>
</tbody>
</table>

**Technical Specifications**

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX1555 L/M</th>
<th>CX1555 H</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form Factor</strong></td>
<td>1 U</td>
<td>1U</td>
</tr>
<tr>
<td><strong>Hard Disk</strong></td>
<td>2 x 250 GB</td>
<td>2 x 500 GB, 2 SSD x 160</td>
</tr>
<tr>
<td><strong>Data Store</strong></td>
<td>400 GB</td>
<td>320 GB SSD</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>25.4x17.2x1.71 in</td>
<td>25.4x17.2x1.71 in</td>
</tr>
<tr>
<td></td>
<td>645.4x436x43.5 mm</td>
<td>645.4x436x43.5 mm</td>
</tr>
<tr>
<td><strong>Weight (without packaging)</strong></td>
<td>36 lbs</td>
<td>36 lbs</td>
</tr>
<tr>
<td></td>
<td>16.36 kg</td>
<td>16.36 kg</td>
</tr>
</tbody>
</table>
### Power Requirements and Consumption

This 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).

<table>
<thead>
<tr>
<th>System</th>
<th>CX1555 L/M</th>
<th>CX1555 H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>All (L/M/H)</td>
<td>All (L/M/H)</td>
</tr>
<tr>
<td>PSU Type</td>
<td>2 x 450 W</td>
<td>2 x 450 W</td>
</tr>
<tr>
<td>AC Input</td>
<td>120V</td>
<td>230V</td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>4.1</td>
<td>3.4</td>
</tr>
<tr>
<td>Max. Watts</td>
<td>220</td>
<td>220</td>
</tr>
<tr>
<td>Typical Watts</td>
<td>175</td>
<td>180</td>
</tr>
<tr>
<td>Max VA</td>
<td>225</td>
<td>265</td>
</tr>
<tr>
<td>Power Factor</td>
<td>97</td>
<td>92</td>
</tr>
<tr>
<td>BTU (Typical)</td>
<td>605</td>
<td>610</td>
</tr>
</tbody>
</table>

### Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th>System</th>
<th>CX1555 L/M</th>
<th>CX1555 H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Acoustic</td>
<td>61.6 dBA Sound Pressure (Typical)</td>
<td></td>
</tr>
<tr>
<td>Temperature (Operating)</td>
<td>10° - 40° C</td>
<td>50° - 104° F</td>
</tr>
<tr>
<td>Temperature (Storage)</td>
<td>-40° - 65° C</td>
<td>-40° - 149° F</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>20% - 80% noncondensing</td>
<td></td>
</tr>
<tr>
<td>Storage Humidity</td>
<td>5% - 95% noncondensing</td>
<td></td>
</tr>
</tbody>
</table>
CX5055 and CX7055 Specifications

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

Status Lights and Ports

This figure illustrates the status light and port locations.

Figure C-7. Front Panel

Disks 0 and 1 are HDD. Disks 2 through 23 are SSD.

Figure C-8. Back Panel

This table summarizes the system LEDs.

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

This table summarizes the technical specifications for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX5055 L/M</th>
<th>CX5055 L</th>
<th>CX7055 M</th>
<th>CX7055 H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>2 U</td>
<td>2 U</td>
<td>2 U</td>
<td>2 U</td>
</tr>
<tr>
<td>Hard Disk/SSD</td>
<td>2 x 500 GB HDD</td>
<td>2 x 500 GB HDD</td>
<td>2 x 500 GB HDD</td>
<td>2 x 500 GB HDD</td>
</tr>
<tr>
<td></td>
<td>8 x 80GB SSDs</td>
<td>10 x 160 GB SSDs</td>
<td>15 x 160 GB SSD</td>
<td>16 x 300 GB SSD</td>
</tr>
<tr>
<td>Data Store</td>
<td>640 GB SSD</td>
<td>1.6 TB SSD</td>
<td>2.4 TB SSD</td>
<td>4.8 TB SSD</td>
</tr>
<tr>
<td>Dimensions</td>
<td>25.4x17.2x3.43 in</td>
<td>25.4x17.2x3.43 in</td>
<td>25.4x17.2x3.43 in</td>
<td>25.4x17.2x3.43 in</td>
</tr>
<tr>
<td></td>
<td>645.4x436x87.1 mm</td>
<td>645.4x436x87.1 mm</td>
<td>645.4x436x87.1 mm</td>
<td>645.4x436x87.1 mm</td>
</tr>
<tr>
<td>Weight (without packaging)</td>
<td>52 lbs/23.6 kg</td>
<td>54 lbs/24.5 kg</td>
<td>54 lbs/24.5 kg</td>
<td>54 lbs/ 4.5 kg</td>
</tr>
<tr>
<td>Voltage Frequency</td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
<td>100-127V, 200-240V</td>
</tr>
<tr>
<td>PSU</td>
<td>2 x 770W</td>
<td>770W</td>
<td>770W</td>
<td>770W</td>
</tr>
<tr>
<td></td>
<td>100-127Vac/8A, 50/60Hz</td>
<td>100-127Vac/8A, 50/60Hz</td>
<td>100-127Vac/8A, 50/60Hz</td>
<td>100-127Vac/8A, 50/60Hz</td>
</tr>
<tr>
<td></td>
<td>200-240Vac/4A, 50/60Hz</td>
<td>200-240Vac/4A, 50/60Hz</td>
<td>200-240Vac/4A, 50/60Hz</td>
<td>200-240Vac/4A, 50/60Hz</td>
</tr>
<tr>
<td>PCI Slots</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Onboard Bypass Ports/Max # Ports</td>
<td>4/20</td>
<td>4/20</td>
<td>4/20</td>
<td>4/20</td>
</tr>
</tbody>
</table>

Power Requirements and Consumption

This 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).

<table>
<thead>
<tr>
<th>System</th>
<th>Configuration</th>
<th>CX5055</th>
<th>CX5055</th>
<th>CX7055</th>
<th>CX7055</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All (M/H)</td>
<td>All (M/H)</td>
<td>All (L/M/H)</td>
<td>All (L/M/H)</td>
<td></td>
</tr>
<tr>
<td>PSU Type</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td>2 x 770W</td>
<td></td>
</tr>
<tr>
<td>AC Input</td>
<td>120V</td>
<td>230V</td>
<td>120V</td>
<td>230V</td>
<td></td>
</tr>
<tr>
<td>Max. Amps.</td>
<td>4.9</td>
<td>2.5</td>
<td>5.3</td>
<td>2.8</td>
<td></td>
</tr>
<tr>
<td>Max. Watts</td>
<td>470</td>
<td>465</td>
<td>525</td>
<td>510</td>
<td></td>
</tr>
<tr>
<td>Typical Watts</td>
<td>375</td>
<td>375</td>
<td>420</td>
<td>410</td>
<td></td>
</tr>
<tr>
<td>Max VA</td>
<td>480</td>
<td>480</td>
<td>530</td>
<td>525</td>
<td></td>
</tr>
<tr>
<td>Power Factor</td>
<td>98</td>
<td>97</td>
<td>98</td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>BTU (Typical)</td>
<td>1280</td>
<td>1275</td>
<td>1425</td>
<td>1390</td>
<td></td>
</tr>
</tbody>
</table>
## Environmental Specifications

This table summarizes the environmental requirements for the systems.

<table>
<thead>
<tr>
<th></th>
<th>CX5055</th>
<th>CX7055</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating Acoustic</strong></td>
<td>65.5 dBA Sound Pressure (Typical)</td>
<td>65.5 dBA Sound Pressure (Typical)</td>
</tr>
<tr>
<td><strong>Temperature (Operating)</strong></td>
<td>10°C - 40°C</td>
<td>10°C - 40°C</td>
</tr>
<tr>
<td></td>
<td>50°F - 104°F</td>
<td>50°F - 104°F</td>
</tr>
<tr>
<td><strong>Temperature (Storage)</strong></td>
<td>-40°C - 65°C</td>
<td>-40°C - 65°C</td>
</tr>
<tr>
<td></td>
<td>-40°F - 149°F</td>
<td>-40°F - 149°F</td>
</tr>
<tr>
<td><strong>Relative Humidity</strong></td>
<td>20% - 80% noncondensing</td>
<td>20% - 80% noncondensing</td>
</tr>
<tr>
<td><strong>Storage Humidity</strong></td>
<td>5% - 95% noncondensing</td>
<td>5% - 95% noncondensing</td>
</tr>
</tbody>
</table>