

# **Steelhead® Appliance Installation and Configuration Guide**

Steelhead® CX (Series xx55)  
Steelhead® (Series xx20, xx50)

Version 6.5.4

February 2012



© 2012 Riverbed Technology. All rights reserved.

Riverbed®, Cloud Steelhead®, Granite™, Interceptor®, RiOS®, Steelhead®, Think Fast®, Virtual Steelhead®, Whitewater®, Mazu®, Cascade®, Cascade Pilot™, Shark®, AirPcap®, SkipWare®, TurboCap®, WinPcap®, Wireshark®, and Stingray™ are trademarks or registered trademarks of Riverbed Technology, Inc. in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed Technology or their respective owners.

Akamai® and the Akamai wave logo are registered trademarks of Akamai Technologies, Inc. SureRoute is a service mark of Akamai. Apple and Mac are registered trademarks of Apple, Incorporated in the United States and in other countries. Cisco is a registered trademark of Cisco Systems, Inc. and its affiliates in the United States and in other countries. EMC, Symmetrix, and SRDF are registered trademarks of EMC Corporation and its affiliates in the United States and in other countries. IBM, iSeries, and AS/400 are registered trademarks of IBM Corporation and its affiliates in the United States and in other countries. Linux is a trademark of Linus Torvalds in the United States and in other countries. Microsoft, Windows, Vista, Outlook, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and in other countries. Oracle and JInitiator are trademarks or registered trademarks of Oracle Corporation in the United States and in other countries. UNIX is a registered trademark in the United States and in other countries, exclusively licensed through X/Open Company, Ltd. VMware, ESX, ESXi are trademarks or registered trademarks of VMware, Incorporated in the United States and in other countries.

Parts of this product are derived from the following software:

Apache © 2000-2003. The Apache Software Foundation. All rights reserved.

Busybox © 1999-2005 Eric Andersen

ethtool © 1994, 1995-8, 1999, 2001, 2002 Free Software Foundation, Inc

Less © 1984-2002 Mark Nudelman

Libevent © 2000-2002 Niels Provos. All rights reserved.

LibGD, Version 2.0 licensed by Boutell.Com, Inc.

Libtecla © 2000, 2001 by Martin C. Shepherd. All rights reserved.

Linux Kernel © Linus Torvalds

login 2.11 © 1993 The Regents of the University of California. All rights reserved.

md5, md5.cc © 1995 University of Southern California, © 1991-2, RSA Data Security, Inc.

my\_getopt.{c,h} © 1997, 2000, 2001, 2002, Benjamin Sittler. All rights reserved.

NM SDK, v4.0P1, © 2008 Netapp Inc. All rights reserved.

NET-SNMP © 1989, 1991, 1992 by Carnegie Mellon University. All rights reserved. Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California. All rights reserved.

OpenSSH © 1983, 1990, 1992, 1993, 1995, 1993 The Regents of the University of California. All rights reserved.

pam © 2002-2004 Tall Maple Systems, Inc. All rights reserved.

pam-radius © 1989, 1991 Free Software Foundation, Inc.

pam-tacplus © 1997-2001 by Pawel Krawczyk

sscep © 2003 Jarkko Turkulainen. All rights reserved.

ssmtp © GNU General Public License

syslogd © 2002-2005 Tall Maple Systems, Inc. All rights reserved.

Vixie-Cron © 1988, 1990, 1993, 1994 by Paul Vixie. All rights reserved.

Zile © 1997-2001 Sandro Sigalam © 2003 Reuben Thomas. All rights reserved.

This product includes software developed by the University of California, Berkeley (and its contributors), EMC, and Comtech AHA Corporation. This product is derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

NetApp Manageability Software Development Kit (NM SDK), including any third-party software available for review with such SDK which can be found at <http://communities.netapp.com/docs/DOC-3777>, and are included in a NOTICES file included within the downloaded files. For detailed copyright and license agreements or modified source code (where required), see the Riverbed Support site at <https://support.riverbed.com>. Certain libraries were used in the development of this software, licensed under GNU Lesser General Public License, Version 2.1, February 1999. For a list of libraries, see the Riverbed Support at <https://support.riverbed.com>. You must log in to the support site to request modified source code.

This documentation is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.



Riverbed Technology  
199 Fremont Street  
San Francisco, CA 94105

Phone: 415.247.8800

Fax: 415.247.8801

Web: <http://www.riverbed.com>

Part Number  
712-00001-13

# Contents

- Chapter 1 - Overview of the Steelhead Appliance ..... vii**
- Overview of the Steelhead Appliance ..... vii
  - Auto-Discovery Process..... ix
  - Configuring Optimization.....x
  - Fail-to-Wire (Bypass) Mode.....x
  - Fail-to-Block (Disconnect) Mode..... xi
- New Features in Version 6.5.4..... xi
- Upgrading RiOS to Version 6.5.4..... xii
  - Upgrading RiOS Software..... xii
  - Downgrading the Software ..... xiii
  
- Preface..... 7**
- About This Guide .....7
  - Audience .....7
  - Document Conventions.....8
- Product Dependencies and Compatibility.....8
  - Hardware and Software Dependencies.....9
  - CMC Compatibility .....9
  - RSP Services 32-Bit and 64-Bit Support.....10
  - Firewall Requirements .....10
  - Ethernet Network Compatibility .....10
  - SNMP-Based Management Compatibility.....11
  - Antivirus Compatibility .....11
- Additional Resources .....11
  - Release Notes .....12
  - Riverbed Documentation and the Support Knowledge Base .....12
- Safety Guidelines .....12
- Contacting Riverbed.....12
  - Internet .....13
  - Technical Support .....13
  - Professional Services .....13
  - Documentation.....13

<b>Chapter 2 - Managing Riverbed Licenses .....</b>	<b>15</b>
Riverbed Licensing Methods .....	15
Automatic Licensing .....	16
Flexible Licensing .....	16
Installing Licenses .....	18
Retrieving Licenses Using the Riverbed Licensing Portal .....	20
Installing Your License Keys .....	22
<b>Chapter 3 - Installing and Configuring the Steelhead Appliance.....</b>	<b>23</b>
Choosing a Network Deployment .....	23
Checking Your Inventory.....	25
Preparing Your Site for Installation.....	26
Completing the Configuration Checklist .....	26
Steelhead Appliance Ports.....	28
Bypass Card Interface Naming Conventions .....	28
Powering On the Steelhead Appliance.....	29
Connecting to the Steelhead Appliance .....	30
Configuring In-Path Steelhead Appliances .....	31
Avoiding Duplex Mismatch.....	31
Configuration Wizard .....	31
Connecting the Steelhead Appliance to Your Network.....	35
Verifying Your Connections .....	36
Connecting to the Management Console .....	38
Verifying Your Configuration .....	39
Configuring Out-of-Path Steelhead Appliances .....	40
Before You Begin.....	40
Connecting the Steelhead Appliance to Your Network.....	43
Configuring the Client-Side Appliance.....	43
<b>Chapter 4 - Troubleshooting.....</b>	<b>45</b>
Troubleshooting .....	45
Cables .....	45
Duplex Mismatch .....	46
In-Path Steelhead Appliances Connection.....	47
Oplock Issues .....	47
CIFS Overlapping Open Optimization Denies Multi-User Access .....	48
IP address Configuration.....	50
Asymmetric Routing.....	50
Packet Ricochet .....	51
Packet Ricochet—Internet Control Messaging Protocol (ICMP) Redirects.....	51
Auto-Discovery Failure .....	53
Protocol Optimization Errors.....	54
Server-Side Out-of-Path Connection Caveats .....	54
Specific Problems.....	55

Resetting a Lost Password.....	55
Network Integration Checklist .....	56
<b>Appendix A - Series xx55 Status Lights and Ports, Technical Specifications.....</b>	<b>59</b>
CX555 and CX755 Status Lights and Ports.....	60
CX1555 Status Lights and Ports.....	62
System LEDs.....	62
CX555 and CX755 Technical Specifications.....	63
CX1555 Technical Specifications.....	64
CX1555 Power Requirements and Consumption .....	64
Environmental Specifications .....	64
<b>Appendix B - Series xx50 Status Lights and Ports, Technical Specifications.....</b>	<b>65</b>
Series xx50 Status Lights and Ports.....	65
Series 250 and 550.....	65
Series 1050 and 2050.....	66
Power Supply LEDs .....	68
Series 5050 and 6050.....	68
Series 7050.....	70
Series xx50 Bypass Cards Status Lights.....	71
Bypass Card Manufacturing Numbers Series xx50.....	72
Four-Port 1GbE TX Copper NIC .....	72
Four-Port 1GbE SX Multi Mode Fiber NIC.....	73
Four-Port 1GbE LX Single Mode Fiber NIC .....	74
Four-Port Copper Gigabit-Ethernet PCI-E Card.....	75
Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-E Card .....	76
Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-E Card .....	76
Two-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E Card .....	77
Four-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E Card.....	77
Two-Port FX Multimode Fiber 100 Mbps PCI-E Card .....	78
Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E Card .....	79
Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E Card .....	79
Technical Specifications .....	80
Environmental Specifications .....	82
<b>Appendix C - Series xx20 Status Lights and Ports, Technical Specifications.....</b>	<b>83</b>
1U Series xx20 Rev-A and Rev-B Status Lights and Ports.....	83
Model 520, 1020, 1520, 2020 Rev-A .....	83
Model 520, 1020, 1520, 2020 Rev-B Status Lights and Ports.....	84
3U Series xx20 Status Lights and Ports.....	85
Series xx20 Bypass Cards Status Lights.....	86
Bypass Card Manufacturing Numbers Series xx20.....	87
Two-Port Copper Fast-Ethernet PCI-X Card .....	87

Contents

Two-Port Copper Gigabit-Ethernet PCI-X Card-A.....	88
Two-Port Copper Gigabit-Ethernet PCI-X Card-B.....	89
Four-Port Copper Gigabit-Ethernet PCI-X Card.....	90
Six-Port Copper Gigabit-Ethernet PCI-X Card.....	91
Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card.....	91
Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card.....	92
Technical Specifications .....	93
Environmental Specifications .....	94
<b>Index .....</b>	<b>95</b>

## CHAPTER 1 Overview of the Steelhead Appliance

This chapter provides an overview of common terms, flexible licensing new features, and upgrade instructions.

---

### Overview of the Steelhead Appliance

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. Steelhead appliances 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 appliance, you can solve a range of problems affecting WANs and application performance, including:

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

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

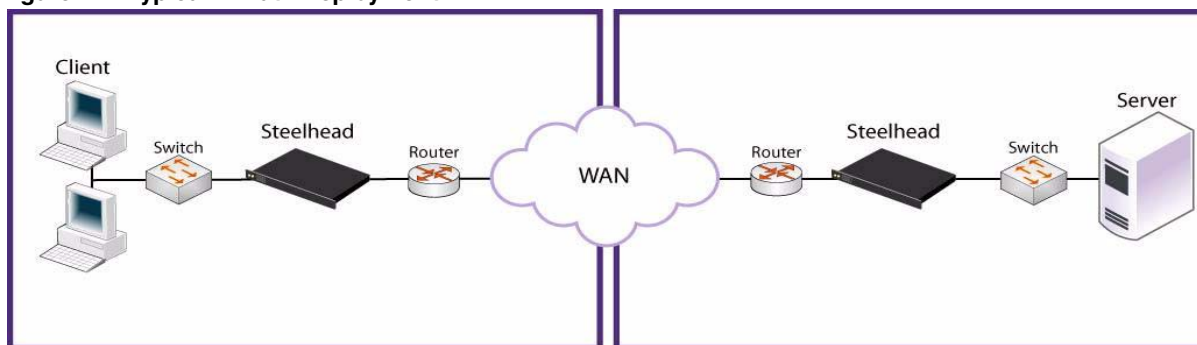
The optimization techniques RiOS utilizes are:

- **Data Streamlining** - Steelhead appliances 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 appliance or Steelhead Mobile host system). Each data chunk is assigned a unique integer label (*reference*) before it is sent to a peer RiOS device across the WAN. When the same byte sequence is seen again in future transmissions from clients or servers, the reference is sent across the WAN instead of the raw data chunk. The peer RiOS device (a Steelhead appliance 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** - Steelhead appliances use a generic latency optimization technique called Transport Streamlining. Transport Streamlining uses a set of standards and proprietary techniques to optimize TCP traffic between Steelhead appliances. 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 can apply application-specific optimizations for certain application protocols: for example, CIFS, MAPI, NFS, TDS, HTTP, Oracle Forms.
- **Management Streamlining** - Management Streamlining refers to the methods that Riverbed has developed to simplify the deployment and management of RiOS devices. These methods include:
  - **Auto-Discovery Process** - Auto-discovery enables Steelhead appliances and Steelhead Mobile to automatically find remote Steelhead appliances, and to then optimize traffic using them. Auto-discovery relieves you from having to manually configure large amounts of network information. The auto-discovery process enables administrators to control and secure connections, specify which traffic is to be optimized, and specify peers for optimization.
  - **Central Management Console (CMC)** - The CMC enables remote Steelhead appliances to be automatically configured and monitored. It also gives you a single view of the overall benefit and health of the Steelhead appliance network.
  - **Steelhead Mobile Controller** - The Mobile Controller is the management appliance you use to track the individual health and performance of each deployed software client, and to manage enterprise client licensing. The Mobile Controller 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.

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

**Figure 1-1. Typical In-Path Deployment**



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



## Auto-Discovery Process

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

Enhanced auto-discovery (RiOS v4.0.x or later) automatically discovers the last Steelhead appliance in the network path of the TCP connection. In contrast, the original auto-discovery protocol automatically discovers the first Steelhead appliance in the path. The difference is only seen in environments where there are three or more Steelhead appliances in the network path for connections to be optimized. Enhanced auto-discovery works with Steelhead appliances running the original auto-discovery protocol.

## Configuring Optimization

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

- **In-Path rules** - In-path rules determine the action a Steelhead appliance 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 appliance. You configure one of the following types of in-path rule actions:
  - **Auto** - Use the auto-discovery process to determine if a remote Steelhead appliance is able to optimize the connection attempting to be created by this SYN packet.
  - **Pass-through** - Allow the SYN packet to pass through the Steelhead appliance. No optimization is performed on the TCP connection initiated by this SYN packet.
  - **Fixed-Target** - Skip the auto-discovery process and use a specified remote Steelhead appliance as an optimization peer. Fixed-target rules require the input of at least one remote target Steelhead appliance; an optional backup Steelhead appliance might also be specified.
  - **Deny** - Drop the SYN packet and send a message back to its source.
  - **Discard** - Drop the SYN packet silently.
- **Peering rules** - Peering rules determine how a Steelhead appliance reacts when it sees a probe query. Peering rules are an ordered list of fields a Steelhead appliance 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 appliance. This is especially useful in complex networks. There are the following types of peering rule actions:
  - **Pass** - The receiving Steelhead appliance does not respond to the probing Steelhead appliance, and allows the SYN+ probe packet to continue through the network.
  - **Accept** - The receiving Steelhead appliance responds to the probing Steelhead appliance and becomes the remote-side Steelhead appliance (that is, the peer Steelhead appliance) for the optimized connection.
  - **Auto** - If the receiving Steelhead appliance is not using enhanced auto-discovery, this has the same effect as the Accept peering rule action. If enhanced auto-discovery is enabled, the Steelhead appliance only becomes the optimization peer if it is the last Steelhead appliance in the path to the server.

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 appliance 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 appliance goes into bypass mode and the traffic passes through uninterrupted.

Certain in-path network interface cards also support a fail-to-block mode. In the case of a failure or loss of power, the Steelhead appliance LAN and WAN interfaces lose link status. The default failure mode is fail-to-wire mode.

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

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

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

When the Steelhead appliance 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, even though without optimization.

In an out-of-path deployment, if the server-side Steelhead appliance fails, the first connection from the client fails. After detecting that the Steelhead appliance is not functioning, a ping channel is setup from the client-side Steelhead appliance to the server-side Steelhead appliance. 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 appliance has an internal software failure or power loss, the Steelhead appliance LAN and WAN interfaces power down and stop bridging traffic.

When fail-to-block is enabled, a failed Steelhead appliance blocks traffic along its path, forcing traffic to be re-routed onto other paths (where the remaining Steelhead appliances 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 appliance blocks it.

---

**Note:** You can use this with connection-forwarding, the **allow-failure** CLI command, and an additional Steelhead appliance 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 appliance CLI. For detailed information, see the *Riverbed Deployment Guide*.

---

## New Features in Version 6.5.4

The following features are available in RiOS Version 6.5.4:

- **Steelhead CX** - RiOS Version 6.5.4 supports Steelhead CX hardware platform. Steelhead CX provides dedicated WAN optimization for those organizations that want to take advantage of WAN optimization for its core function.

- **Automatic Licensing** - RiOS Version 6.5.4 supports Automatic Licensing. After you connect your Steelhead appliance to the network, the Steelhead appliance automatically contacts the Riverbed Licensing Portal to download and install licenses. You can also manually fetch and activate licenses for Riverbed products using the Riverbed Licensing Portal at <https://licensing.riverbed.com/index.htm>. For details, see [Chapter 2, “Managing Riverbed Licenses.”](#)

---

## Upgrading RiOS to Version 6.5.4

RiOS Version 6.5.4 is backward compatible with previous RiOS versions. However, to obtain the full benefits of the new features in RiOS Version 6.5.4, you must upgrade the client-side and server-side Steelhead appliances on any given WAN link. After you have upgraded all appliances, all the benefits of the Version 6.5.4 features and enhancements are available.

---

**Important:** You cannot upgrade Series xx20 hardware to RiOS Version 6.5.4.

---

If you mix RiOS software versions in your network, the releases might support different optimization features and you cannot take full advantage of the features that are not part of the older software versions.

The following table summarizes the steps for upgrading from 32-bit systems to 64-bit systems.

Current RiOS Software Version (32-bit code)	1.Upgrade to RiOS: (32-bit code)	2.Upgrade to RiOS: (64-bit code)
v4.1.x	v4.1.7c	v6.00
v5.0.x	v5.0.5b	v6.00
v4.1.7c or later	No stepping stone build required.	v7.01
v5.0.5b or later	No stepping stone build required.	v7.01
v6.0 or later	No stepping stone build required.	v7.01

## Upgrading RiOS Software

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

---

**Important:** RiOS v7.0 is not supported on the Series xx20 platforms.

---

### To upgrade RiOS software

1. Download the software image from the Riverbed Support to a location such as your desktop.
2. Log in to the Management Console using the Administrator account (admin).

3. Go to the Configure > Maintenance > Software Upgrade page and choose one of the following options:
  - **From URL** - Type the URL that points to the software image in the text box.
  - **From Local File** - Browse your file system and select the software image.
  - **Schedule Upgrade for Later** - Select this option to schedule an upgrade for a later time. Type the date and time in the Date and Time text boxes using the following formats YYYY/MM/DD and HH:MM:SS.
  - Click **Install**.
4. Reboot the appliance.

The software image is quite large; uploading the image can take a few minutes. This is normal behavior as the software is configuring the recovery flash device. Do not press Ctrl-C, unplug, or otherwise shut down the system during this first boot. There is no indication displayed during the system boot that the recovery flash device is being configured.

After the upload is complete, you are reminded to reboot the system to switch to the new version of the software. After reboot, the software version is displayed on the Home page of the Management Console.

## Downgrading the Software

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

---

**Note:** When downgrading from an image that supports four 10 GigE cards to an older image that does not, 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.

---



# Preface

Welcome to the *Steelhead Appliance Installation and Configuration Guide* (Series xx20, xx50, CX xx55). Read this preface for an overview of the information provided in this guide and for an understanding of the documentation conventions used throughout.

---

## About This Guide

The *Steelhead Appliance Installation and Configuration Guide* describes how to install and configure the Steelhead appliance.

## Audience

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

## Document Conventions

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

Convention	Meaning
<i>italics</i>	Within text, new terms and emphasized words appear in italic typeface.
<b>boldface</b>	Within text, CLI commands and GUI controls appear in bold typeface.
Courier	Code examples appear in Courier font: <pre>amnesiac &gt; enable amnesiac # configure terminal</pre>
< >	Values that you specify appear in angle brackets: <b>interface &lt;ipaddress&gt;</b>
[ ]	Optional keywords or variables appear in brackets: <b>ntp peer &lt;addr&gt; [version &lt;number&gt;]</b>
{ }	Required keywords or variables appear in braces: <b>{delete &lt;filename&gt;   upload &lt;filename&gt;}</b>
	The pipe symbol represents a choice between the keyword or variable to the left or right of the symbol (the keyword or variable can be either optional or required): <b>{delete &lt;filename&gt;   upload &lt;filename&gt;}</b>

## Product Dependencies and Compatibility

This section provides information about product dependencies and compatibility. It includes the following information:

- [“Hardware and Software Dependencies” on page 9](#)
- [“CMC Compatibility” on page 9](#)
- [“RSP Services 32-Bit and 64-Bit Support” on page 10](#)
- [“Ethernet Network Compatibility” on page 10](#)
- [“SNMP-Based Management Compatibility” on page 11](#)
- [“Antivirus Compatibility” on page 11](#)



## Hardware and Software Dependencies

The following table summarizes the hardware and software requirements for the Steelhead appliance.

Riverbed Component	Hardware and Software Requirements
Steelhead Appliance	19-inch (483 mm) two or four-post rack.
Steelhead Management Console	<p>Any computer that supports a Web browser with a color image display.</p> <p>The Management Console has been tested with Mozilla Firefox version v3.0.x or later, and Microsoft Internet Explorer version v6.x and v7.x or later</p> <p><b>Note:</b> JavaScript and cookies must be enabled in your Web browser.</p>

## CMC Compatibility

The Steelhead appliance has been tested with the following Central Management Console (CMC) versions:

Steelhead RiOS Version	Recommended CMC Version	CMC 6.5.x	CMC v6.1.x	CMC v6.0.x	CMC v5.5.x
v7.0.1	v6.5.3	v6.5.3 parity	Manages only v6.1.x features, does not support QoS.	Not supported.	Not supported.
v6.5.x	v6.5.x	v6.1.x partial support	Manages only v6.1.x features, does not support QoS.	Not supported.	Not supported.
v6.1.x	v6.1.0	v6.1.0	Parity; Includes Virtual Steelhead, does not support ProCurve.	Manages some RiOS v6.1.x features might be supported in subsequent point releases of CMC v6.0.	Not supported.
v6.0.x	v6.1.0, 6.0.1	v6.1.0, 6.0.1	Parity; Manages all Steelhead appliance v6.0.2 and later features.	Parity; Manages all Steelhead appliance v6.0.x features.	CMC v5.5.3 and later, manages only v5.5 Steelhead appliance features.
v5.5.x	v6.1.0, 6.0.1	v6.1.0, 6.0.1	Parity; Manages all Steelhead appliance v5.5.4 only.	Parity; Manages all Steelhead appliance v5.5.4 features only.	Parity.

## RSP Services 32-Bit and 64-Bit Support

The following table describes the models that support 32-bit and 64-bit Virtual Machines (VMs). The 64-bit guest VMs (such as Windows Server 2008 R2) are not supported on Models 250, 550, and the 1U xx20s because these models do not incorporate Virtual Technology (VT) support.

Steelhead Model	RiOS	RSP Image	32-bit Guest VMs	64-bit Guest VMs
250/550	32-bit	32-bit	Yes	No
520/1020/1520/2020	64-bit	64-bit	Yes	No
1050/2050	64-bit	64-bit	Yes	Yes (starting v5.5.3a)
3020/3520	64-bit	64-bit	Yes	Yes (starting v5.5.1)
5050/6050/7050	64-bit	64-bit	Yes	Yes
CX555/CX755/CX1555	64-bit	64-bit	Yes	Yes

## Firewall Requirements

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

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

## Ethernet Network Compatibility

The Steelhead appliance supports the following Ethernet networking standards:

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

The Steelhead appliance ports support the following connection types and speeds:

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

1000 Base-SX and 1000 Base-LX interface options are not available for the Steelhead appliance 250 and 550 models.

The Steelhead appliance supports VLAN Tagging (IEEE 802.3 - 2008). It does not support the ISL protocol. All copper interfaces are auto-sensing for speed and duplex (IEEE 802.3 - 2008).

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

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

## SNMP-Based Management Compatibility

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

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

## Antivirus Compatibility

The Steelhead appliance has been tested on clients and file servers generating CIFS traffic with the following antivirus software with no impact on performance:

- Network Associates (McAfee) VirusScan v7.0.0 Enterprise on the server
- Network Associates (McAfee) VirusScan v7.1.0 Enterprise on the server
- Network Associates (McAfee) VirusScan v7.1.0 Enterprise on the client
- Symantec (Norton) AntiVirus Corporate Edition v8.1 on the server

The Steelhead appliance has been tested on clients and file servers generating CIFS traffic with the following antivirus software with moderate impact on performance:

- F-Secure Anti-Virus v5.43 on the client
- F-Secure Anti-Virus v5.5 on the server
- Network Associates (McAfee) NetShield v4.5 on the server
- Network Associates VirusScan v4.5 for multiple platforms on the client
- Symantec (Norton) AntiVirus Corporate Edition v8.1 on the client

---

## Additional Resources

This section describes resources that supplement the information in this guide. It contains the following sections:

- [“Release Notes” on page 12](#)
- [“Riverbed Documentation and the Support Knowledge Base” on page 12](#)

## Release Notes

The following online file supplements the information in this manual. It is available on the Riverbed Support site at <https://support.riverbed.com>.

Online File	Purpose
<product>_<version_number><build_number>.pdf	Describes the product release and identifies fixed problems, known problems, and workarounds. This file also provides documentation information not covered in the manuals or that has been modified since publication.

Examine this file before you begin the installation and configuration process. It contains important information about this release of the Steelhead appliance.

## Riverbed Documentation and the Support Knowledge Base

For a complete list and the most current version of Riverbed documentation, log in to the Riverbed Support site at <https://support.riverbed.com>.

The Riverbed Knowledge Base is a database of 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>.

## Safety Guidelines

Follow the safety precautions outlined in the *Safety and Compliance Guide* when installing and setting up your equipment.

**Important:** Failure to follow these safety guidelines can result in injury or damage to the equipment. Mishandling of the equipment voids all warranties. Read and follow safety guidelines and installation instructions carefully.

Many countries require the safety information to be presented in their national languages. If this requirement applies to your country, consult the *Safety and Compliance Guide*. Before you install, operate, or service the Riverbed products, you must be familiar with the safety information. Refer to the *Safety and Compliance Guide* if you do not clearly understand the safety information provided in this guide.

## Contacting Riverbed

This section describes how to contact departments within Riverbed.

## Internet

You can learn about Riverbed products through our Web site at <http://www.riverbed.com>.

## 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](mailto:proserve@riverbed.com) or go to <http://www.riverbed.com>.

## Documentation

We continually strive to improve the quality and usability of our documentation. We appreciate any suggestions you may have about our online documentation or printed materials. Send documentation comments to [techpubs@riverbed.com](mailto:techpubs@riverbed.com).



## CHAPTER 2 Managing Riverbed Licenses

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

- [“Riverbed Licensing Methods” on page 15](#)
- [“Automatic Licensing” on page 16](#)
- [“Retrieving Licenses Using the Riverbed Licensing Portal” on page 20](#)

---

### Riverbed Licensing Methods

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

- **Automatic Licensing** - After you connect your Steelhead appliance to the network, the Steelhead appliance automatically contacts the Riverbed Licensing Portal to download and install licenses. For detailed information, see [“Connecting to the Steelhead Appliance” on page 30](#).
- **Manual Licensing** - You can manually fetch and activate licenses for Riverbed products using the Riverbed Licensing Portal. Simply go to <https://licensing.riverbed.com/index.htm> and follow the instructions to retrieve license keys.
- **Factory Licensing** - You can have all your Riverbed licenses installed at the factory for a small fee.
- **Token Method** - You use tokens to activate Riverbed software, such as the Virtual Steelhead Mobile, Virtual Whitewater, Virtual Steelhead, and HP ProCurve. For detailed information, see the respective installation guides for these products.

---

## Automatic Licensing

Automatic licensing allows the Steelhead appliance, 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 an XML file to the Steelhead Central Management Console. For detailed information, see [“Retrieving Licenses Using the Riverbed Licensing Portal” on page 20](#).

---

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

---

## Flexible Licensing

RiOS provides a flexible way to manage Steelhead appliance upgrades. Rather than performing an incremental model upgrade or replacing an appliance, RiOS provides *specification licenses* that configure specific performance characteristics of an appliance. A specification license points to a specific, validated model and includes the required license and the hardware specification. If a model upgrade requires additional hardware, the specification license determines which hardware is necessary to complete the upgrade.

By activating a specification license on an appliance you can transform the capabilities of the appliance to meet performance characteristics for any model within a platform family.

Some model upgrades require new hardware components: for example, to upgrade a model 1050L to a 1050H, you must install an additional 250 GB of disk space and an additional 2 GB of memory. To accomplish this, order a hardware kit that contains the additional hardware from Riverbed Support or Sales.

After adding the required hardware and license to the Steelhead appliance, activate the hardware specification instead of replacing the appliance in the Licenses page of the Management Console.



## Flexible Licensing and Upgrade Possibilities by Appliance Model

The following table summarizes the upgrade options for the Steelhead appliance by model.

Source Appliance Model	Destination Appliance Model	Upgrade Requires	Minimum RiOS Version	Impact on RiOS data store	Impact on Appliance Configuration	Reboot Required
250L	250M	License only	v4.1.9d v5.0.7e v5.5.2d	None	None	No
250L	250H	License only	v4.1.9d v5.0.7e v5.5.2d	None	None	No
250M	250H	License only	v4.1.9d v5.0.7e v5.5.2d	None	None	No
550M	550H	License only	v4.1.9d v5.0.7e v5.5.2d	None	None	No
CX555M	CX555H	License only	v6.5.4	None	None	No
CX755L	CX755M	License only	v6.5.4	None	None	No
1050U	1050L	License only	v5.5.9 v6.0.4 v6.1.2	None	None	No
1050L	1050LR	License and Hardware Kit	v5.0.9 v5.5.4	Clears: <ul style="list-style-type: none"> <li>• RiOS data store</li> <li>• log files</li> </ul>	None	Yes
1050L	1050M	License only	v4.1.9d v5.0.7e v5.5.2d	None	None	No
1050L	1050H	1050H License and Hardware Kit	v4.1.9d v5.0.7e v5.5.2d	Clears all data	None	Yes
1050M	1050H	1050H License and Hardware Kit	v4.1.9d v5.0.7e v5.5.2d	Clears all data	None	Yes
1050M	1050MR	License and Hardware Kit	v5.0.9 v5.5.4	Clears: <ul style="list-style-type: none"> <li>• RiOS data store</li> <li>• log files</li> </ul>	None	Yes

Source Appliance Model	Destination Appliance Model	Upgrade Requires	Minimum RiOS Version	Impact on RiOS data store	Impact on Appliance Configuration	Reboot Required
1050H	1050HR	License and Hardware Kit	v5.0.9 v5.5.4	Clears: • RiOS data store • log files	None	Yes
1050LR	1050MR	License only	v5.0.9 v5.5.4	None	None	No
1050LR	1050HR	License and Hardware Kit	v5.0.9 v5.5.4	Clears: • RiOS data store	None	No
1050MR	1050HR	License and Hardware Kit	v5.0.9 v5.5.4	Clears: • RiOS data store	None	No
CX1555L	CX1555M	License only	v6.5.4	None	None	No
2050M	2050H	License only	v4.1.9d v5.0.7e v5.5.2d	None	None	No
5050L	5050M	License only	v5.5.7 v6.0.2	None	None	No
5050L	5050H	License and Hardware Kit	v5.5.7 v6.0.2	Clears: • RiOS data store • log files	None	Yes
5050M	5050H	5050H License and Hardware Kit	v4.1.9d v5.0.7e v5.5.2d	Clears all data in the RiOS data store, and also clears: • all statistics • all log files	None	Yes

For details on hardware specifications that require hardware upgrades, see the *Upgrade and Maintenance Guide*.

## Installing Licenses

This section describes how to request and fetch a license manually from the Riverbed Licensing Portal or install a license manually after receiving it from Riverbed Support or Sales.

### To view licenses on a new Steelhead appliance

- Connect the new Steelhead appliance to the network.

The Steelhead appliance 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 appliance 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.

**To fetch a license on demand**

1. In the Management Console choose Configure > 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*.

---

## Retrieving Licenses Using the Riverbed Licensing Portal

You can retrieve and manage Riverbed licenses using the Riverbed Licensing Portal. The Riverbed Licensing Portal simplifies license management by providing an automated way to fetch and activate licenses for Riverbed products.

### To retrieve your licenses using the Riverbed Licensing Portal

1. Copy the barcoded Serial Number (SN) and Manufacturing Serial Number (MFG) that is located on the front, back, or side of your appliance.
2. Go to the License Activation page in the Riverbed Licensing Portal at <https://licensing.riverbed.com/index.htm>

Figure 2-1. Riverbed Licensing Portal

The screenshot shows the Riverbed Licensing Portal interface. At the top, there is a navigation bar with the Riverbed logo, the word "support", and a search bar. Below the navigation bar, there are several menu items: Home, Account, Cases, Documentation, Downloads, Forum, Knowledge Base, and Contact Us. The main content area is titled "GENERATE OR RETRIEVE LICENSES FOR YOUR RIVERBED PRODUCTS". There are three main sections: "BY ACTIVATION CODE:", "BY SERIAL NUMBER:", and "FOR STINGRAY OPTIMIZER:". Each section contains a form with input fields and a "Submit" button. The "BY SERIAL NUMBER:" section also includes a "REDEEM LICENSES FOR OTHER RIVERBED PRODUCTS:" section with a list of links: [Stingray Traffic Manager](#), [Stingray Application Firewall Manager](#), and [Stingray Optimizer](#).

3. To retrieve your licenses by serial number, type your name, email address, phone number, Serial Number (SN), and Manufacturing (hardware) Serial Number (MFG) and click **Submit** to display the Software License Summary page. The SN and MFG numbers are barcoded labels located on the front, back, or side of your appliance.

- For each serial number, click the check box for the software feature you want to activate and click **Refresh**. Make sure your serial numbers match the software features. You cannot make changes after you have activated selected licenses.

Figure 2-2.

The screenshot shows the Riverbed Support portal interface. At the top, there is a navigation bar with links for Home, Account, Cases, Documentation, Downloads, Forum, Knowledge Base, and Contact Us. The main content area displays a success message: "Your license key(s) has been created". Below this, it states that a serial number F84MY000995AF was entered and lists the software features purchased. A table shows the status of licenses, including LIC-EXA-1160-L (Base) and LIC-GRANITE-1160 (Addon). A section titled "SELECT SOFTWARE FEATURE:" provides instructions on how to activate licenses. A table lists the license keys for the entered serial number, including the activated license key and the activation date. At the bottom, there are buttons for "Refresh" and "New Search", and a section for downloading XML files or emailing keys, with a text box for the email address and an "Email Keys" button.

Welcome, Customer, [Log Out](#)

Search > ?

Home Account Cases Documentation Downloads Forum Knowledge Base Contact Us

## Your license key(s) has been created

You have entered serial number **F84MY000995AF**.

The following software features have been purchased on the same order as the serial number you have entered.

PO Number:	PO-00411
Sales Order:	135911

**Status of Licenses**

License/Software	License Type	Total	Activated	Remaining	Not Activated
LIC-EXA-1160-L	Base	1	1	0	0
LIC-GRANITE-1160	Addon	1	1	0	0

**SELECT SOFTWARE FEATURE:**

For each serial number, select the software feature you want to activate the license key for. You cannot make changes after you have activated selected licenses.

Total number of records found: 1  
Model Number: EXA-01160-B030

<input checked="" type="checkbox"/>	Serial No.	Software	Activated License Key	Activation Date
<input checked="" type="checkbox"/>	F84MY000995AF	LIC-EXA-1160-L	LK1-MSPECL-0000-0000-1-7497-B445-F589	12-20-2011 12:08:20 PM
		LIC-GRANITE-1160	LK1-GRANITE-3BFE-3C58-5-D16D-B119-2199	12-20-2011 12:08:20 PM

Request SSL on the Riverbed Support Site, on the [Account > SSL License Key Registration](#) page.

Download or email an XML file of your license keys, which can be imported by the Steelhead Central Management Console (CMC) to activate the licenses manage by the CMC:

or Email address(es) :

- Optionally, you 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.
- Optionally, if you are behind a firewall, click **Download XML** to download an XML file. The XML file can be imported by the Steelhead Central Management Console.

---

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

---

## Installing Your License Keys

Each license key is generated for a specific appliance, make sure to install your license key on the appropriate appliance.

### To install a license using the CLI

1. Connect to the CLI of the appliance and enter configuration mode. For details see the *Riverbed Command-Line Interface Reference Manual*.
2. At the system prompt, enter the following commands:

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

### To install a license using the Management Console

1. Connect to the Management Console of the appliance. For details, see the *Steelhead Management Console User's Guide*.
2. Choose Configure > Maintenance > Licenses to display the Licenses Page.
3. In the Licenses Text Box, 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 Appliance

This chapter describes how to install and configure the Steelhead appliance.

---

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

---

---

### Choosing a Network Deployment

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

---

**Note:** If there are one or more firewalls between two Steelhead appliances, ports 7800 and 7810 must be passed through firewall devices located between the pair of Steelhead appliances. 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 Steelhead appliances and their respective clients and servers. Steelhead appliances should be as close as possible to your network end points (client-side Steelhead appliances should be as close to your clients as possible and server-side Steelhead appliances should be as close to your servers as possible).

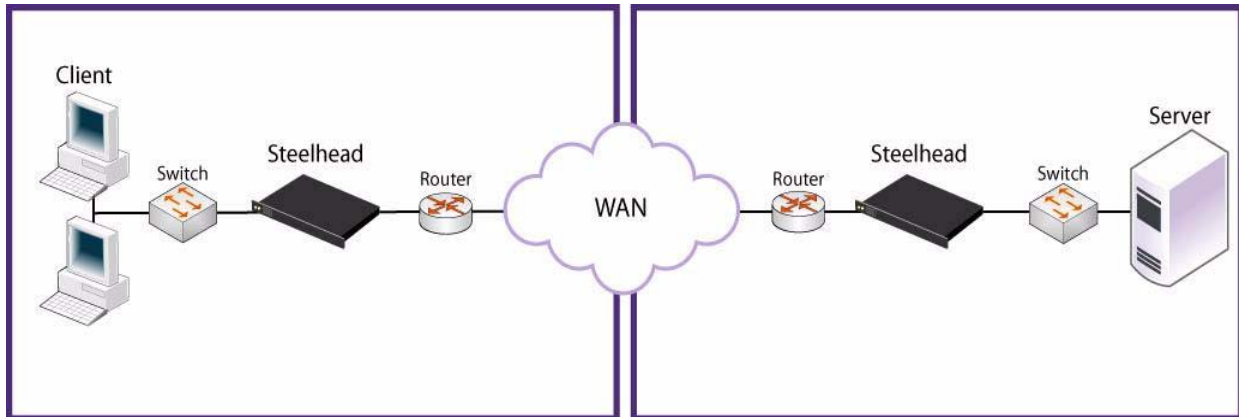
Ideally, Steelhead appliances optimize only traffic that is initiated or terminated at their local site. The best and easiest way to achieve this is to deploy the Steelhead appliances where the LAN connects to the WAN, and not where any LAN-to-LAN or WAN-to-WAN traffic can pass through (or be redirected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

For detailed information about your deployment options and best practices for deploying Steelhead appliances, see the *Riverbed Deployment Guide*.

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

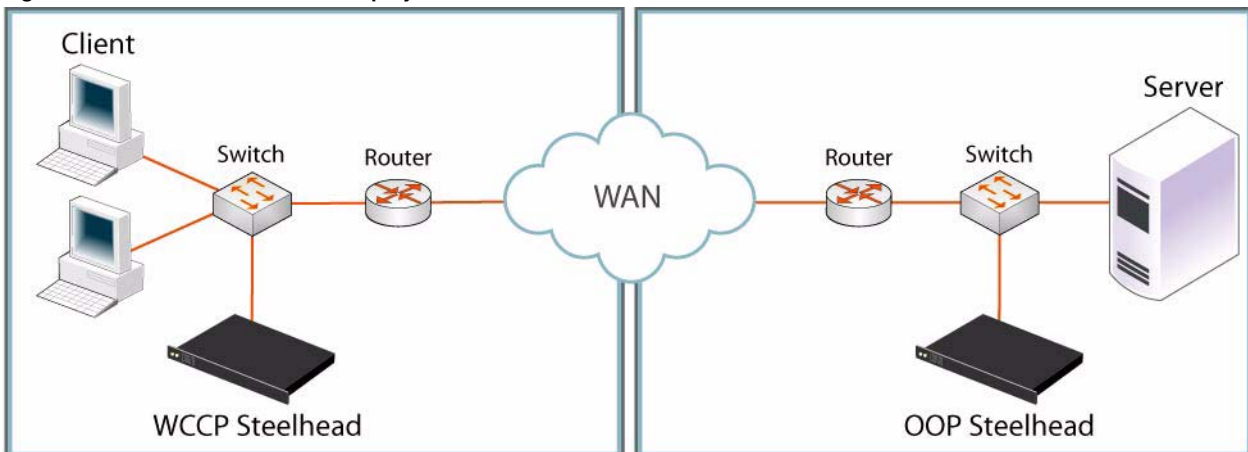
- Physical In-Path** - In a physical in-path deployment, the Steelhead appliance is *physically* in the direct path between clients and servers. The clients and servers continue to see client and server Internet Protocol (IP) addresses. In-path designs are the simplest to configure and manage, and the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

Figure 3-1. Physical In-Path Deployment



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

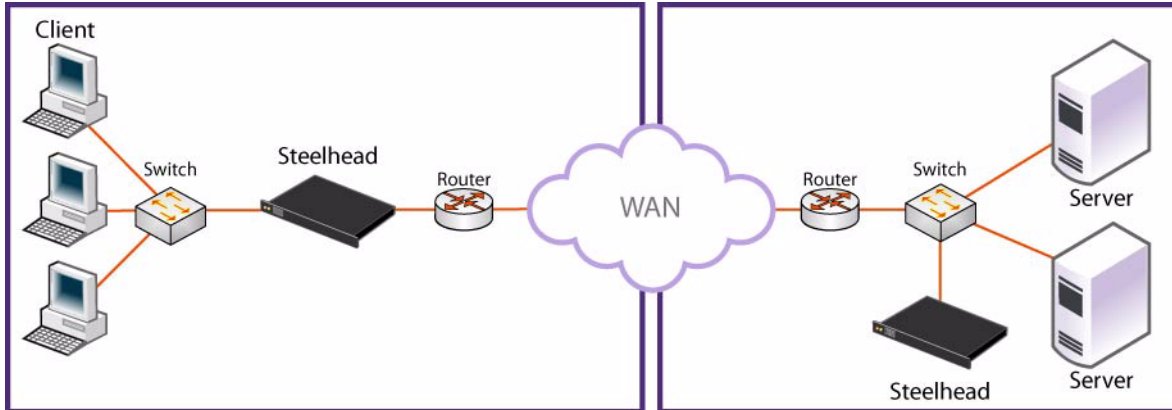
Figure 3-2. Virtual In-Path: WCCP Deployment





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

**Figure 3-3. Out-of-Path Deployment**



## Checking Your Inventory

Your shipping carton contains the following items:

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

Aside from country-specific requirements, all systems ship with the same power cable. The power cable has a IEC 60320 C13 plug on one end (to connect to the Steelhead appliance) 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 appliance using either the cable in the accessories box or another cable that is approved for use by the IEC in the country in which the appliance is connected.

You cannot connect a Steelhead appliance 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 Series xx50 and xx60 platforms.
- One mounting kit
- Documentation kit

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

---

## Preparing Your Site for Installation

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

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

- It is a standard electronic environment where the ambient temperature does not exceed 40° C (104° F) and the relative humidity does not exceed 80% (noncondensing). For detailed information, see the appendices that follow.
- Ethernet connections are available within the standard Ethernet limit.
- There is available space on a two- or four-post 19-inch rack. For details about installing the Steelhead appliance 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.

---

---

## Completing the Configuration Checklist

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

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

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

**Note:** The Steelhead appliance 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.

## Steelhead Appliance Ports

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

Port	Description
Console	Connects the serial cable to a terminal device. You establish a serial connection to a terminal emulation program for console access to the configuration wizard and the Steelhead CLI.
Primary (PRI)	<p>The management interface that connects the Steelhead appliance to a LAN switch. This management interface enables you to connect to the Management Console and the Steelhead CLI.</p> <p><b>Tip:</b> The primary and auxiliary ports cannot share the same network subnet.</p> <p><b>Tip:</b> The primary and in-path interfaces can share the same subnet.</p> <p><b>Tip:</b> You must use the primary port on the server-side for out-of-path deployments.</p>
Auxiliary (AUX)	<p>An optional port that provides an additional management interface for a secondary network. You cannot have the primary and auxiliary ports on the same subnet.</p> <p><b>Tip:</b> The auxiliary and in-path interfaces cannot share the same network subnet.</p> <p><b>Tip:</b> You cannot use the auxiliary port for out-of-path Steelhead appliances.</p>
WAN	Connects the WAN port of the Steelhead appliance and the WAN router using a crossover cable.
LAN	<p>Connects the LAN port of the Steelhead appliance and the LAN switch using a straight-through cable.</p> <p><b>Note:</b> If the Steelhead appliance is deployed between two switches, both the LAN and WAN ports must be connected with straight-through cables.</p>

## 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*.

---

## Powering On the Steelhead Appliance

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

---

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

---

### To power on the system

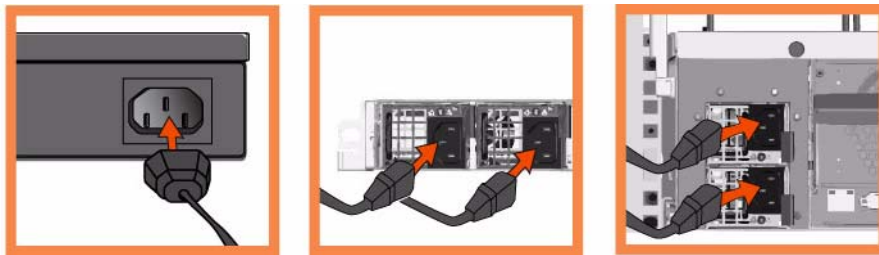
1. If your system has a master power switch, ensure that the system and master power switch is in the off position on the rear of the Steelhead appliance.
2. Plug the AC power cord into the Steelhead appliance.

---

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

---

**Figure 3-4. Connecting the AC Power**



3. Plug the AC power cord into an uninterrupted AC power source.
4. Press the system power switch on. If the Steelhead appliance does not immediately power on, press the power switch off, then press the power switch on again.
5. Check the status lights on the Steelhead appliance. For detailed information about the status lights, see the appendices that follow.

---

**Note:** The Steelhead CX appliance (Series xx55) takes approximately 10 minutes to boot.

---

---

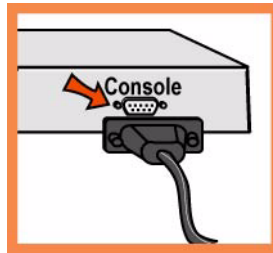
## Connecting to the Steelhead Appliance

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

### To connect to the Steelhead appliance

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

**Figure 3-5. Connecting to the Steelhead Appliance**



2. Start your terminal emulation program, such as Tera Term Pro. The terminal device must have the following settings:
  - Baud rate: 9600 bps
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - vt100 emulation
  - No flow control

---

**Note:** If you are using the Steelhead appliance with a terminal server, the terminal server must use hardware flow control for the port connected to the Steelhead appliance.

---

---

**Tip:** 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 appliance using the configuration wizard:

- For in-path configurations, see [“Configuring In-Path Steelhead Appliances” on page 31](#).
- For out-of-path configurations, see [“Configuring Out-of-Path Steelhead Appliances” on page 40](#).

---

## Configuring In-Path Steelhead Appliances

In a physical in-path deployment, the Steelhead appliance 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 appliance. For a detailed figure, see [“Choosing a Network Deployment” on page 23](#).

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

### Avoiding Duplex Mismatch

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

The Steelhead appliance 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 appliance WAN interface.
- Steelhead appliance LAN interface.
- Steelhead appliance primary interface.

The following can be signs of a duplex mismatch:

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

For detailed information about checking for duplex mismatches, see [Chapter 4, “Troubleshooting.”](#)

### Configuration Wizard

The configuration wizard automatically starts when you log in to the CLI for the first time.

The following rules apply to the configuration wizard:

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

If you quit the configuration wizard, you can restart it from the Steelhead CLI. You must be in configuration mode to restart the configuration wizard.

## To restart the configuration wizard

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

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

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

## To configure the Steelhead appliance in an in-path deployment

1. If you have a Steelhead Central Management Console (CMC) appliance installed in your network to manage multiple Steelhead appliances, you can use it to automatically configure them:

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

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

---

**Tip:** 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 32](#).

---

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

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

3. Complete the configuration wizard steps on the client-side and the server-side Steelhead appliances as described in the following table.

Wizard Prompt	Description	Example
Step 1: Host name?	Enter the host name for the Steelhead appliance.	hostname? amnesiac
Step 2: Use DHCP on the primary interface?	You are given the option to enable the DHCP to automatically assign an IP address to the primary interface for the Steelhead appliance.  Riverbed recommends that you do not set DHCP.  The default value is no.	Use DHCP? no
Step 3: Primary IP address?	Enter the IP address for the Steelhead appliance.	Primary IP address? 10.10.10.6
Step 4: Netmask?	Enter the netmask address.	Netmask? 255.255.0.0
Step 5: Default gateway?	Enter the default gateway for the Steelhead appliance.	Default gateway? 10.0.0.1
Step 6: Primary DNS server?	Enter the primary DNS server IP address.	Primary DNS server? 10.0.0.2



Wizard Prompt	Description	Example
Step 7: Domain name?	Enter the domain name for the network where the Steelhead appliance is to reside.  If you set a domain name, you can enter host names in the system without the domain name.	Domain name? example.com
Step 8: Admin password?	Riverbed strongly recommends that you change the default administrator password at this time. The password must be a minimum of six characters.  The default administrator password is password.	Admin password? xxxyyy
Step 9: SMTP server?	Enter the name of the SMTP server. External DNS and external access for SMTP traffic is required for email notification of events and failures to function.  <b>Important:</b> Make sure that you provide a valid SMTP server to ensure that the email notifications for events and failures.	SMTP server? natoma
Step 10: Notification email address?	Enter a valid email address to which notification of events and failures are to be sent.	Notification email address? example@example.com
Step 11: Set the primary interface speed?	Enter the speed on the primary interface (that is, the Steelhead appliance). Make sure that this value matches the settings on your router or switch.  The default value is auto.	Set the primary interface speed? [auto] auto
Step 12: Set the primary interface duplex?	Enter the duplex mode on the primary interface. Make sure that this value matches the settings on your router or switch. The default value is auto.	Set the primary interface duplex? [auto] auto
Step 13: Would you like to activate the in-path configuration?	Enter <i>yes</i> at the system prompt to configure in-path support. An in-path configuration is a configuration in which the Steelhead appliance is in the direct path of the client and server.  For detailed information about in-path configurations, see the <i>Riverbed Deployment Guide</i> .	Would you like to activate the in-path configuration? yes
Step 14: In-Path IP address?	Enter the in-path IP address for the Steelhead appliance.	In-Path IP address? 10.11.11.6
Step 15: In-Path Netmask?	Enter the in-path netmask address.	In-Path Netmask? 255.255.0.0
Step 16: In-Path Default gateway?	Enter the in-path default gateway (the WAN gateway).	In-Path Default Gateway? 10.11.11.16

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

#### 4. The system confirms your settings.

```

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

```

The Steelhead appliance configuration wizard automatically saves your configuration settings.

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

```
amnesiac> exit
```

## Connecting the Steelhead Appliance to Your Network

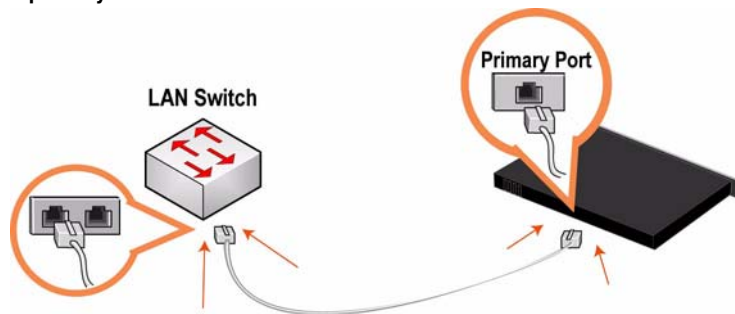
You use standard Ethernet straight-through and crossover cables to connect to your network in an in-path configuration. Make sure that you use the correct cables to establish your network connections:

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

### To connect to your network

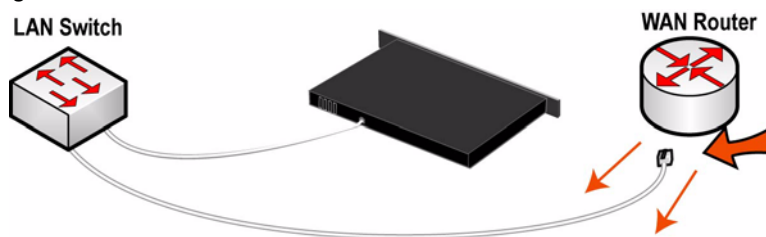
1. Plug the straight-through cable into the primary port of the Steelhead appliance and the LAN switch. This can be any port on your LAN switch configured to connect to a host.

**Figure 3-6. Connecting the primary Port to the LAN Switch**



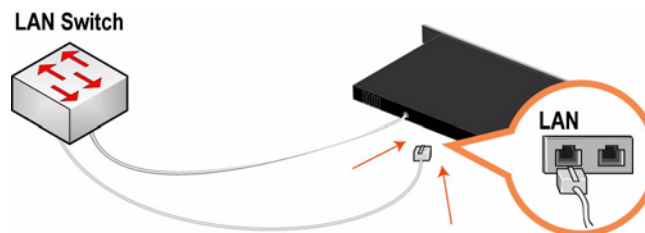
2. Identify the straight-through cable that connects your LAN switch to your WAN router. Unplug the end connected to the WAN router.

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



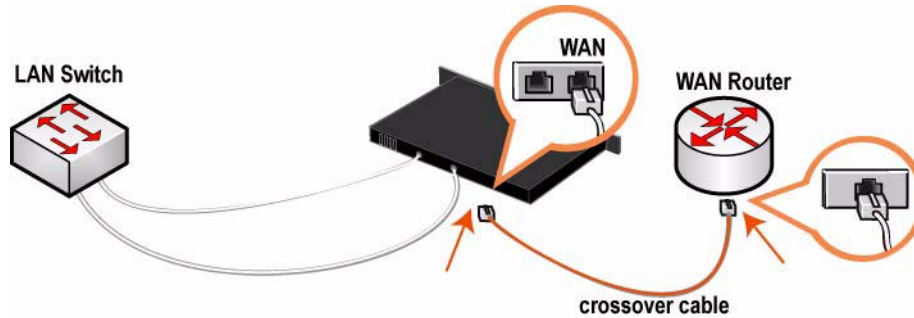
3. Plug the straight-through cable that you disconnected from the WAN router into the LAN port of the Steelhead appliance.

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



- Using the provided crossover cable, plug the cable into the WAN port of the Steelhead appliance and the WAN router. This must be a crossover cable.

**Figure 3-9. Connecting the WAN Port to the WAN Router**




---

**Note:** If you have a four- 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*.

---

You can now optimize WAN traffic using the Steelhead appliance.

## Verifying Your Connections

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

### To verify your connections

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

- At the system prompt, enter the following command:

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

or

```
ssh admin@ipaddress
```

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

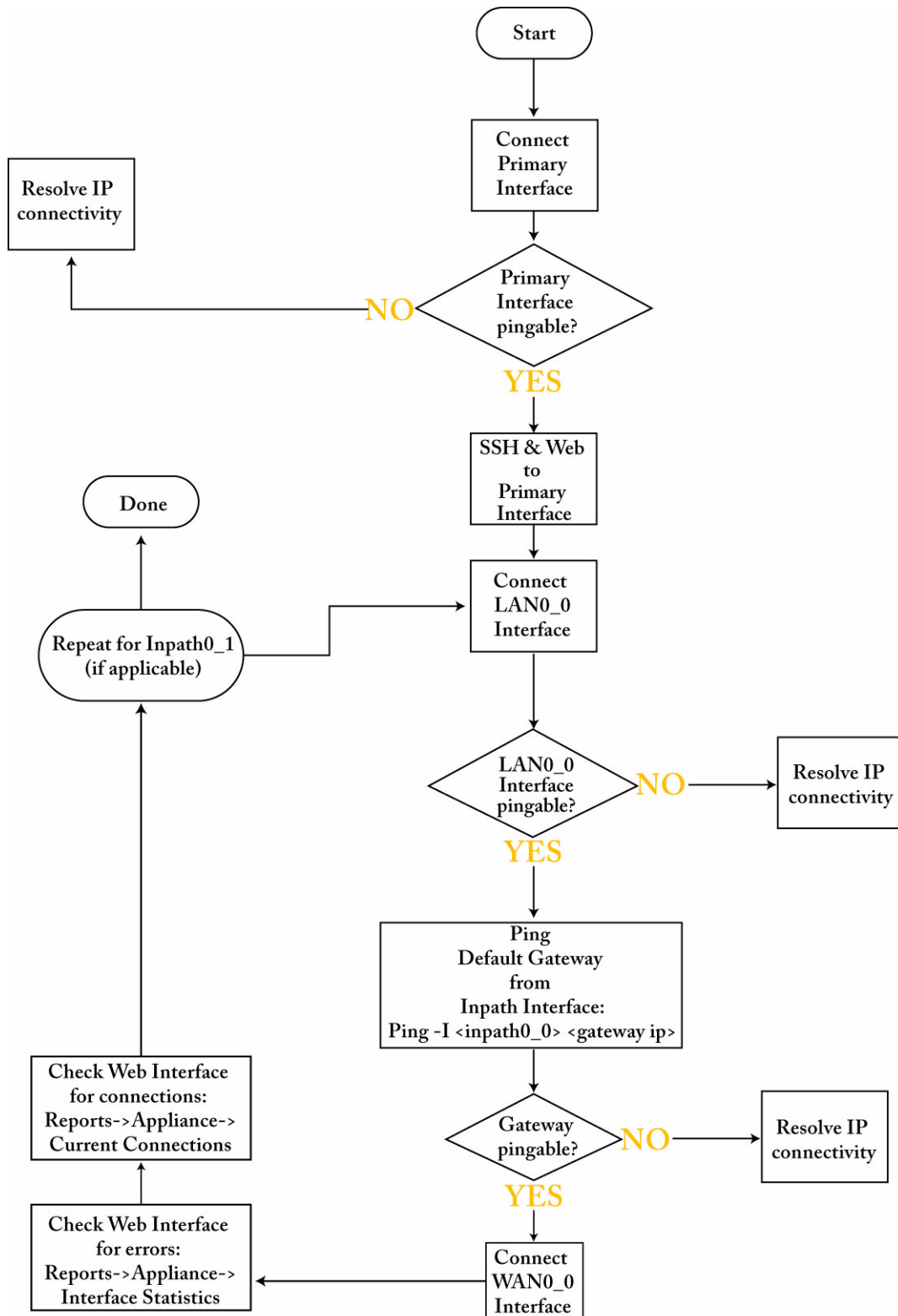
- At the system prompt, ping from the management interface:

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

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

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

Figure 3-10. Resolving IP Connectivity



## Connecting to the Management Console

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

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

---

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

---

### To connect to the Management Console

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

*protocol://host.domain*

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


---

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

---

The Management Console appears, displaying the Login page.

**Figure 3-11. Login Page**



Management Console for gen-sh221

Riverbed Steelhead

Username:

Password:

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

Users with administrator (`admin`) privileges can configure and administer the Steelhead appliance. Users with monitor (`monitor`) privileges can view the Steelhead appliance reports, user logs, and change their own password. A monitor user cannot make configuration changes.

3. In the Password text box, type the password you assigned in the configuration wizard of the Steelhead appliance. (The Steelhead appliance is shipped with the default password: `password`.)
4. Click **Log In** to display the Home page.

The Home page summarizes the current status of your system.

## Verifying Your Configuration

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

If you selected auto-negotiation (`auto`) for your in-path and primary interfaces, you must ensure that the Steelhead appliance 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 `Configure > Networking > Inpath0_0` page and the `Configure > Networking > Base Interfaces` page of the Management Console.

### To check for speed and duplex errors

1. In the Management Console, go to the `Reports > Diagnostics > System Logs` page.
2. Check the system logs for duplex or speed errors.
3. Go to the `Reports > Networking > Current Connections` page.
4. Check for duplex and speed errors.
5. If you find errors, change the speed and duplex settings on your LAN and WAN interface in the `Configure > Networking > Inpath 0_0` page.

### To verify optimization in an in-path configuration

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.

---

## Configuring Out-of-Path Steelhead Appliances

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

An out-of-path configuration is suitable for data center locations where physical in-path or logical in-path configurations are not possible. For a detailed figure, see [“Choosing a Network Deployment” on page 23](#).

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

### Before You Begin

Before you begin the configuration process, check the duplex and speed settings on the router and switch that connects to your Steelhead appliance. Make sure that the settings on the router, switch, and the Steelhead appliance match. For example, ensure that settings are auto speed and duplex on the LAN and WAN or 100 FULL on the LAN and WAN. If the settings do not match, optimization might be degraded.

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 restart it, see [“Configuration Wizard” on page 31](#).

---

**Important:** In an out-of-path configuration, the client-side Steelhead appliance is configured as an in-path device and the server-side Steelhead appliance is configured as an out-of-path device.

---

### To configure the server-side Steelhead appliance in an out-of-path deployment

1. If you have a Central Management Console appliance installed in your network to manage multiple Steelhead appliances, you can use it to automatically configure them.

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

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

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

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

---

**Tip:** If you mistakenly answer **no**, to return to the wizard from the CLI, enter the **configuration jump-start** command from configuration mode. For detailed information, see the [“To restart the configuration wizard” on page 32](#).

---



### 3. Complete the configuration wizard steps on the client side and server side.

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

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

The system confirms your settings:

```

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

```

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

The Steelhead appliance configuration wizard automatically saves your settings.

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

```
amnesiac> exit
```

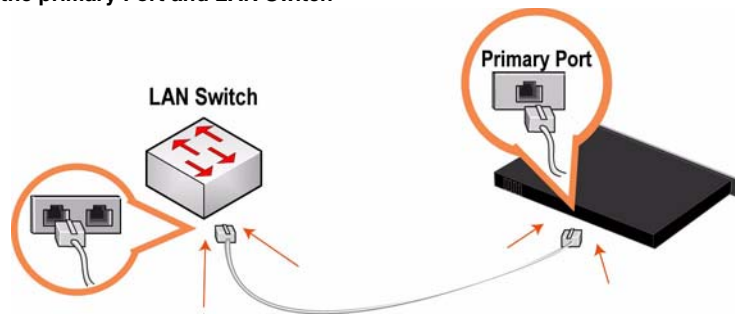
## Connecting the Steelhead Appliance to Your Network

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

### To connect the Steelhead appliance to your network

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

**Figure 3-12. Connecting the primary Port and LAN Switch**



## Configuring the Client-Side Appliance

In an out-of-path configuration, you configure the client-side Steelhead appliance 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 appliance that points to the out-of-path, server-side Steelhead appliance. You can define fixed-target rules using the Management Console or the CLI.

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

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

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

### To configure the client-side Steelhead appliance

1. Follow the procedures for an in-path configuration. For details, see [“Configuring In-Path Steelhead Appliances” on page 31](#).
2. Connect to the Management Console. For details, see [“Connecting to the Management Console” on page 38](#).

- Go to the Configure > Optimization > In-Path Rules page.

Figure 3-13. In-Path Rules Page

**In-Path Rules:**

▼ Add a New In-Path Rule    — Remove Selected Rules    ⇅ Move Selected Rules...

Type: Fixed-Target ▼

Position: End ▼

Source Subnet: 0.0.0.0/0

Destination Subnet: 0.0.0.0/0    Port: all

Target Appliance IP Address: \*    Port: 7810

Backup Appliance IP Address:    Port: 7810

VLAN Tag ID: all (all, untagged, 1..4094)

Preoptimization Policy: None ▼

Optimization Policy: Normal ▼

Latency Optimization Policy: Normal ▼

Neural Framing Mode: Always ▼

Auto Kickoff:

WAN Visibility Mode: Correct Addressing ▼

Description:

Add

<input type="checkbox"/>	Rule	Type	Source	Destination	Target	Backup	Preoptimization Policy	Optimization Policy	Latency Policy	Neural	Kickoff	WAN Visibility	VLAN
<input type="checkbox"/>	Q 1	Pass	All	All:Secure	--	--	--	--	--	--	--	--	All
<input type="checkbox"/>	Q 2	Pass	All	All:Interactive	--	--	--	--	--	--	--	--	All
<input type="checkbox"/>	Q 3	Pass	All	All:RBT-Proto	--	--	--	--	--	--	--	--	All

- Under In-Path Rules, click **Add a New In-Path Rule** to display the in-path rule configuration options.
- For Type, select **Fixed-Target** from the drop-down list.

- For Target Appliance IP Address, specify the IP address and port number for the peer Steelhead appliance.

Use the format 0.0.0.0/0. The IP address must be the primary Port IP address on the target Steelhead appliance. The default port is 7810.

- Optionally, if you have a backup, out-of-path Steelhead appliance 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 the format 0.0.0.0/0. The default port is 7810.

- Click **Add Rule** to apply the rule to the running configuration.
- Click **Save** to write your settings to memory.

For detailed information about verifying your connections and configuration settings, see [“Verifying Your Connections” on page 36](#) and [“Verifying Your Configuration” on page 39](#).

You can now optimize WAN traffic using the Steelhead appliance.

## CHAPTER 4 Troubleshooting

This chapter describes how to troubleshoot the Steelhead appliance installation.

---

### Troubleshooting

This section describes how to troubleshoot the following:

- [“Cables” on page 45](#)
- [“Duplex Mismatch” on page 46](#)
- [“In-Path Steelhead Appliances Connection” on page 47](#)
- [“Oplock Issues” on page 47](#)
- [“CIFS Overlapping Open Optimization Denies Multi-User Access” on page 48](#)
- [“IP address Configuration” on page 50](#)
- [“Asymmetric Routing” on page 50](#)
- [“Packet Ricochet” on page 51](#)
- [“Packet Ricochet—Internet Control Messaging Protocol \(ICMP\) Redirects” on page 51](#)
- [“Auto-Discovery Failure” on page 53](#)
- [“Protocol Optimization Errors” on page 54](#)
- [“Server-Side Out-of-Path Connection Caveats” on page 54](#)
- [“Specific Problems” on page 55](#)

### Cables

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

## Solution

To ensure that the traffic flows when the Steelhead appliance is optimizing traffic, and when the Steelhead appliance transitions to bypass mode, use the appropriate crossover or straight-through cable to connect the Steelhead appliance 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 appliance to router: crossover cable
- Steelhead appliance to switch: straight-through cable
- Steelhead appliance to Steelhead appliance: crossover cable
- Steelhead appliance to a host: crossover cable

## Duplex Mismatch

The following symptoms occur due to a duplex mismatch:

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

## Possible Cause

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

## Example

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

- no Steelhead appliance – 3:16
- cold Steelhead appliance – 5:08
- warm Steelhead appliance – 3:46

Adding a pass through rule for an application does not help. Slow connections appear as optimized in the Management Console on the Current Connections report page. However, stopping the Steelhead appliance 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 appliance CLI and enter the flood-ping command to check the duplex mismatch:

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

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

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

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

## In-Path Steelhead Appliances Connection

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

### Possible Cause

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

### Solutions

To resolve the Steelhead appliance connection issue:

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

## Oplock Issues

The following 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 anti-virus 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 cannot 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 appliance only optimizes data when a client has exclusive access to the data.

When an oplock is not available, the Steelhead appliance does not 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, Steelhead appliances still increase WAN performance, but not as effectively as when application optimizations are available.

To resolve oplock issues:

- Upgrade your anti-virus 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 48](#).
- 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 Cascade 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 anti-virus software that is scanning the files over the WAN or that the anti-virus software does not 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

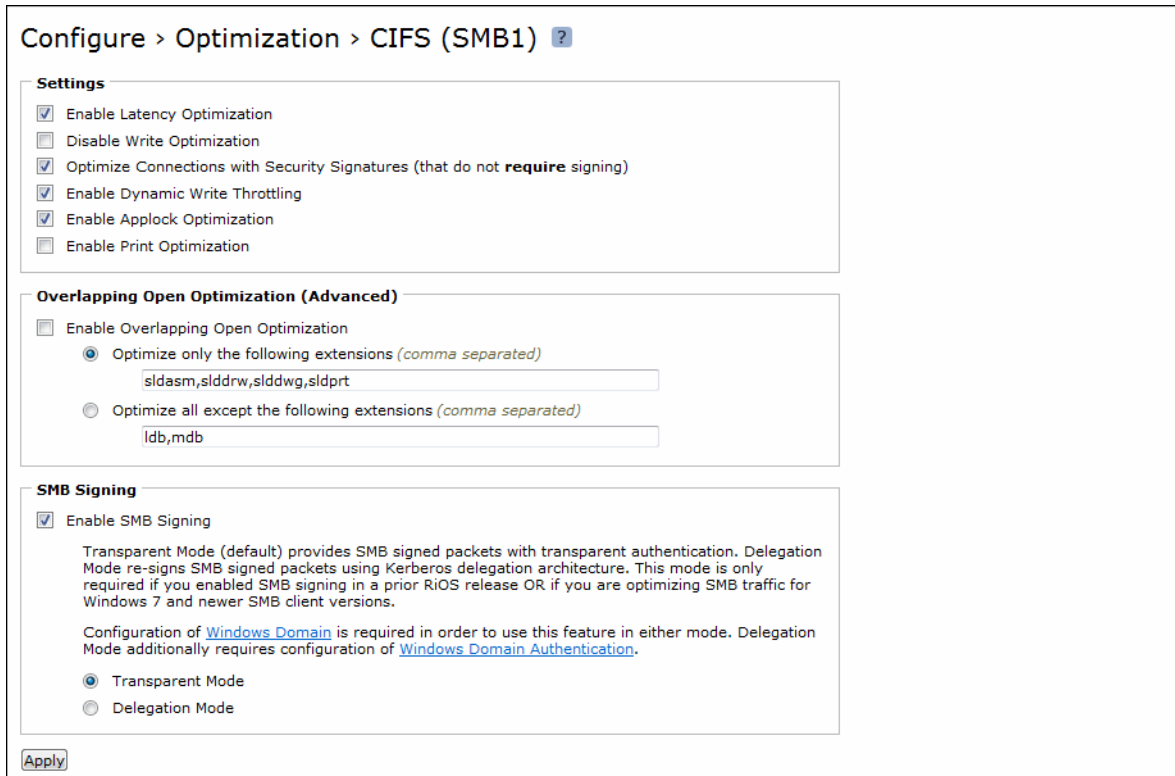
To resolve the CIFS overlapping open optimization issue, configure CIFS overlapping open optimization on the client-side Steelhead appliance as follows:

1. Connect to the Steelhead Management Console. For details, see the *Steelhead Management Console User's Guide*.



- On the client-side Steelhead appliance, choose Configure > Optimization > CIFS (SMB1) to display the CIFS (SMB1) page.

Figure 4-1. CIFS (SMB1) Page



- Under Overlapping Open Optimization (Advanced), complete the configuration as described in the following table.

Control	Description
Enable Overlapping Open Optimization	<p>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.</p> <p><b>Note:</b> Enable this setting on the client-side Steelhead appliance.</p> <p>With overlapping opens enabled, the Steelhead appliance optimizes data where exclusive access is available (when locks are granted). When an oplock is not available, the Steelhead appliance does not perform application-level latency optimizations but still performs SDR and compression on the data as well as TCP optimizations.</p> <p><b>Note:</b> 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 the file fails to go through a v3.x.x or later Steelhead appliance or if it does not go through a Steelhead appliance: for example, certain applications that are sent over the LAN. If this occurs, you should disable overlapping opens for such applications.</p> <p>Use the radio buttons to set either an include list or exclude list of file types subject to overlapping opens optimization.</p>

Control	Description
Optimize only the following extensions	Specify a list of extensions you want to include in overlapping opens optimization.
Optimize all except the following extensions	Specify a list of extensions you do not want to include. For example, you should specify any file extensions that use Enable Applock Optimization.

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 Steelhead appliances cannot connect to each other or to your network.

### Solutions

To verify the IP address has been configured correctly:

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

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

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

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

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

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

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

- Verify that the client-side Steelhead appliance is visible to the server-side Steelhead appliance.

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

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

## Asymmetric Routing

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

## Possible Cause

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

## Solutions

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

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

## Packet Ricochet

The following symptoms occur due to packet ricochet:

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

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

## Possible Cause

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

## Solutions

To resolve packet ricochet issues:

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

## Packet Ricochet—Internet Control Messaging Protocol (ICMP) Redirects

The following symptoms occur due to packet ricochet ICMP redirects:

- Connections fail on first attempt, but succeed on second attempt.
- On one or both sites, the in-path interface on the Steelhead appliance 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 appliance to the next hop LAN gateway.
- The WAN router is probably dropping the SYN from the Steelhead appliance 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 52](#).
- 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 appliance 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 appliance is in a different subnet from the client and the server.

Without simplified routing, if a Steelhead appliance 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 appliance. In some cases, even with the static routes defined, the Access Control List (ACL) on the default gateway can still drop traffic that should have gone through the other router. Enabling simplified routing eliminates this issue.

Simplified routing has the following constraints:

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

---

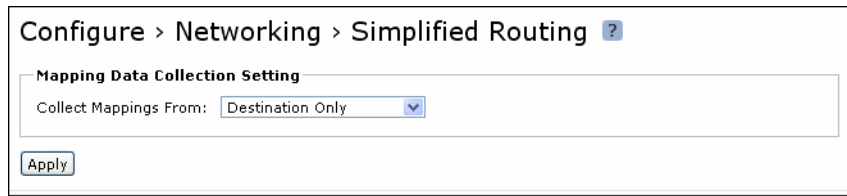
**Tip:** For detailed information, see the *Riverbed Deployment Guide*.

---

### To enable simplified routing

1. Choose Configure > Networking > Simplified Routing to display the Simplified Routing page.

Figure 4-2. Simplified Routing Page



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

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

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

## Auto-Discovery Failure

When auto-discovery fails, all traffic passes through with the Steelhead appliance 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 appliance.
  - Specify the **Target Appliance IP Address** and its port as 7800 on the opposite Steelhead appliance (in-path without auto-discovery).
- Configure end nodes (firewalls) to allow your probe to pass through.
- Configure the Steelhead appliance IP address as the friendly IP address for IDS or IPS.

- Cisco PIX Firewall IOS v7.0 might block the auto-discovery probe. Some firewall configurations strip TCP options or drop packets with these options. You can keep this configuration and switch to fixed-target rules or change the configuration on the firewall.

## Protocol Optimization Errors

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

### Solutions

To resolve protocol optimization errors, check:

- that connections have been successfully established.
- that Steelhead appliances 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 Steelhead appliances unoptimized.
- that the LAN and WAN cables are not inadvertently swapped.

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

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

- OOP configuration does not support auto-discovery. You must create a fixed-target rule on the client-side Steelhead appliance.
- You must create an OOP connection from an in-path or logical in-path Steelhead appliance and direct it to port 7810 on the primary interface of the server-side Steelhead appliance. This setting is mandatory.
- Interception is not supported on the primary interface.
- An OOP configuration provides non-transparent optimization from the server perspective. Clients connect to servers, but servers treat it like a server-side Steelhead appliance connection. This affects:
  - log files.
  - server-side ACLs.
  - bi-directional applications such as rsh.
- You can use OOP configurations along with in-path or logical in-path configurations.

## Specific Problems

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

Problem	Solution
The <b>show interfaces</b> CLI command displays 4294967295 as the number of errors on an interface.	The bypass card is not properly installed; reinstall it. For details, see the <i>Network Interface Card Installation Guide</i> .
The Steelhead appliance blocks traffic when going into bypass mode.	If a Steelhead appliance blocks traffic when going into bypass mode, verify that connections to its neighboring devices are correctly configured. Ensure that the cable from the Steelhead appliance to the switch is a straight-through cable and the cable from the Steelhead appliance to the router is a crossover cable. Also, ensure that there are no network speed or duplex mismatches.
The Steelhead appliance does not come out of bypass mode when the network connection is restored.	If a Steelhead appliance does not come out of bypass mode, verify that: <ul style="list-style-type: none"> <li>The in-path interface has an IP address. For example, at the system prompt, enter the <b>show interfaces</b> CLI command.</li> <li>In-path interception is enabled. For example, at the system prompt, enter the <b>show in-path</b> CLI command. Expected results are: <pre>Enabled: yes Optimizations Enabled On: inpath0_0</pre> </li> <li>The bypass service is running. For example, at the system prompt, enter the <b>show service</b> CLI command. To enable the Steelhead appliance service if it is not running, use the CLI command <b>service enable</b>.</li> <li>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 <b>show licenses</b> CLI command. For questions about licenses, contact Riverbed Support at <a href="https://support.riverbed.com">https://support.riverbed.com</a>.</li> </ul>
The Steelhead appliance fails to boot.	Ensure that: <ul style="list-style-type: none"> <li>The power strip or the uninterruptable power supply (UPS) the Steelhead appliance is plugged into is turned on and is functioning properly.</li> <li>The rocker switch on the back of the Steelhead appliance (Series xx20) is turned on. (When on, the rocker switch is in the depressed, or 1 position.)</li> </ul>

## 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 appliance remotely, delete

```
console=tty0
```

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

```
console=ttyS0
```

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

```
single fastboot
```

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

---

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

---

9. Press Enter.

10. Press B to continue booting. 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 appliance, check the following configuration settings:

- Speed and duplex.
- QoS integration.
- Multi-hop optimization.
- Packet ricochet.



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



## APPENDIX A    **Series xx55 Status Lights and Ports, Technical Specifications**

This appendix describes the status lights and ports, and the technical and environmental specifications. It includes the following sections:

- [“CX555 and CX755 Status Lights and Ports” on page 60](#)
- [“CX1555 Status Lights and Ports” on page 62](#)
- [“CX555 and CX755 Technical Specifications” on page 63](#)
- [“CX1555 Technical Specifications” on page 64](#)
- [“Environmental Specifications” on page 64](#)

## CX555 and CX755 Status Lights and Ports

The following figure illustrates the CX555 and CX755 status light and port locations.

Figure A-1. Front Panel

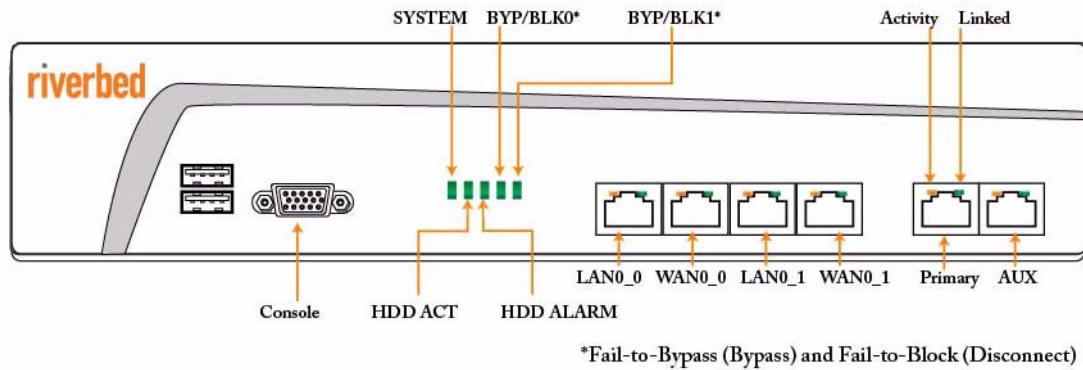
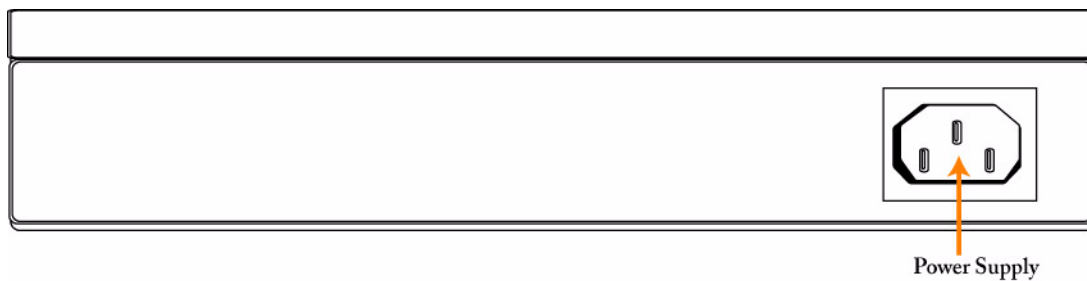


Figure A-2. Back Panel



## System LEDs

The following table summarizes the system LEDs.

<b>SYSTEM</b>	Healthy = Blue Degraded = Yellow Critical = Red System Boot = Yellow
<b>HDD ACT</b>	HDD Activity = Blinking Blue
<b>BYP/BLK (Bypass or Block (Disconnect) Mode)</b>	Normal = No Light Bypass or Block (Disconnect) = Orange

---

<b>HDD ALARM</b>	Disk Connected = Solid Blue Read/Write Activity = Blinking Blue Failed Disk = Orange
<b>LAN-WAN LEDs</b>	Left LED Link = Solid Green Activity = Blinking Green  Right LED GB = Green 100-MB = Orange 10-MB = No Light

---

## CX1555 Status Lights and Ports

The following figures illustrate the 1U CX1555 status light and port locations.

Figure A-3. Front Panel

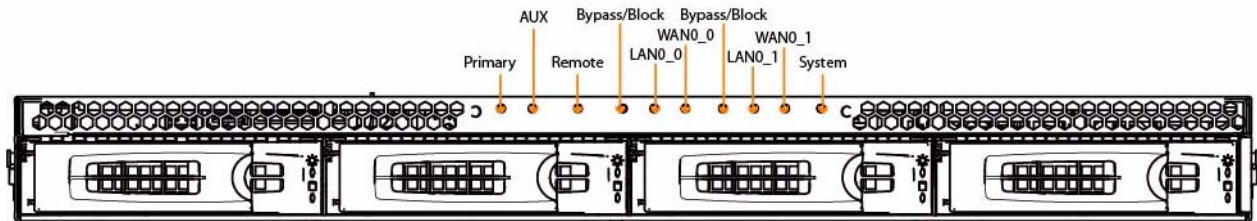
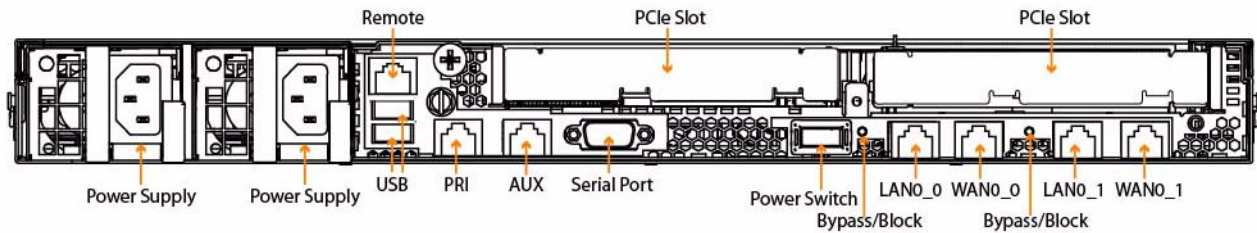


Figure A-4. Back Panel



## System LEDs

The following table summarizes the CX1555 system LEDs.

LED	Status
<b>SYSTEM</b>	Normal = Solid Blue Powering Up = Red
<b>PRI = Primary</b> <b>AUX = Auxiliary</b> <b>REM = Remote</b>	Link and Traffic = Flashes Blue
<b>LAN-WAN</b>	Link and Traffic = Flashes Blue
<b>BYP/BLK</b> <b>BYP = Bypass</b> <b>BLK = Block (Disconnect)</b>	Normal = No Light Bypass or Block (Disconnect) = Amber
<b>HDDs/SSDs</b>	Disk Connected = Solid Blue Read/Write Activity = Blinks Blue Failed Disk = Amber

LED	Status
<b>Back Panel</b> <b>PRI = Primary</b> <b>AUX = Auxiliary</b> <b>REM = Remote</b>	<b>Left LED</b> Link = Solid Green Activity = Flashes Green
	<b>Right LED</b> GB = Amber 100 MB = Green (REM only at 100 MB) 10 MB = No Light
<b>Back Panel</b> <b>LAN-WAN</b>	<b>Left LED</b> Link = Solid Green Activity = Flashes Green
	<b>Right LED</b> GB = Amber 100 MB = Green 10 MB = No Light
	<b>BYP/BLK</b> Normal = No Light Bypass or Block (Disconnect) = Amber

## CX555 and CX755 Technical Specifications

The following table summarizes the technical specifications for the CX555 and CX755 systems.

Series	Power (Typical)	VA (max)	BTU	Hard Disk	Data Store	Dimensions (LxWxH)	Weight (without packaging)	Voltage Frequency	PSU	Bypass Ports/ Max # Ports
CX555* Desktop M-H	45 W	62.5	145 BTU	2 x 250 GB	80 GB	7.1x12x1.65 in 180.3x304.8x 42 mm	4.7 lbs 2.15 kg	100-127V, 200-240V	Single 100 W Internal 100- 240Vac, 50/60Hz, 2-1 A	4
CX755 Desktop L-M-H	50 W	66.5	165 BTU	2 x 250 GB H= 1 x 250 GB HDD + 1 x 160 SSD	100-160 GB	7.1x12x1.65 in 180.3x304.8x 42 mm	4.7 lbs. 2.15 kg	100-127V, 200-240V	Single 100 W Internal 100- 240Vac, 50/60Hz, 2-1 A	4

## CX1555 Technical Specifications

The following table summarizes the technical specifications for the CX Series xx55 platform.

Series	HDD/SSD	Data Store	Dimensions (LxWxH)	Weight (without packaging)	Voltage	PSU	PCIe Slots	Bypass Ports/Max # Ports
CX1555	4 x 500 GB	400 GB	25.4x17.2x1.71 in	36 lbs	100-127V, 200-240V	2 x 450 W	2	12
1U		H=320 GB	645.4x436x43.5 mm	16.36 kg		100-127Vac/8A, 50/60Hz		
L/M/H	H=1320 GB	SSD				200-240Vac/4A, 50/60Hz		

## CX1555 Power Requirements and Consumption

The following table summarizes the power specifications for the CX1555 systems. The systems are rated at the following power characteristics when operating at nominal AC input voltages (120 V and 230 V)..

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

## Environmental Specifications

The following table summarizes the environmental requirements for the CX Series xx55 platforms.

Model	Operating Acoustic	Temperature (Operating)	Temperature (Storage)	Relative Humidity	Storage Humidity
CX555, CX755	45 dBA Sound pressure (Typical)	0° - 45° C 32° - 113° F	-40° - 65° C -40° - 149° F	20% - 80% non-condensing	5% - 95% non-condensing
CX1555	62 dBA Sound Pressure (Typical)	10° - 40° C 50° - 104° F	-40° - 65° C -40° - 149° F	20% - 80% non-condensing	5% - 95% non-condensing



## APPENDIX B Series xx50 Status Lights and Ports, Technical Specifications

This appendix describes the status lights and ports, and the technical and environmental specifications. It includes the following sections:

- [“Series xx50 Status Lights and Ports” on page 65](#)
- [“Series xx50 Bypass Cards Status Lights” on page 71](#)
- [“Technical Specifications” on page 80](#)
- [“Environmental Specifications” on page 82](#)

---

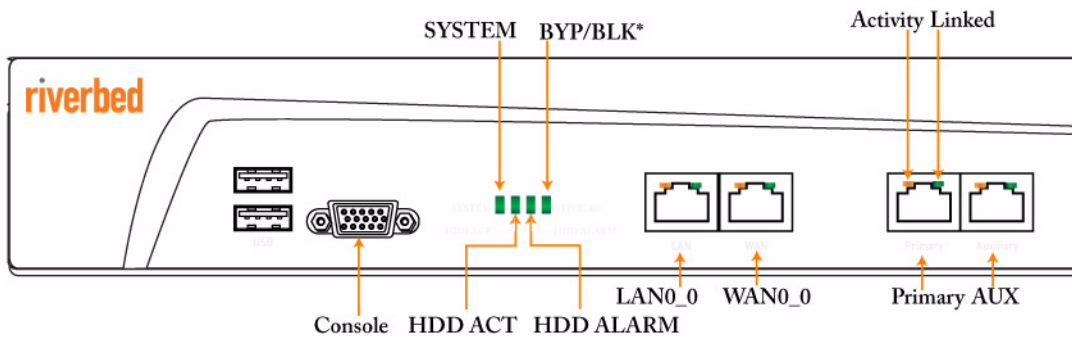
### Series xx50 Status Lights and Ports

This section describes the Series xx50 status lights and ports.

#### Series 250 and 550

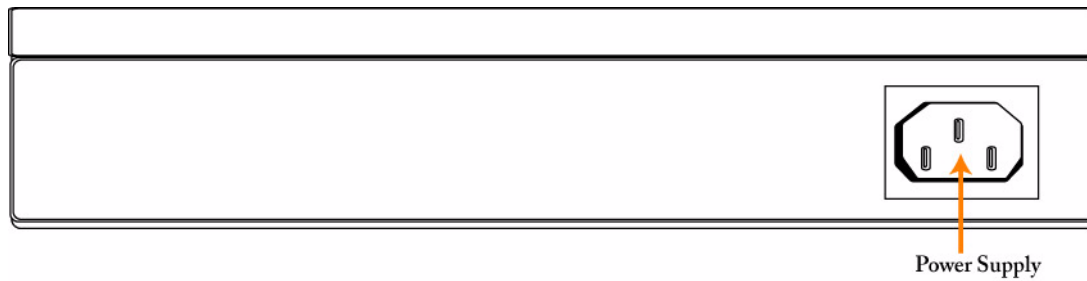
The following figure illustrates the Series 250 and 550 status light and port locations.

**Figure B-1. Front Panel**



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

Figure B-2. Back Panel



## System LEDs

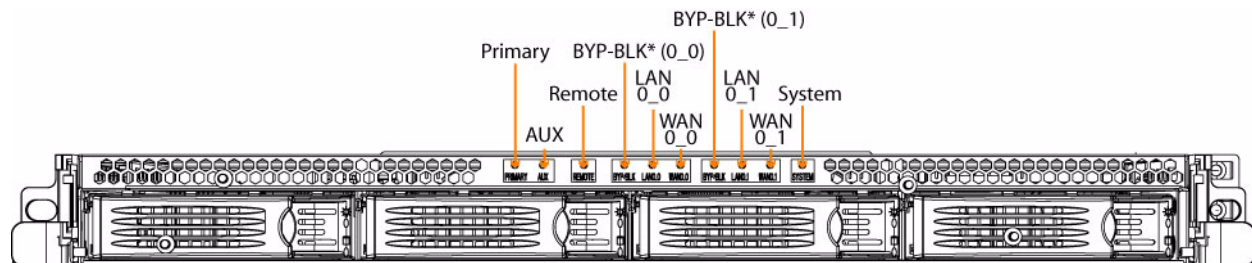
The following table summarizes the 250 and 550 system LEDs.

<b>SYSTEM</b>	Healthy = Blue Degraded = Yellow Critical = Red System Boot = Yellow
<b>HDD ACT</b>	HDD Activity = Blinking Blue
<b>BYP/BLK (Bypass or Block (Disconnect) Mode)</b>	Normal = No Light Bypass or Block (Disconnect) = Orange
<b>HDD ALARM</b>	Disk Connected = Solid Blue Read/Write Activity = Blinking Blue Failed Disk = Orange
<b>LAN-WAN LEDs</b>	Left LED Link = Solid Green Activity = Blinking Green  Right LED GB = Green 100-MB = Orange 10-MB = No Light

## Series 1050 and 2050

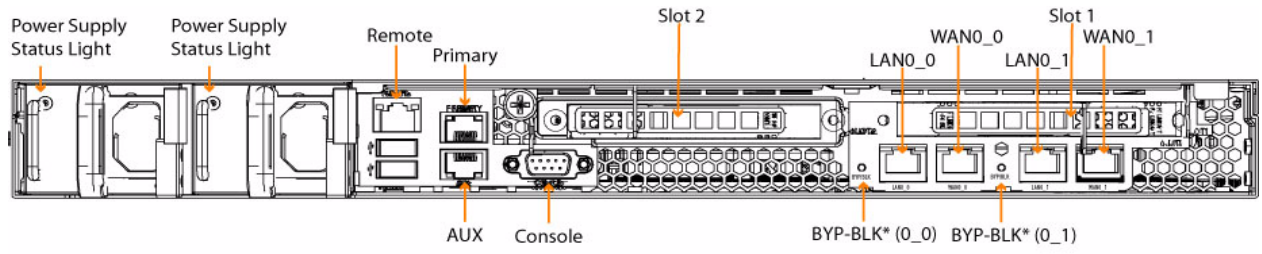
The following figure illustrates the Series 1050 and 2050 status light and port locations.

Figure B-3. Front Panel



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

Figure B-4. Back Panel



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

## System LEDs

<b>SYSTEM LEDs</b>	Healthy = Blue Degraded = Yellow Critical = Red System Boot = Yellow
<b>NETWORK STATUS LEDs (Front LAN-WAN LEDs)</b>	Link = Solid Blue Activity = Blinking Blue
<b>BYP/BLK (Bypass or Block (Disconnect) Mode)</b>	Normal = No Light Bypass or Block (Disconnect) = Orange
<b>HDD LEDs</b>	Disk Connected = Solid Blue Read/Write Activity = Blinking Blue Failed Disk = Orange
<b>LAN-WAN LEDs</b>	Left LED Link = Solid Green Activity = Blinking Green  Right LED GB = Orange 100-MB = Green 10-MB = No Light

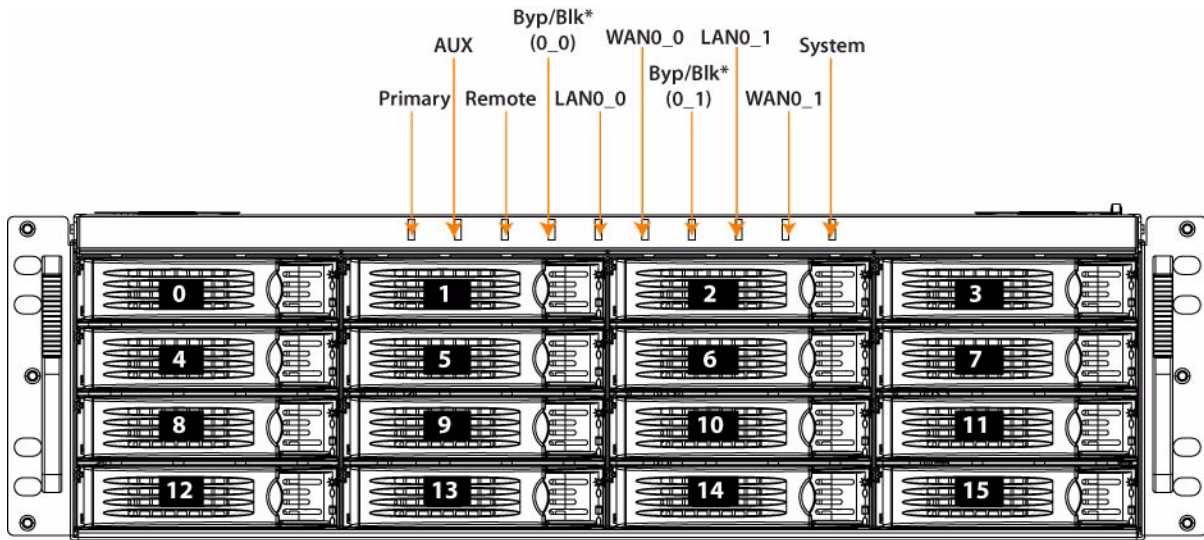
## Power Supply LEDs

LED	Condition
Solid Green	Healthy power supply with AC power connected.
Blinking Green	Unit is halted, but the power supplies are still connected to AC power.
Solid Orange	AC power is not connected to this power supply, but the unit is still powered on due to the other power supply. Occurs when the power supply automatically shuts off due to some error condition, such as an overheat.
Blinking Orange	Indicates a power supply predictive-fail condition, such as a fan failure. The power supply may then shut itself off, which changes the LED to solid orange. A log entry of this predictive-fail can be viewed using the <b>show hardware error-log all</b> command in the Riverbed Command-Line Interface.
No LED	No AC power connected.

## Series 5050 and 6050

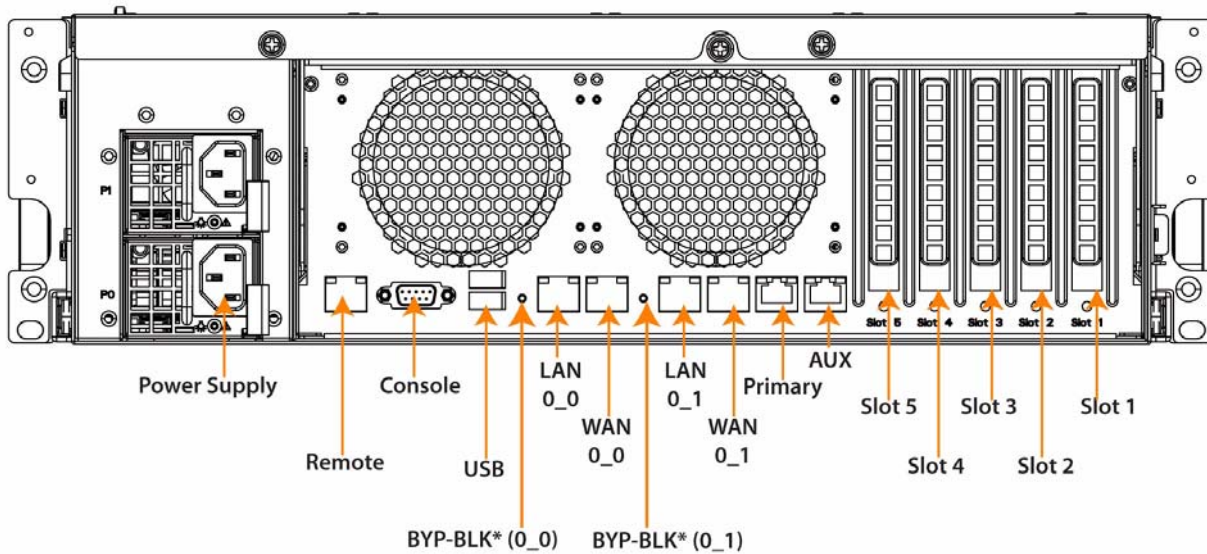
The following figure illustrates the Series 5050 and 6050 status light and port locations.

Figure B-5. Front Panel



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

Figure B-6. Back Panel.



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

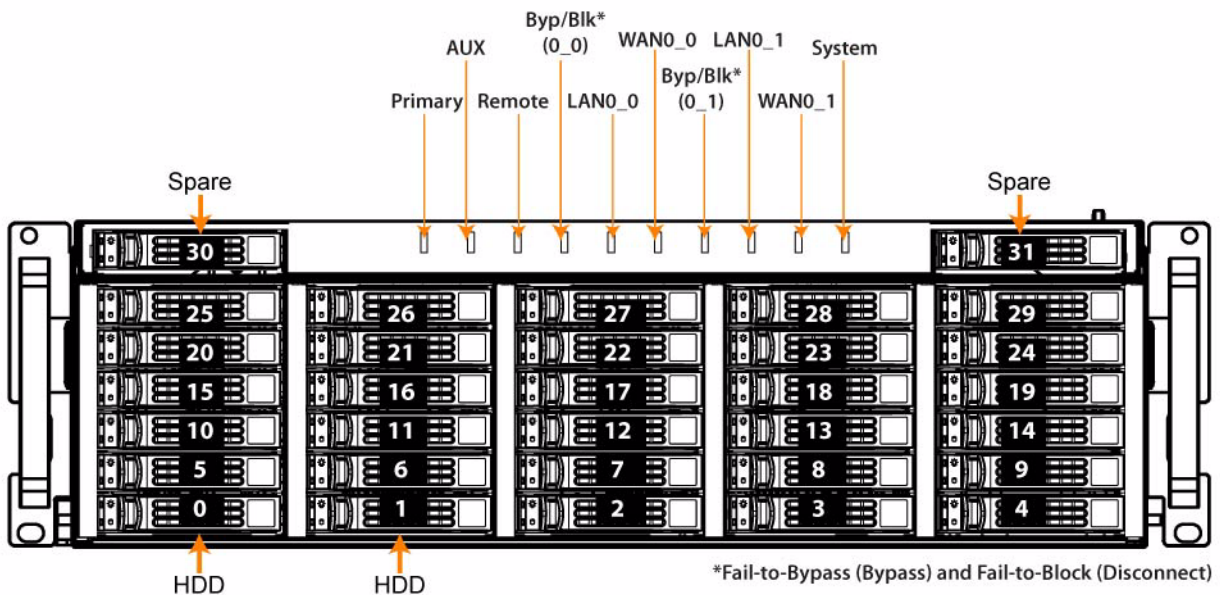
## System LEDs

<b>SYSTEM LEDs</b>	Healthy = Blue Degraded = Yellow Critical = Red System Boot = Yellow
<b>NETWORK STATUS LEDs</b>	Link = Solid Blue Activity = Blinking Blue
<b>BYP/BLK (Bypass or Block (Disconnect) Mode)</b>	Normal = No Light Bypass or Block (Disconnect) = Orange
<b>HDD LEDs</b>	Disk Connected = Solid Blue Read/Write Activity = Blinking Blue Failed Disk = Orange
<b>LAN-WAN LEDs</b>	Left LED Link = Solid Green Activity = Blinking Green  Right LED GB = Orange 100-MB = Green 10-MB = No Light

## Series 7050

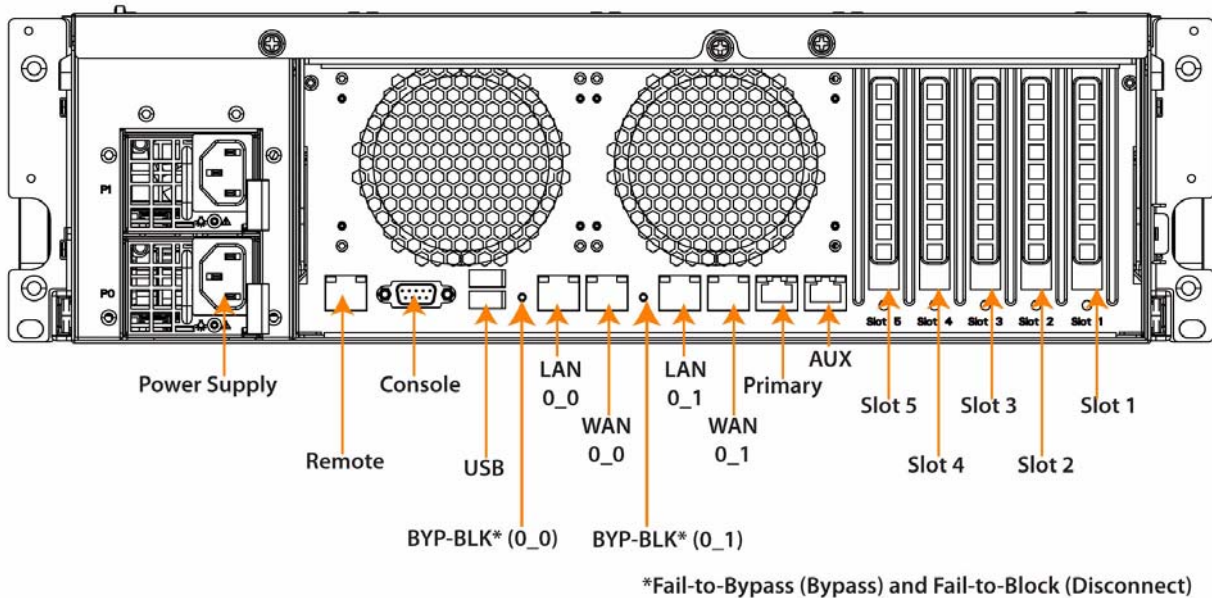
The following figure illustrates the Series 7050 status light and port locations.

Figure B-7. Front Panel



**Note:** Disk drive numbers 0 and 1 are HDD. Drive numbers 2-29 are SSD.

Figure B-8. Back Panel



## System LEDs

<b>SYSTEM LEDs</b>	Healthy = Blue Degraded = Yellow Critical = Red System Boot = Yellow
<b>NETWORK STATUS LEDs</b>	Link = Solid Blue Activity = Blinking Blue
<b>BYP/BLK (Bypass or Block (Disconnect) Mode)</b>	Normal = No Light Bypass or Block (Disconnect) = Orange
<b>HDD LEDs</b>	Disk Connected = Solid Blue Read/Write Activity = Blinking Blue Failed Disk = Orange
<b>LAN-WAN LEDs</b>	Left LED Link = Solid Green Activity = Blinking Green  Right LED GB = Orange 100-MB = Green 10-MB = No Light

For details on the power supply LEDs, see [“Power Supply LEDs” on page 68](#).

## Series xx50 Bypass Cards Status Lights

The following section describes the status lights for the bypass cards supported on Series xx50 platforms. It includes the following sections:

- [“Bypass Card Manufacturing Numbers Series xx50” on page 72](#)

- “Four-Port Copper Gigabit-Ethernet PCI-E Card” on page 75
- “Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-E Card” on page 76
- “Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-E Card” on page 76
- “Two-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E Card” on page 77
- “Four-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E Card” on page 77
- “Two-Port FX Multimode Fiber 100 Mbps PCI-E Card” on page 78
- “Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E Card” on page 79
- “Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E Card” on page 79

## Bypass Card Manufacturing Numbers Series xx50

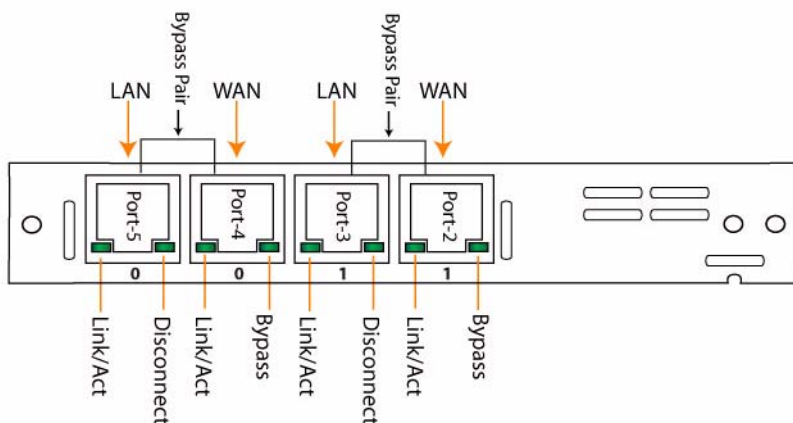
The following section describes the bypass card manufacturing part numbers. To determine the manufacturing part number for your bypass card, run the **show hardware** command in the CLI.

NICs for Series xx50	Manufacturing Part #	Orderable Part #
Four-Port Copper GigE PCI-E Card	410-00103-01	NIC-01G0-4TX
Two-Port SX Multimode Fiber GigE PCI-E Card	410-00101-01	NIC-01G-2SX
Four-Port SX Multimode Fiber GigE PCI-E Card	410-00102-01	NIC-01G-4SX
Two-Port LX Single Mode Fiber GigE PCI-E Card	410-00105-01	NIC-01G-2LX
Four-Port LX Single Mode Fiber GigE PCI-E Card	410-00106-01	NIC-01G-4LX
Two-Port FX Multimode Fiber 100 Mbps PCI-E Card	410-00107-01	NIC-01M-2FX
Two-Port SR Multimode Fiber 10 GigE PCI-E Card	410-00302-01	NIC-10G-2SR
Two-Port LR Single Mode Fiber 10 GigE PCI-E Card	410-00301-01	NIC-10G-2LR

## Four-Port 1GbE TX Copper NIC

The following section describes the Four-Port Copper Gigabit-Ethernet PCI-E (Four-Port Copper GigE PCI-E) card (410-00103-01) status lights.

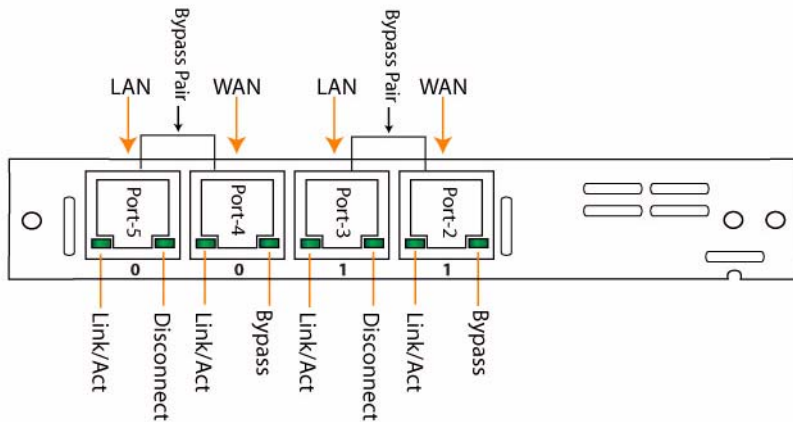
Figure B-9. Four-Port Copper GigE PCI-E Card





The following section describes the Four-Port Copper Gigabit-Ethernet PCI-E (Four-Port Copper GigE PCI-E) card (410-00103-01) status lights.

**Figure B-10. Four-Port Copper GigE PCI-E Card**



The following table describes the Four-Port Copper GigE PCI-E card status and LED lights.

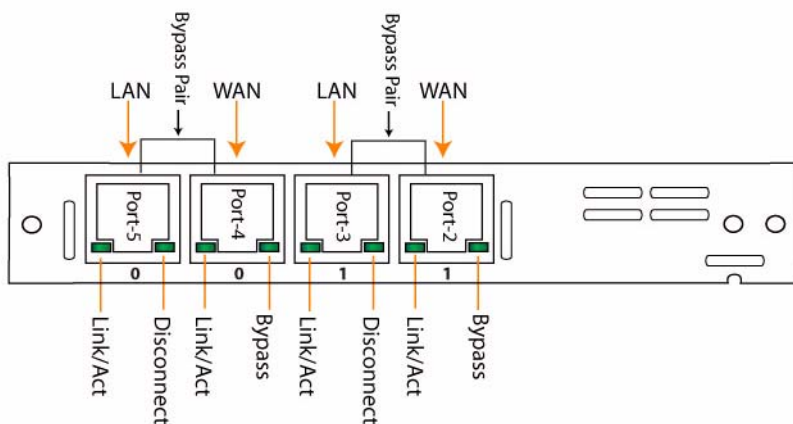
LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass	Solid green when in bypass mode.
Disconnect	Solid green in disconnect mode.

The interface names for the NICs in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

## Four-Port 1GbE SX Multi Mode Fiber NIC

The following section describes the Four-Port Copper Gigabit-Ethernet PCI-E (Four-Port Copper GigE PCI-E) card (410-00103-01) status lights.

**Figure B-11. Four-Port Copper GigE PCI-E Card**



The following table describes the Four-Port Copper GigE PCI-E card status and LED lights.

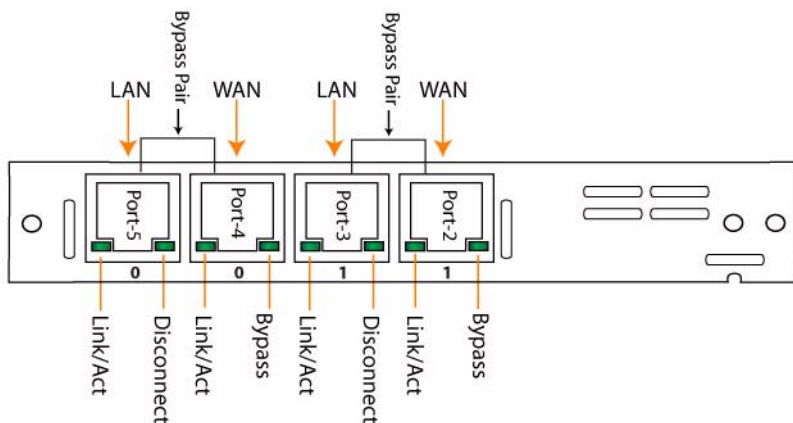
LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass	Solid green when in bypass mode.
Disconnect	Solid green in disconnect mode.

The interface names for the NICs in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

## Four-Port 1GbE LX Single Mode Fiber NIC

The following section describes the Four-Port Copper Gigabit-Ethernet PCI-E (Four-Port Copper GigE PCI-E) card (410-00103-01) status lights.

Figure B-12. Four-Port Copper GigE PCI-E Card



The following table describes the Four-Port Copper GigE PCI-E card status and LED lights.

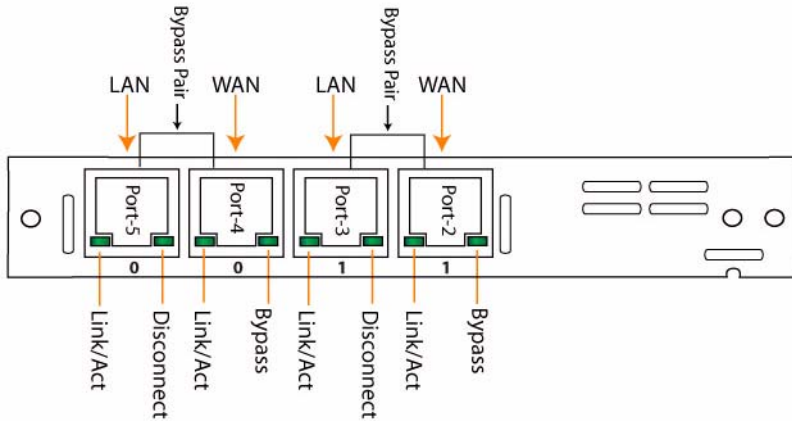
LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass	Solid green when in bypass mode.
Disconnect	Solid green in disconnect mode.

The interface names for the NICs in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

## Four-Port Copper Gigabit-Ethernet PCI-E Card

The following section describes the Four-Port Copper Gigabit-Ethernet PCI-E (Four-Port Copper GigE PCI-E) card (410-00103-01) status lights.

**Figure B-13. Four-Port Copper GigE PCI-E Card**



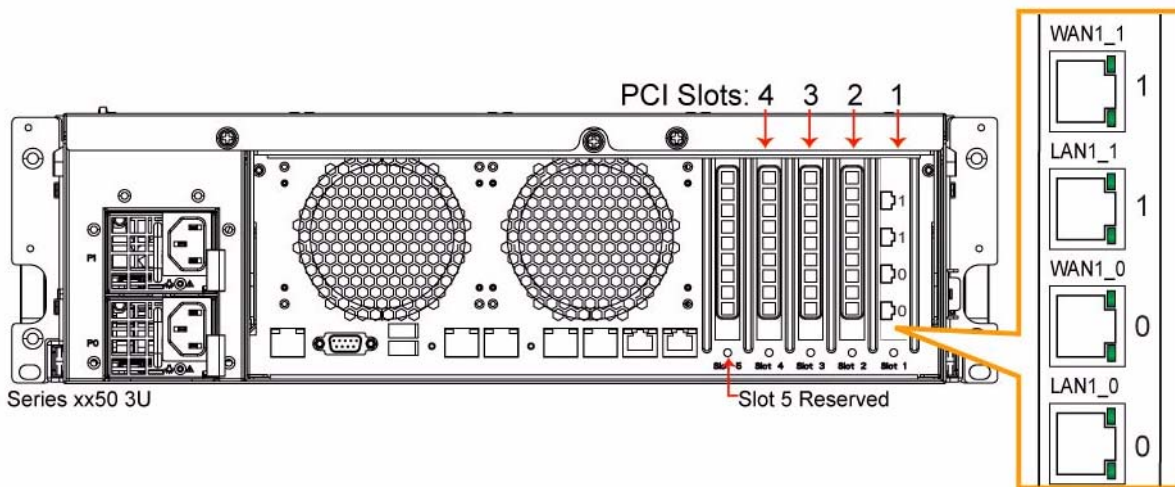
The following table describes the Four-Port Copper GigE PCI-E card status and LED lights.

LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass	Solid green when in bypass mode.
Disconnect	Solid green in disconnect mode.

The interface names for the NICs in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

For example, if a four-port NIC is located in slot 1 of your system, the interface names are lan1\_0, wan1\_0, lan1\_1, and wan1\_1, respectively.

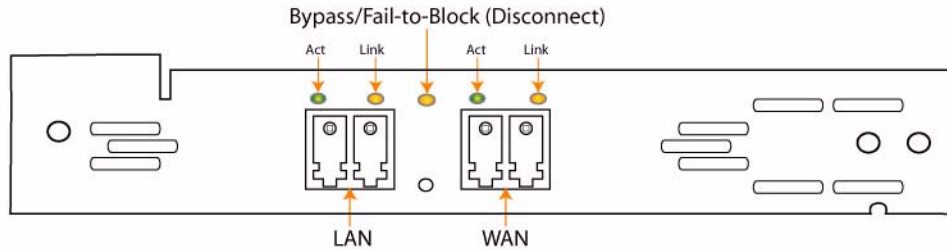
**Figure B-14. 3U Series xx50 Appliance Populated by a Four-Port Copper GigE PCI-E Card**



## Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-E Card

The following section describes the Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-E (Two-Port SX Multimode Fiber GigE PCI-E) card (410-00101-01) status lights.

**Figure B-15. Two-Port SX Multimode Fiber GigE PCI-E Card**



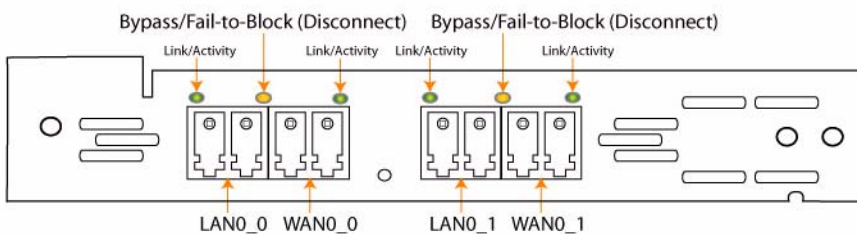
The following table describes the Two-Port SX Multimode Fiber GigE PCI-E card status and LED lights.

LED	Condition
Link	Solid yellow on link.
Activity	Blinks green on activity.
Bypass/Fail-to-Block (Disconnect)	Solid green in bypass mode. Solid yellow in disconnect mode.

## Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-E Card

The following section describes the Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-E (Four-Port SX Multimode Fiber GigE PCI-E) card (410-00102-01) status lights.

**Figure B-16. Four-Port SX Multimode Fiber GigE PCI-E Card**



The following table describes the Four-Port SX Multimode Fiber GigE PCI-E card status and LED lights.

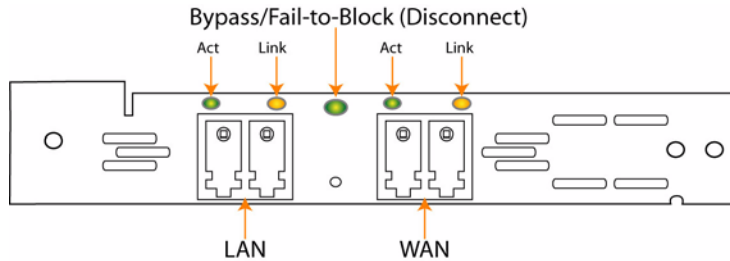
LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass/Fail-to-Block (Disconnect)	Solid green in bypass mode. Solid yellow in disconnect mode.

## Two-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E Card

**Important:** The LX Fiber PCI-E NICs require software v4.1.9, v5.0.7, or v5.5.2 or later.

The following section describes the Two-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E (Two-Port LX Single Mode Fiber GigE PCI-E) card (410-00105-01) status lights.

**Figure B-17. Two-Port LX Single Mode Fiber GigE PCI-E Card**



The following table describes the Two-Port LX Single Mode Fiber GigE PCI-E card status and LED lights.

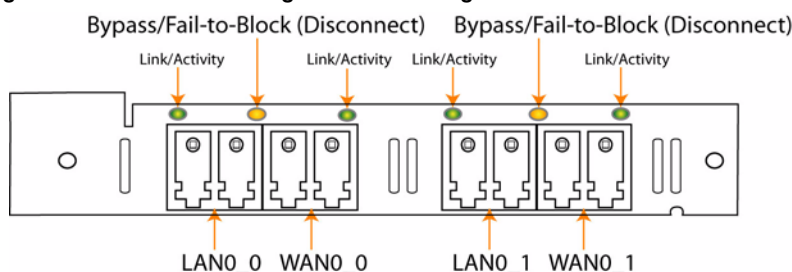
LED	Condition
Link	Solid yellow on link.
Activity	Blinks green on activity.
Bypass/Fail-to-Block (Disconnect)	Solid green in bypass mode. Solid yellow in disconnect mode.

## Four-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E Card

The following section describes the Four-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E (Four-Port LX Single Mode Fiber GigE PCI-E) card (410-00106-01) status lights.

**Important:** The LX Fiber PCI-E NICs require software v4.1.9, v5.0.7, or v5.5.2 or later.

**Figure B-18. Four-Port LX Single Mode Fiber GigE PCI-E Card**



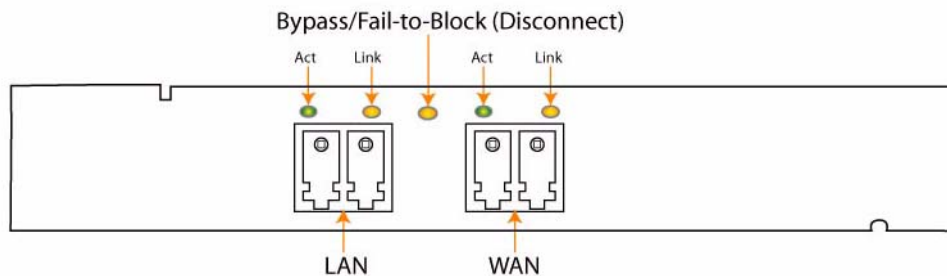
The following table describes the Four-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E card status and LED lights.

LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass/Fail-to-Block (Disconnect)	Solid green in bypass mode. Solid yellow in disconnect mode.

## Two-Port FX Multimode Fiber 100 Mbps PCI-E Card

The following section describes the Two-Port FX Multimode Fiber 100 Mbps PCI-E card (410-00107-01) status lights.

**Figure B-19. Two-Port FX Multimode Fiber 100 Mbps PCI-E Card**



The interface names for the NICs in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

For example, if a four-port NIC is located in slot 1 of your system, the interface names are lan1\_0, wan1\_0, lan1\_1, and wan1\_1, respectively.

**Important:** In a 1U appliance the LAN and WAN ports are numbered in ascending order (0, 1, 2, etc.) from left to right.

**Important:** In a 3U appliance the LAN and WAN ports are numbered in ascending order (0, 1, 2, etc.) from bottom to top.

The following table describes the Two-Port FX Multimode Fiber 100 Mbps PCI-E card status and LED lights.

LED	Condition
Link	GB = Yellow 100-MB = Green
Activity	Blinks green on activity.
Bypass/Fail-to-Block (Disconnect)	Solid green in bypass mode. Solid yellow in disconnect mode.

**Note:** Upon installation the Two-Port FX Multimode Fiber 100 Mbps PCI-E card defaults to 100-Mbps.

## Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E Card

The following section describes the Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E (Two-Port SR Multimode Fiber 10 GigE PCI-E) card (410-00302-01) status lights, for detailed information see, the *Network Interface Card Installation Guide*.

---

**Important:** RiOS software v5.5.7, v6.0.2 or later is required to run the Two-Port SR Multimode Fiber 10 GigE PCI-E card.

---

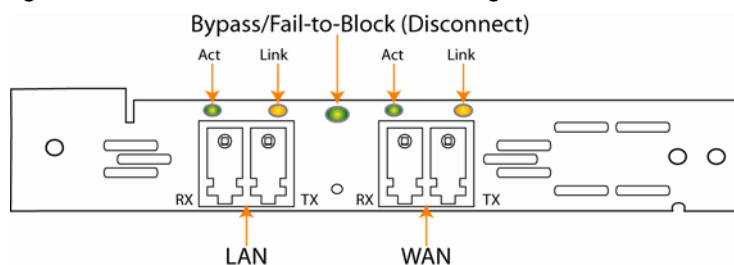
**Important:** Interceptor software v2.0.2a, v1.2.0a or later is required to run the Two-Port SR Multimode Fiber 10 GigE PCI-E card on Interceptor 9350 platforms. Interceptor software v2.0.3 is required to run four (4) Two-Port SR Multimode Fiber 10 GigE PCI-E cards. In systems running versions prior to v2.0.3 the Two-Port SR Multimode Fiber 10 GigE PCI-E card can be installed in slots 1, 2, and 3 of the Interceptor 9350. If slot 3 is populated with a Two-Port SR Multimode Fiber 10 GigE PCI-E card then slot 4 must remain empty.

---

**Important:** It is not necessary to plug in the 12 volt connector of the Two-Port SR Multimode Fiber 10 GigE PCI-E card.

---

**Figure B-20. Two-Port SR Multimode Fiber 10 GigE PCI-E Card**



The following table describes the Two-Port SR Multimode Fiber 10 GigE PCI-E card status and LED lights.

LED	Condition
Link	Solid green on link.
Activity	Blinks green on activity.
Bypass/Fail-to-Block (Disconnect)	Solid green in bypass mode. Solid yellow in disconnect mode.

---

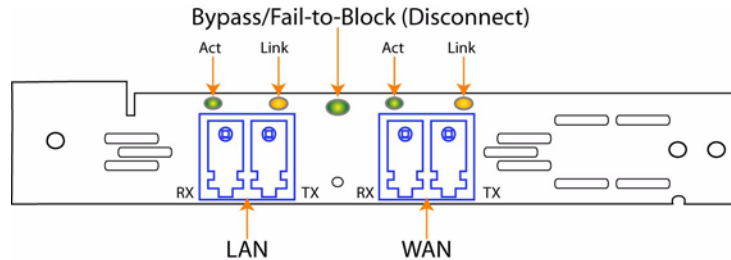
## Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E Card

The following section describes the Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E (Two-Port LR Single Mode Fiber 10 GigE PCI-E) card (410-00301-01) status lights.

**Important:** RiOS software v6.0.2 or later is required to run the Two-Port LR Single Mode Fiber 10 GigE PCI-E card.

**Figure B-21.** Interceptor software v2.0.4 or later is required to run the Two-Port LR Single Mode Fiber 10 GigE PCI-E card on Interceptor 9350 platforms.

**Figure 4-3.** Two-Port LR Single Mode Fiber 10 GigE PCI-E Card



The interface names for the NICs in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

For example, if a four-port NIC is located in slot 1 of your system, the interface names are lan1\_0, wan1\_0, lan1\_1, and wan1\_1, respectively.

**Important:** In a 1U appliance the LAN and WAN ports are numbered in ascending order (0, 1, 2, etc.) from left to right.

**Important:** In a 3U appliance the LAN and WAN ports are numbered in ascending order (0, 1, 2, etc.) from bottom to top.

## Technical Specifications

The following table summarizes the physical and power specifications for the latest hardware platform for the Steelhead appliance.

Series	Power Amps	VA (max)	BTU	HDD	Data Store	Dimensions (LxWxH)	Weight (without packaging)	Voltage	Power Supply	PCI Slots	Bypass Ports/ Max # Ports
250*	62.5 W	62.5	213 BTU	120 GB	40 GB	12 x 7.1 x 1.65 in	4.12 lb. 2.15 kg	100-127V, 200-240V	Single 100 W Internal	2	2/2
Desktop L-M-H 32-bit	.514 A					304.8 x 180.3 x 42 mm			100-240Vac, 50/60Hz, 2-1 A		
550*	66.5 W	66.5	227 BTU	160 GB	80 GB	1.65 x 7.1 x 12 in	4.12 lb. 2.15 kg	100-127V, 200-240V	Single 100 W Internal	2	2/2
Desktop M-H 32-bit	.541 A					4.2 x 18.0 x 30.5 cm			100-240Vac, 50/60Hz, 2-1 A		



Series	Power Amps	VA (max)	BTU	HDD	Data Store	Dimensions (LxWxH)	Weight (without packaging)	Voltage	Power Supply	PCI Slots	Bypass Ports/ Max # Ports
1050 1U U- L-M-H 64-bit	138-151 W  1.24- 1.35 A	145- 153	471- 515  BTU	250-500 GB  1-2 Hot Swappa ble Disks	100-200 GB	25.4 x 17.2 x 1.71 in  645.4 x 436 x 43.5 mm	29 lbs / 13.1 kg  H=30 lbs / 13.6 kg	100-127V, 200-240V	1+1 Redun- dant 660 W  100-127Vac/ 8A, 50/60Hz  200-240Vac/ 4A, 50/60Hz  -48Vdc, 8A	2	4/8
2050 1U L-M-H 64-bit	197 W  1.8 A	212	672 BTU	1 TB 4 Hot Swappa ble Disks	400 GB	25.4 x 17.2 x 1.71 in  645.4 x 436 x 43.5 mm	31.1 lb. 14.1 kg	100-127V, 200-240V	1+1 Redun- dant 660 W  100-127Vac/ 8A, 50/60Hz  200-240Vac/ 4A, 50/60Hz  -48Vdc, 8A	2	4/8
5050 3U L-M-H 64-bit	203-225 W  2.73- 3.15 A	325- 335	693- 768 BTU	2-3 TB 8-12 Hot Swappa ble Disks	600-800 GB	25.72 x 17.0 x 5.2 in  653.4 x 431.6 x 131.9 mm	59 lbs / 26.7 kg  H= 64 lbs/ 29 kg	100-127V, 200-240V	1+1 Redun- dant 770 W  100-127Vac/ 8A, 50/60Hz  200-240Vac/ 4A, 50/60Hz  -48Vdc, 8A	4	20
6050 3U 64-bit	352 W  4.9 A	452	1670 BTU	8 TB 16 Hot Swappa ble Disks	3.5 TB	25.72 x 17.0 x 5.2 in  653.4 x 431.6 x 131.9 mm	71 lbs / 32.2 kg	100-127V, 200-240V	1+1 Redun- dant 770 W  100-127Vac/ 8A, 50/60Hz  200-240Vac/ 4A, 50/60Hz  -48Vdc, 8A	4	20
7050 3U L-M 64-bit	425-430 W  4.2 A	455	1455- 1470 BTU	2.8-5.0 TB  2x 300GB 2.5" HDD  14--28x 160GB 2.5" SSD	2.2-4.4 TB	25.72 x 17.0 x 5.2 in  653.4 x 431.6 x 131.9 mm	55 lbs / 25 kg  M=59 lbs/ 25.8 kg	100-127V, 200-240V	1+1 Redun- dant 770 W  100-127Vac/ 8A, 50/60Hz  200-240Vac/ 4A, 50/60Hz  -48Vdc - - 60Vdc, 12A	4	20

\*Models 250 and 550 do not support 64-bit VMs. The 64-bit guest VMs (such as, Windows Server 2008 R2) are not supported on the 250 and 550 because these models do not incorporate VT support.

---

**Note:** Some values, such as the hard disk size, vary according to the configuration option you have ordered. The table lists the range of these values from lowest to highest.

---



---

**Note:** Depth does not include bezel on 1U and 3U (approximately 1 inch or 2.5 cm).

---

## Environmental Specifications

The following table summarizes the environmental requirements for the Steelhead appliance.

Model	Temperature (Operating)	Temperature (Storage)	Relative Humidity	Storage Humidity	Operating Altitude
250, 550	0° - 45° C 32° - 113° F	-40° - 65° C -40° - 149° F	20% - 80% non-condensing	5% - 95% non-condensing	Up to 10,000 ft.
1050, 2050, 5050, 6050, 7050	10° - 40°C 50° - 95°F	-40° - 65° C -40° - 149° F	20% - 80% non-condensing	5% - 95% non-condensing	Up to 10,000 ft.

## APPENDIX C Series xx20 Status Lights and Ports, Technical Specifications

This appendix describes the status lights and ports, and the technical and environmental specifications. It includes the following sections:

- [“1U Series xx20 Rev-A and Rev-B Status Lights and Ports” on page 83](#)
- [“Series xx20 Bypass Cards Status Lights” on page 86](#)
- [“Technical Specifications” on page 93](#)
- [“Environmental Specifications” on page 94](#)

---

**Important:** RiOS v7.0 is not supported on the Series xx20 platforms.

---

### 1U Series xx20 Rev-A and Rev-B Status Lights and Ports

This section describes the status lights and ports for the Model xx20 Rev-A and Rev-B platform.

#### Model 520, 1020, 1520, 2020 Rev-A

The following figure illustrates the Models 520, 1020, 1520, and 2020 Rev-A.

**Figure C-1. Front Panel**

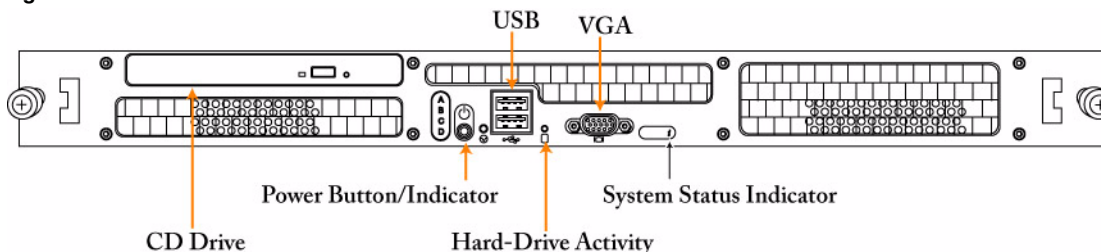
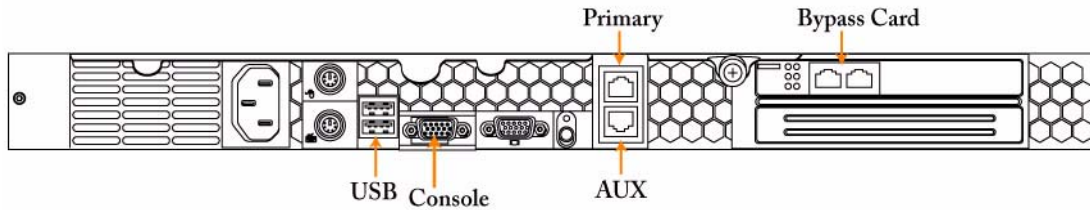


Figure C-2. Back Panel




---

**Important:** RiOS v7.0 is not supported on the Series xx20 platforms.

---

## Model 520, 1020, 1520, 2020 Rev-B Status Lights and Ports

The following figure illustrates the Models 520, 1020, 1520, and 2020 Rev-B.

Figure C-3. Front Panel Rev-B

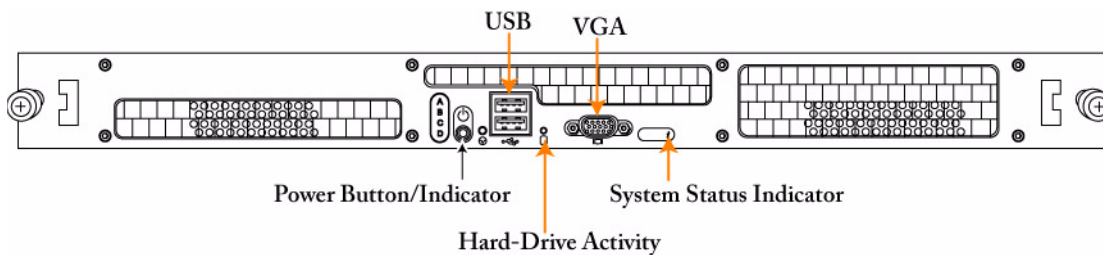
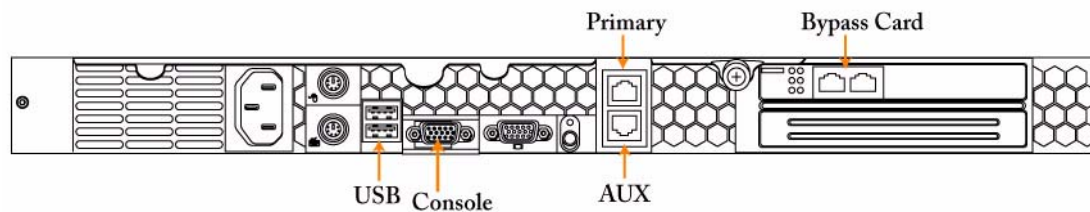


Figure C-4. Back Panel Rev-B



The following table summarizes the LED descriptions for the Model 520, 1020, 1520, and 2020 Rev-A and Rev-B.

LED Indicator	Description
Blue/amber system status indicator	<p>The blue system status indicator lights up during normal system operation. To stop the indicator from blinking, click the system status indicator button on the front or back panel.</p> <p>The amber system status indicator flashes when the system needs attention due to a system problem.</p>
Hard-drive indicator	<p>The green hard-drive activity indicator flashes when the hard drives are in use.</p>

LED Indicator	Description
NIC1 and NIC2 link indicators	The indicators for the two integrated network adapters light if the network adapters are connected to the network.
Power indicator	The green indicator in the center of the power button flashes if AC power is available to the system, but the system is not powered on. The green indicator is on when the system is powered on. If the system is not connected to AC power, the green indicator is off.

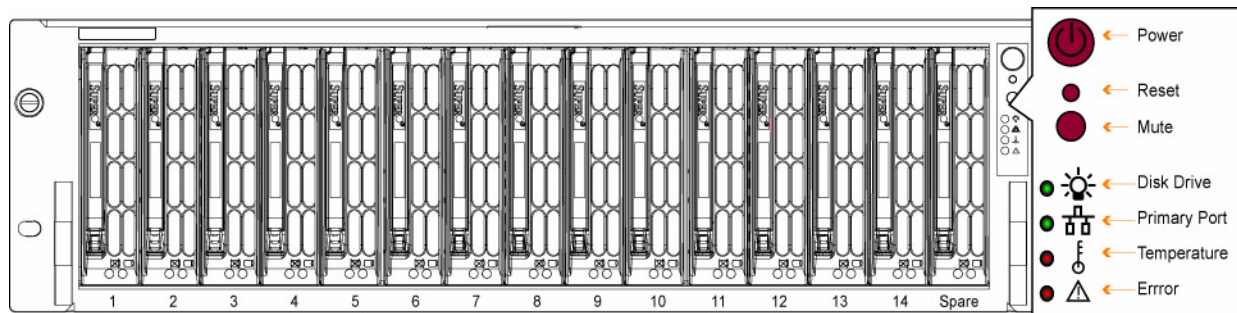
**Caution:** The Model 520, 1020, 1520, and 2020 is not intended for use at workplaces with visual display units in accordance with Part 2 of the Ordinance for Workplaces with Visual Display Units.

**Important:** RiOS v7.0 is not supported on the Series xx20 platforms.

### 3U Series xx20 Status Lights and Ports

The following figure illustrates the Models 3020, 3520, 5520, 6020, and 6120.

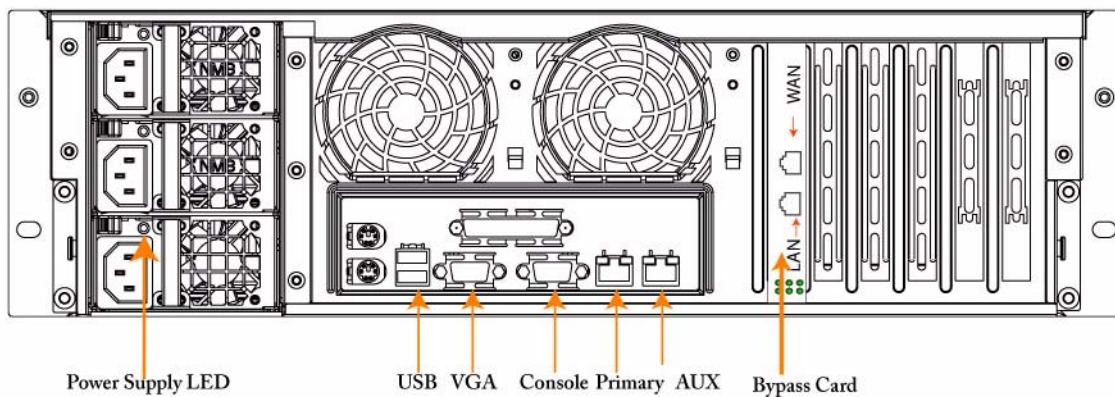
**Figure 4-4. Front Panel**



The following table summarizes the LED descriptions for the Model 3020, 3520, 5520, 6020, and 6120

LED Button	Color	Condition	Description
Power	Green	ON	System On
		OFF	System Off
Hard Disk Drive	Amber	FLASHING	Hard Disk Drive Activity
		OFF	No Activity
Network	Green	ON	Linked
		FLASHING	LAN Activity
		OFF	Disconnected
Overheat	Red	ON	System Overheat
		OFF	System Normal
Error	Red	ON	One or more power module failures
		OFF	System Normal

Figure C-5. Back Panel



## Series xx20 Bypass Cards Status Lights

The following section describes the status lights for the bypass cards supported on Series xx20 platforms. It includes the following sections:

- [“Bypass Card Manufacturing Numbers Series xx20” on page 87](#)
- [“Two-Port Copper Fast-Ethernet PCI-X Card” on page 87](#)
- [“Two-Port Copper Gigabit-Ethernet PCI-X Card-A” on page 88](#)
- [“Two-Port Copper Gigabit-Ethernet PCI-X Card-B” on page 89](#)
- [“Four-Port Copper Gigabit-Ethernet PCI-X Card” on page 90](#)
- [“Six-Port Copper Gigabit-Ethernet PCI-X Card” on page 91](#)
- [“Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card” on page 91](#)
- [“Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card” on page 92](#)

## Bypass Card Manufacturing Numbers Series xx20

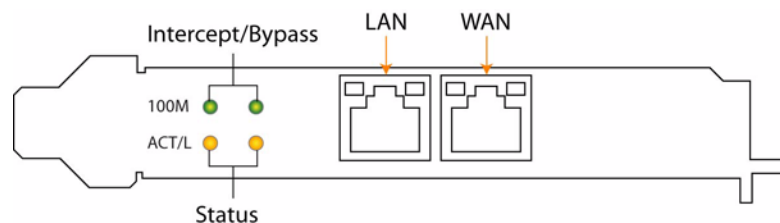
The following section describes the bypass card manufacturing part numbers. To determine the manufacturing part number for your bypass card, run the **show hardware** command in the CLI.

Description	Old Manufacturing Part #	New Manufacturing Part #	Orderable Part #
Two-Port Copper Fast-Ethernet PCI-X Card	CMP-00005	150-00001	Only on existing models
Two-Port Copper Gigabit-Ethernet PCI-X Card-A	CMP-00053	150-00004	CMP-NIC-2TX0
Two-Port Copper Gigabit-Ethernet PCI-X Card-B	CMP-00028	150-00002	CMP-NIC-2TX1
Four-Port Copper Gigabit-Ethernet PCI-X Card	CMP-00074	150-00006	CMP-NIC-4TX0
Six-Port Copper Gigabit-Ethernet PCI-X Card	N/A	150-00011	CMP-NIC-6TX0
Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card	CMP-00062	150-00062	CMP-NIC-2SX0
Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card	CMP-00135	150-00010	CMP-NIC-4SX0

## Two-Port Copper Fast-Ethernet PCI-X Card

The following section describes the Two-Port Copper Fast-Ethernet PCI-X card (150-00001) status lights.

**Figure C-6. Two-Port Copper Fast-Ethernet PCI-X Card**



The following table describes the Two-Port Copper Fast-Ethernet PCI-X card status lights. The status lights on the left correspond to the LAN link; the lights on the right correspond to the WAN link.

LED	Status	Description
<b>Intercept/Bypass (Activity)</b>	FLASHING (GREEN)	Data Transmission is Active
	SOLID (YELLOW)	LAN-WAN Link
	DARK (OFF)	LAN-WAN Disconnect
<b>Status (10/100)</b>	FLASHING (YELLOW)	Bypass is Active
	SOLID (YELLOW)	100-Mbps
	DARK (OFF)	10-Mbps

### To validate a Two-Port Copper Fast-Ethernet PCI-X Card (150-00001)

For the Two-Port Copper Fast-Ethernet PCI-X card (150-00001), the links are indicated by four status lights:

- The bottom two amber lights indicate the card is not in bypass mode.
- The top two green LEDs are lit if there is link.
- The top two green LEDs flash if there is traffic flowing through them.

Removing the cable from the ports causes the green LEDs to turn dark (off). You must induce traffic to ensure that the card is working correctly.

### To induce traffic, enter the following text at the system prompt

```
ping -c 1 -I <inpath_ipaddr> -b <broadcast_ip_addr>
```

For example, (where the netmask is /24):

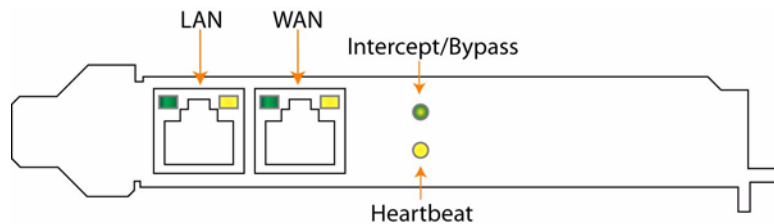
```
ping -c 1 -I 10.11.128.8 -b 10.11.128.255
```

This **ping** command creates a loop for testing the Steelhead appliance in isolation.

## Two-Port Copper Gigabit-Ethernet PCI-X Card-A

The following section describes the Two-Port Copper Gigabit-Ethernet PCI-X (Two-Port Copper GigE PCI-X) Card-A (150-00004) status lights.

Figure C-7. Two-Port Copper GigE PCI-X Card-A



The following table describes the Two-Port Copper GigE PCI-X card-A status lights.

Status Lights	Signal	Description
<b>Intercept/Bypass</b>	SOLID	Normal State
	OFF	Bypass or Power Off
<b>Status</b>	ON	Heartbeat Time Out
	FLASHING	Heartbeat Running
	OFF	Heartbeat Disabled

The following table describes the Two-Port Copper GigE PCI-X card-A, Light-Emitting Diode (LED) lights.

Status	Left LED	Right LED
<b>Network Link Not Established</b>	OFF	OFF
<b>10-Mbps (10 Base T)</b>	<b>Link</b>	OFF
	<b>Active</b>	FLASHING



Status		Left LED	Right LED
<b>100-Mbps (100 Base T)</b>	<b>Link</b>	SOLID	OFF
	<b>Active</b>	FLASHING	OFF
<b>1000-Mbps (1000 Base T)</b>	<b>Link</b>	FLASHING	SOLID
	<b>Active</b>	FLASHING	FLASHING

### To validate a Two-Port Copper Gigabit-Ethernet PCI-X Card (150-00004)

For the Two-Port Copper Gigabit-Ethernet PCI-X card (150-00004), the links are indicated by the following status lights:

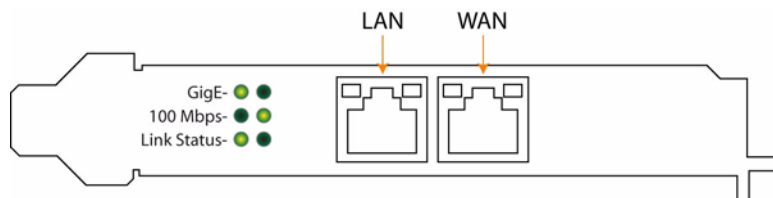
- Flashing green LEDs on the ports.
- Heartbeat LED to the right of ports is lit and flashing amber.
- Intercept/Bypass LED is solid.

Removing the cable when the card has a link causes the green LEDs on the ports to stop flashing.

## Two-Port Copper Gigabit-Ethernet PCI-X Card-B

The following section describes the Two-Port Copper Gigabit-Ethernet PCI-X (Two-Port Copper GigE PCI-X) Card-B (150-00002) status lights.

**Figure C-8. Two-Port Copper Gigabit-Ethernet PCI-X Card-B**



The following table describes the Two-Port Copper GigE PCI-X Card-B, status lights.

Status Lights	Signal	Description
<b>Intercept/Bypass</b>	SOLID (GREEN)	Normal State
<b>Heartbeat</b>	OFF	Bypass or Power Off

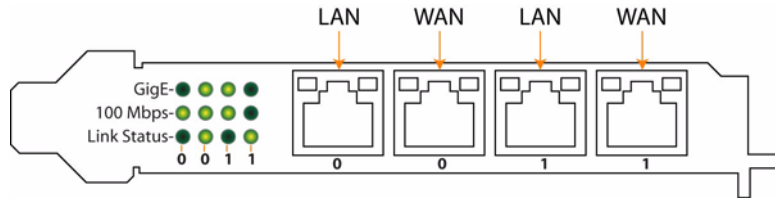
The following table describes the Two-Port Copper GigE PCI-X Card-B, LED lights.

Status	Left LED (Solid Green)	Right LED (Solid Yellow)
<b>Link</b>	ACTIVE	LINK
<b>Network Link Not Established</b>	OFF	OFF

## Four-Port Copper Gigabit-Ethernet PCI-X Card

The following section describes the Four-Port Copper Gigabit-Ethernet PCI-X (Four-Port Copper GigE PCI-X) card (150-00006) status lights.

**Figure C-9. Four-Port Copper GigE PCI-X Card**



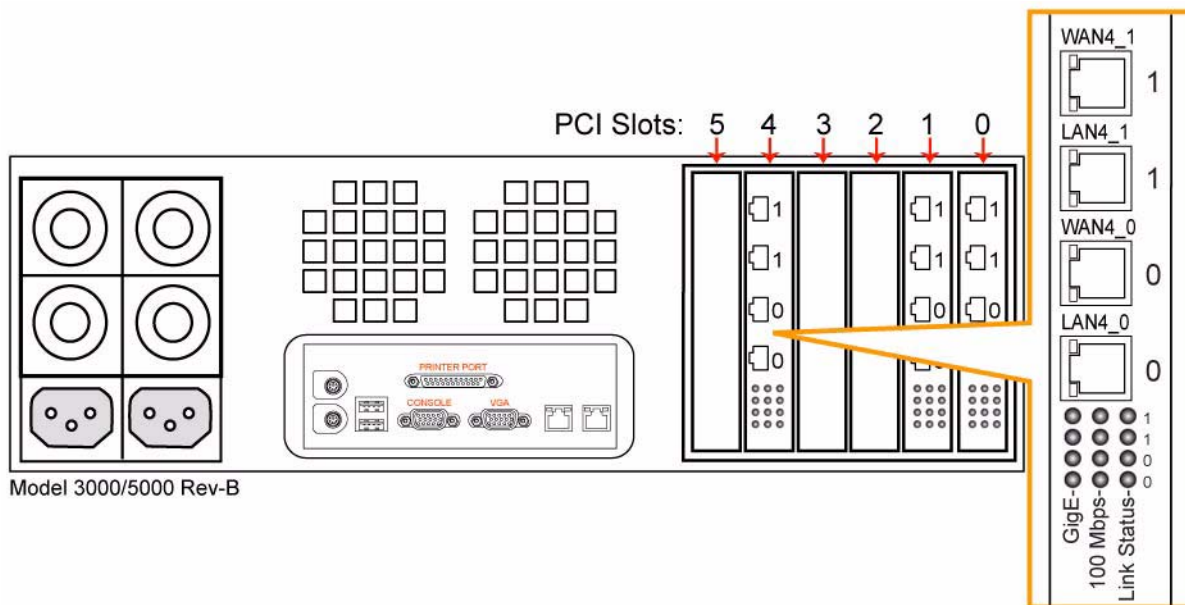
The following table describes the Four-Port Copper GigE PCI-X card status and LED lights.

	Interface In-Path 0	Interface In-Path 1	Bypass
<b>Gig-E 1000-Mbps (1000 Base T)</b>	SOLID	SOLID	SOLID
<b>100-Mbps (100 Base T)</b>	SOLID	SOLID	SOLID
<b>Network Link</b>	SOLID	SOLID	OFF

The interface names for the bypass cards in the Steelhead Management Console and the CLI are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<slot>\_<pair>).

For example, if a four-port bypass card is located in slot 4 of your system, the interface names are lan4\_0, wan4\_0, lan4\_1, and wan4\_1, respectively.

**Figure C-10. Model 3000 Rev-B Appliance Populated by Four-Port Copper Gigabit-Ethernet PCI-X Cards**

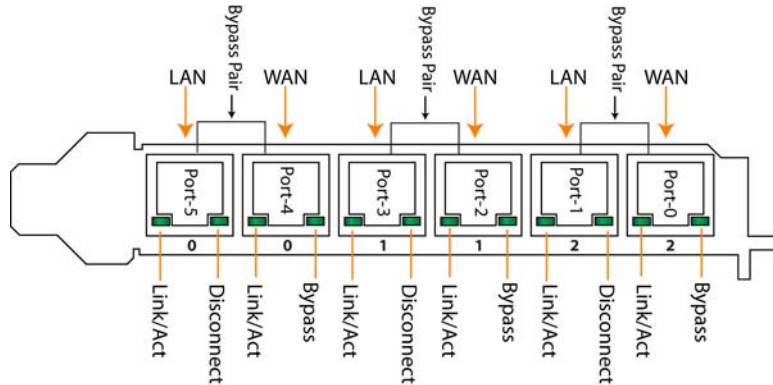


Model 3000/5000 Rev-B

## Six-Port Copper Gigabit-Ethernet PCI-X Card

The following section describes the Six-Port Copper Gigabit-Ethernet PCI-X (Six-Port Copper GigE PCI-X) card (150-00011) status lights. The Six-Port Copper GigE PCI-X card has full fail-to-block support.

**Figure C-11. Six-Port Copper GigE PCI-X Card**



The following table describes the Six-Port Copper GigE PCI-X card status and LED lights.

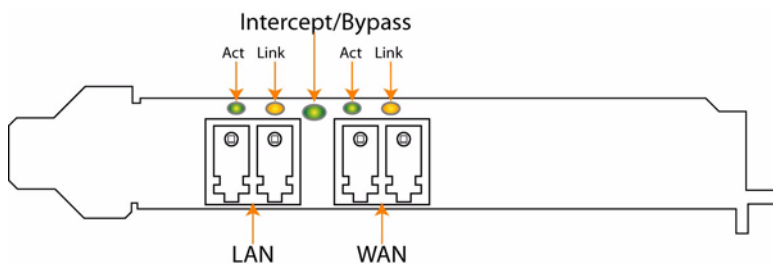
LED	Condition
Link / Act	Solid green on link, blinks on activity.
Bypass	Solid green when in bypass mode.
Disconnect	Solid green in disconnect mode.

The interface names for the bypass cards are a combination of the slot number and the port pairs (lan<slot>\_<pair>, wan<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.

## Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card

The following section describes the Two-Port SX Multimode Fiber Gigabit-Ethernet PCI-X (Two-Port SX Multimode Fiber GigE PCI-X) card (150-00062) status lights.

**Figure C-12. Two-Port SX Multimode Fiber GigE PCI-X Card**

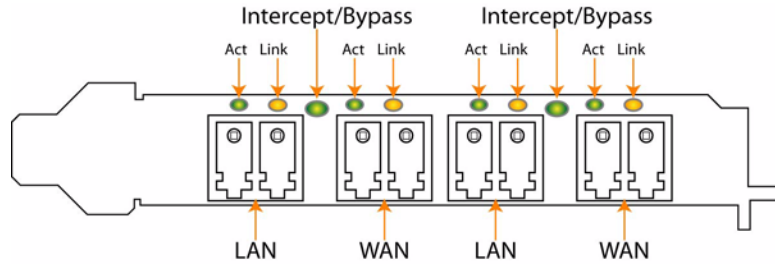


The Bypass LED is ON (Green) if the Two-Port SX Multimode Fiber GigE PCI-X card is in bypass mode; it is OFF if the bypass card is in normal mode.

## Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card

The following section describes the Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X (Four-Port SX Multimode Fiber GigE PCI-X) card (150-00010) status lights.

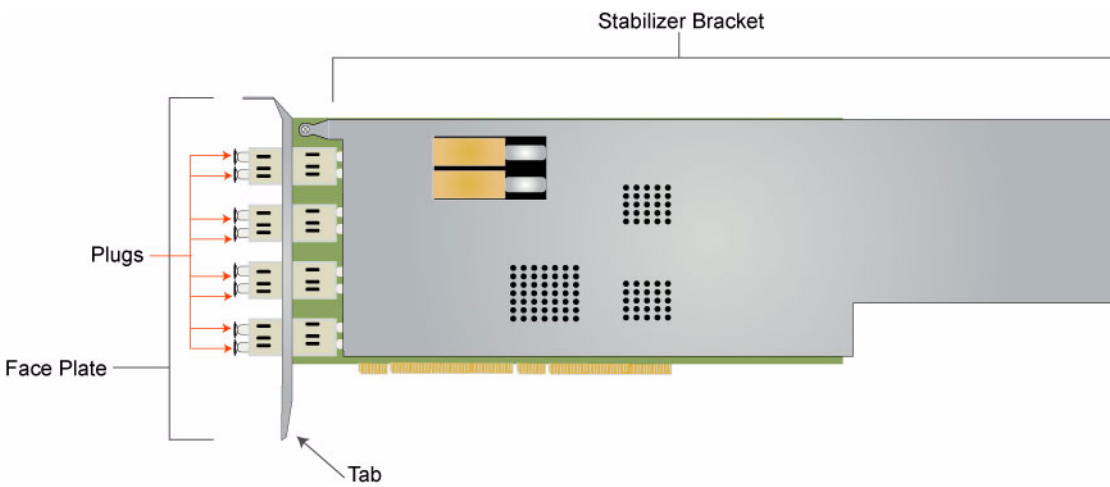
**Figure C-13. Four-Port SX Multimode Fiber GigE PCI-X Card**



The Bypass LED is ON (Green) if the Four-Port Copper GigE PCI-X card is in bypass mode; it is OFF if the bypass card is in normal mode.

The Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X card ships with a stabilizer bracket to ensure that the proper and secure seating of the bypass card.

**Figure C-14. Four-Port SX Multimode Fiber Gigabit-Ethernet PCI-X Card with Stabilizer Bracket**



## Technical Specifications

The following table summarizes the physical and power specifications for the x20, and xx20 (Rev-A and Rev-B, where applicable) Steelhead appliances.

Model	Volts Amperes (V*A)	Power (W)	Amperes (A)	Power Factor (W/VA)	BTU	Hard Disk	Data Store	Height, Width, and Depth	Weight	Voltage and Frequency	PSU
520* (1U) Rev-A	207	206 W	1.76 A	0.99	646 BTU	1 x 250 GB	80 GB	1.69 x 17.6 x 21.5 in 4.27 x 44.7 x 54.61 cm	26 lb. 12 kg	100-240 V 50-60 Hz	Single 345 W
Rev-B	151	149 W	1.28 A	0.98	508 BTU						
1020* (1U) Rev-A	207	206 W	1.76 A	0.99	646 BTU	1 x 250 GB	80 GB	1.69 x 17.6 x 21.5 in 4.27 x 44.7 x 54.61 cm	26 lb. 12 kg	100-240 V 50-60 Hz	Single 345 W
Rev-B	151	149 W	1.28 A	0.98	508 BTU						
1520* (1U) Rev-A	207	206 W	1.76 A	0.99	646 BTU	1 x 250 GB	80 GB	1.69 x 17.6 x 21.5 in 4.27 x 44.7 x 54.61 cm	26 lb. 12 kg	100-240 V 50-60 Hz	Single 345 W
Rev-B	151	149 W	1.28 A	0.98	508 BTU						
2020* (1U) Rev-A	207	206 W	1.76 A	0.99	646 BTU	2 x 250 GB SATA + 1 spare	150 GB	1.69 x 17.6 x 21.5 in 4.27 x 44.7 x 54.61 cm	26 lb. 12 kg	100-240 V 50-60 Hz	Single 345 W
Rev-B	151	149 W	1.28 A	0.98	508 BTU						
3020 (3U)	435	425 W	3.7 A	0.97	1450 BTU	4 x 250 GB SATA + 1 spare	250 GB	5.2 x 17.7 x 25.5 in 13.2 x 45 x 64.7 cm	89 lb. 40 kg	100-240 V 50-60 Hz	Triple 760 W
3520 (3U)	435	425 W	3.7 A	0.97	1450 BTU	6 x 250 GB SATA + 1 spare	500 GB	5.2 x 17.7 x 25.5 in 13.2 x 45 x 64.7 cm	92 lb. 42 kg	100-240 V 50-60 Hz	Triple 760 W
5520 (3U)	435	425 W	3.7 A	0.97	1450 BTU	6 x 250 GB SATA + 1 spare	700 GB	5.2 x 17.7 x 25.5 in 13.2 x 45 x 64.7 cm	92 lb. 42 kg	100-240 V 50-60 Hz	Triple 760 W

Model	Volts Amperes (V*A)	Power (W)	Amperes (A)	Power Factor (W/VA)	BTU	Hard Disk	Data Store	Height, Width, and Depth	Weight	Voltage and Frequency	PSU
6020 (3U)	435	425 W	3.7 A	0.97	1450 BTU	8 x 400 GB (8 x 400 GB SATA + 1 spare	1.4 TB	5.2 x 17.7 x 25.5 in 13.2 x 45 x 64.7 cm	95 lb. 43 kg	100-240 V 50-60 Hz	Triple 760 W
6120 (3U)	520	505 W	4.4 A	0.97	1723 BTU	14 x 500 GB 14 x 500 GB SATA + 1 spare	3.2 TB	5.2 x 17.7 x 25.5 in 13.2 x 45 x 64.7 cm	105 lb. 47 kg	100-240 V 50-60 Hz	Triple 760 W

\*1U xx20s do not support 64-bit VMs. The 64-bit guest VMs (such as, Windows Server 2008 R2) are not supported on the 1U xx20s (even though they are 64-bit systems) because these models do not incorporate VT support.

## Environmental Specifications

The following table summarizes the environmental requirements for the Steelhead appliance.

Model	Temperature (Operating)	Temperature (Storage)	Relative Humidity	Storage Humidity	Operating Altitude
520, 1020, 1520, 2020,	10° - 35°C 50° - 95°F	-40° - 65°C -40° - 149°F	20% - 80% non-condensing	5% - 95% non-condensing	Up to 10,000 ft.
3020, 3520, 5520,	10° - 35°C 50° - 95°F	-40° - 70°C -40° - 158°F	20% - 80% non-condensing	5% - 95% non-condensing	Up to 10,000 ft.

# Index

## Numerics

- 1050, 2050, status lights and ports 66
- 5050, 6050, status lights and ports 68
- 7050, status lights and ports 70

## A

- AC power, connecting 29
- Appliance
  - connecting to 30
  - installing 23, 45
  - powering on 29
- Appliance ports, definitions of 28
- Application Streamlining, overview of viii
- Auto-Discovery process, overview of viii
- Auto-discovery rule, overview of x
- Auto-discovery, enhanced, overview of ix
- Auxiliary port, definition of 28

## B

- Blocked traffic in bypass mode 55
- Boot failure 55
- Bypass cards
  - errors on 55
  - interface naming convention 28, 74
  - status lights xx50 71
- Bypass mode
  - troubleshooting 55
  - troubleshooting for 55
- Bypass mode, definition of x

## C

- Client-side appliance, configuring 43
- CMC compatibility 9
- CMC, overview of viii
- Configuration information, required 26
- configuration jump-start command, restarting the wizard 32
- Configuration wizard
  - about 31
  - restarting 32
- Configuration, verifying 36, 39
- Connecting
  - LAN switch to LAN port, illustration of 35
  - Primary port to LAN switch, illustration of 35, 43
  - WAN port to WAN router, illustration of 36
- Console port, definition of 28

- CX1555, status lights and ports 62
- CX555, CX755, status lights and ports 60

## D

- Data Streamlining, overview of vii
- Deny rules, overview of x
- Discard rules, overview of x
- Documentation, contacting 13
- Duplex and speed, checking your settings 40

## E

- Environmental specifications
  - CX Series xx55 64
  - Series xx20 94
  - Series xx50 82
- Error 4294967295 55
- Ethernet network compatibility 10

## F

- Fail-to-block mode
  - overview of xi
- Failure modes
  - fail-to-block, overview of xi
- Fixed-target rules, overview of x
- Flexible licensing 16
- Four-Port Copper Gig-E Bypass card
  - illustration of 90
  - status lights 90

## I

- In-Path rules, overview of x
- In-path, configuring 31
- Interface naming convention 28, 74

## K

- Known issues 12

## L

- LAN port, definition of 28
- LAN switch, connecting 35
- Logical in-path WCCP deployment, diagram of 24
- Login page 38

## M

- Management Streamlining, overview of viii
- Models 1020, 1520, 2020, no 64-bit VM support 10, 94

Models 250 and 550, no 64-bit VM support 10

## N

Network, connecting to 35  
NIC cards  
  Series xx20 87  
NIC cards, status lights xx50 71  
NIC manufacturing part numbers, xx20 87

## O

Online documentation 12  
Online notes 12  
Out-of-path deployment, diagram of 25  
Out-of-path, configuring 40

## P

Pass-through rules, overview of x  
Peering rules, overview of x  
Physical in-path deployment, diagram of 24  
Physical in-path, overview of 24  
Ports, definitions of 28  
Power specifications, detailed CX1555 64  
Preparing your site 26  
Primary port, connecting 35  
Primary port, definition of 28  
Product inventory 25  
Professional services, contacting 13

## R

Release notes 12  
Required equipment 26

## S

Safety guidelines 12  
Scalable Data Referencing, overview of vii  
SDR, overview of vii  
Series xx20, bypass cards 87  
Six-Port Copper Gigabit-Ethernet PCI-X card, illustration of 91  
SNMP compatibility 11  
Specification license 16  
Speed and duplex, checking your settings 40  
Status lights  
  Four-Port Gig-E Bypass card 90  
  Two-Port Fast-Ethernet Bypass Card 87  
  Two-Port Fiber Gig-E Bypass card 91, 92  
  Two-Port Gig-E Bypass card-B 89  
Status lights and ports  
  1050, 2050 66  
  250, 550 65  
  5050, 7050 68  
  7050 70  
  CX1555 62  
  CX555, CX755 60  
Steelhead Mobile Controller, overview of viii  
System LEDs  
  250, 550 66  
  CX1555 62  
  CX555, CX755 60

## T

Technical specifications

CX1555 64  
CX555, CX755 63  
Series xx20 93  
Series xx50 80  
Technical support, contacting 13  
Traffic, blocked in bypass mode 55  
Transport Streamlining, overview of viii  
Two-Port Copper Fast-Ethernet PCI-X card (150-00001) status lights 87  
Two-Port Copper Gigabit-Ethernet PCI-X (Two-Port Copper GigE PCI-X) Card-A (150-00004) status light 88  
Two-Port Fast-Ethernet Bypass Card, illustration of 87  
Two-Port Fast-Ethernet Bypass card, illustration of 87  
Two-Port Fiber Gig-E Bypass card, illustration of 91, 92  
Two-Port Gig-E Bypass card-A status lights 88  
Two-Port Gig-E Bypass card-B, illustration of 89

## U

Upgrade possibilities 16

## V

Virtual in-path deployments, overview of 24  
VMs, no 64-bit support 10, 94

## W

WAN port, connecting 36  
WAN port, definition of 28  
WAN router, disconnecting 35  
Wizard, about 31  
Wizard, restarting 32