

# **Riverbed Services Platform Installation and Configuration Guide**

RiOS Version 5.5.4

September 2009

**riverbed**<sup>®</sup>

**Think fast.**<sup>™</sup>

© 2003-2009 Riverbed Technology, Incorporated. All rights reserved.

Riverbed Technology, Riverbed, Steelhead, RiOS, Interceptor and the Riverbed logo are trademarks or registered trademarks of Riverbed Technology, Inc. All other trademarks used or mentioned herein belong to their respective owners.

Linux is a trademark of Linus Torvalds in the United States and in other countries. VMware is a trademark of VMware, Incorporated. Oracle and JInitiator are trademarks or registered trademarks of Oracle Corporation. Microsoft, Windows, Windows NT, Windows 2000, Windows Vista, Outlook, and Internet Explorer are trademarks or registered trademarks of Microsoft 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.

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.

NET-SNMP © Copyright 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

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. This product is derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

For detailed copyright and license agreements or modified source code (where required), see the Riverbed Technical 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 Technical Support at <https://support.riverbed.com>. You must log in to the support site to request modified source code.

Other product names, brand names, marks, and symbols are registered trademarks or trademarks of their respective owners. The content of this manual is furnished on a RESTRICTED basis and is subject to change without notice and should not be construed as a commitment by Riverbed Technology, Incorporated. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in Subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable. Riverbed Technology, Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in this book.



Riverbed Technology  
199 Fremont Street  
San Francisco, CA 94105

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

Part Number  
712-00032-05

# Contents

<b>Contents .....</b>	<b>iii</b>
<b>Introduction.....</b>	<b>5</b>
About This Guide .....	5
Types of Users .....	5
Organization of This Guide.....	5
Document Conventions .....	6
Product Dependencies and Compatibility.....	6
Additional Resources .....	7
Online Notes.....	8
Riverbed Documentation .....	8
Online Documentation .....	8
Riverbed Support Knowledge Base .....	8
Related Reading.....	8
Contacting Riverbed.....	9
Internet .....	9
Technical Support .....	9
Professional Services .....	9
Documentation.....	9
<b>Chapter 1 - Overview of RSP .....</b>	<b>11</b>
Overview of RSP .....	11
RSP Packages.....	13
Virtual Network Interfaces.....	15
VNI Rules.....	16
RSP Watchdog .....	17
New RSP Features in RiOS Version 5.5.4.....	18
Next Steps .....	18
<b>Chapter 2 - Installing and Configuring RSP Using the Management Console .....</b>	<b>19</b>
Basic Steps for Installing and Configuring RSP .....	19
Prerequisites and Tips .....	20
Installing a Package in a Slot.....	23
Enabling a Slot .....	24
Disabling a Slot .....	24
Viewing Slot Status.....	25

Configuring RSP Data Flow .....	26
Adding a VNI to the Data Flow .....	26
Adding Rules to an Optimization VNI .....	27
Bridging a Management VNI to an Interface .....	30
Performing RSP Tasks .....	31
Updating VLAN Settings .....	31
Configuring an RSP Watchdog .....	31
Configuring RSP Alarm Settings .....	32
Managing Virtual Machines .....	34
Opening a VM Console.....	34
Changing the Memory Footprint for a VM .....	34
Viewing RSP Statistics Reports .....	35
<b>Chapter 3 - Installing and Configuring RSP Using the CLI.....</b>	<b>37</b>
Basic Steps for Installing and Configuring RSP .....	37
Installing the RSP Installation Image.....	39
Prerequisites and Tips .....	39
Verifying RSP Requirements.....	39
Downloading the RSP Installation Image.....	40
Uploading the RSP Installation Image on the Steelhead Appliance.....	40
Starting RSP .....	41
Deleting the RSP installation Image File.....	41
Adding RSP Packages .....	42
Obtaining an RSP Package .....	42
Prerequisites and Tips .....	42
Downloading the RSP Package .....	43
Uploading the RSP Package on the Steelhead Appliance .....	43
Installing a Package Into a Slot.....	44
Enabling a Slot .....	44
Disabling a Slot .....	45
Setting Slot Priority .....	45
Renaming a Slot .....	45
Uninstalling an RSP Package From a Slot.....	46
Deleting an RSP Package Installation File .....	46
Renaming an RSP Package.....	46
Upgrading the RSP Image.....	47
Configuring an IP Address for an RSP Package .....	47
Configuring RSP Data Flow .....	48
Adding a VNI to the Data Flow .....	48
Adding a Rule to the VNI.....	49
Bridging a Management VNI to an Interface .....	50
Verifying VNI Statistics.....	51
Performing RSP Tasks .....	52
Updating VLAN Settings .....	52
Configuring an RSP Watchdog.....	53
Configuring Fail-to-Block for an Interface.....	54

Configuring Email Alerts .....	55
Using RSP Backups.....	56
Verifying Your RSP Backup Configuration.....	57
Managing Virtual Machines .....	57
Opening a VMware Console for an Installed VM .....	57
Changing the Memory Footprint for a VM .....	58
Verifying Your Configuration .....	58
<b>Chapter 4 - Using VMware Infrastructure Software.....</b>	<b>61</b>
Using VMware Infrastructure Software .....	61
Using the VMware Infrastructure Client (for Windows).....	61
Using VMware Infrastructure Web Access and Windows Client .....	62
<b>Chapter 5 - Creating an RSP Package for a Windows Server .....</b>	<b>63</b>
Installing the Windows Package.....	63
Overview of RSP Package Creation .....	64
Hardware and Software Dependencies.....	64
Basic Steps for Creating an RSP Package .....	65
Creating the Virtual Machine.....	66
Installing Windows Server on the Virtual Machine.....	69
Installing VMware Tools on the Virtual Machine .....	70
Configuring Services on the Virtual Machine .....	71
Reconfiguring the Virtual Machine for RSP.....	71
Enabling a Named-Pipe Serial Support .....	72
Converting the Virtual Machine into an RSP Package for a Windows Server.....	72
Troubleshooting Error Messages.....	78
<b>Acronyms and Abbreviations.....</b>	<b>79</b>
<b>Glossary .....</b>	<b>85</b>
<b>Index .....</b>	<b>91</b>



# Introduction

Welcome to the *Riverbed Services Platform Installation and Configuration Guide*. Read this introduction for an overview of the information provided in this guide and the documentation conventions used throughout, hardware and software dependencies, additional reading, and contact information. This introduction includes the following sections:

- [“About This Guide,”](#) next
- [“Product Dependencies and Compatibility”](#) on page 6
- [“Additional Resources”](#) on page 7
- [“Contacting Riverbed”](#) on page 9

---

## About This Guide

The *Riverbed Services Platform Installation and Configuration Guide* describes how to install and configure Riverbed Services Platform (RSP) on the Steelhead appliance using the Riverbed CLI.

## Types of Users

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

## Organization of This Guide

The *Riverbed Services Platform Installation and Configuration Guide* includes the following chapters:

- [Chapter 1, “Overview of RSP”](#) provides an overview of RSP.
- [Chapter 2, “Installing and Configuring RSP Using the Management Console”](#) describes how to install and configure RSP on the Steelhead appliance using the Riverbed Command-Line Interface.
- [Chapter 3, “Installing and Configuring RSP Using the CLI”](#) describes how to install and configure RSP on the Steelhead appliance using the Riverbed Command-Line Interface.
- [Chapter 4, “Using VMware Infrastructure Software”](#) describes how to manage virtual machines using VMware infrastructure software.

- [Chapter 5, “Creating an RSP Package for a Windows Server”](#) describes how to create an RSP package for the Steelhead appliance using the Riverbed Package Generator and VMware Server v2.0.

A list of acronyms and a glossary of terms follows the chapters. A comprehensive index directs you to areas of particular interest.

## Document Conventions

This manual uses the following standard set of typographical conventions to introduce new terms, 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, commands, keywords, identifiers (names of classes, objects, constants, events, functions, program variables), environment variables, filenames, GUI controls, and other similar terms appear in bold typeface.
Courier	Information displayed on your terminal screen and information that you are instructed to enter appears in Courier font.
< >	Within syntax descriptions, values that you specify appear in angle brackets. For example: <b>interface &lt;ipaddress&gt;</b>
[ ]	Within syntax descriptions, optional keywords or variables appear in brackets. For example: <b>ntp peer &lt;addr&gt; [version &lt;number&gt;]</b>
{ }	Within syntax descriptions, required keywords or variables appear in braces. For example: <b>{delete &lt;filename&gt;   upload &lt;filename&gt;}</b>
	Within syntax descriptions, the pipe symbol represents a choice to select one keyword or variable to the left or right of the symbol. (The keyword or variable can be either optional or required.) For example: <b>{delete &lt;filename&gt;   upload &lt;filename&gt;}</b>

## Product Dependencies and Compatibility

This section provides information about product dependencies and compatibility.

The following tables summarize the hardware and software requirements for RSP.

Riverbed Steelhead Appliance	Hardware and Software Requirements
Steelhead appliance	19 inch (483 mm) two or four-post rack. RSP is supported on Steelhead appliance models 250, 520, 550, 1020, 1050, 1520, 2020, 2050, 3020, 3520, 5050, and 6050.
Steelhead Management Console	Any computer that supports a Web browser with a color image display. The Management Console has been tested with Mozilla Firefox v1.5.x, v2.0.x, and Microsoft Internet Explorer v6.0.x, and v7.0. <b>Note:</b> Javascript and cookies must be enabled in your Web browser.



Riverbed CLI Hardware Requirements	Hardware and Software Requirements
<p>One of the following:</p> <ul style="list-style-type: none"> <li>An ASCII terminal or emulator that can connect to the serial console (9600 baud, 8 bits, no parity, 1 stop bit, and no flow control).</li> <li>A computer with a Secure Shell (<b>ssh</b>) client that is connected by an IP network to the appliance primary interface.</li> </ul>	<p>Secure Shell (<b>ssh</b>). Free <b>ssh</b> clients include PuTTY for Windows computers, OpenSSH for many Unix and Unix-like operating systems, and Cygwin.</p>

Riverbed Services Platform (RSP)	Hardware and Software Requirements
Operating System	RiOS v5.5.x
RSP Partition	<ul style="list-style-type: none"> <li>The required RSP partition size on the Steelhead appliance depends on the size of your RSP package and whether you are running other packages on the RSP partition.</li> <li>The RSP partition size varies among Steelhead appliance models. For details, see the Steelhead appliance specification sheets located at <a href="http://www.riverbed.com/products/appliances/">http://www.riverbed.com/products/appliances/</a>.</li> </ul>
Memory	2 GB additional memory on the Steelhead appliance is required for RSP. For details, see the <i>Upgrade and Maintenance Guide</i> .

**Note:** RSP requires RiOS software v5.5 or higher. To upgrade from a version prior to v5.5 to v5.5 with RSP, you must first upgrade to v4.1.7d, v4.1.8, v5.0.5b, v5.0.6 or later, and then upgrade to v5.5 with RSP.

For details about sizing your system for RSP, see the following Riverbed Knowledge Base article, *RSP Sizing Guidelines* located at <https://support.riverbed.com>.

For details about Steelhead appliance system specifications by model, see the Steelhead appliance specification sheets located at <http://www.riverbed.com/products/appliances/>.

## Additional Resources

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

- [“Online Notes,”](#) next
- [“Riverbed Documentation”](#) on page 8
- [“Online Documentation”](#) on page 8
- [“Riverbed Support Knowledge Base”](#) on page 8

- [“Related Reading” on page 8](#)

## Online Notes

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

Online File	Purpose
<code>&lt;product&gt;_&lt;version_number&gt;.pdf</code>	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.

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

## Riverbed Documentation

For a complete list of Riverbed documentation log in to the Riverbed Technical Support Web site located at <https://support.riverbed.com>.

The Riverbed user documentation set is periodically updated with new information. To access the most current version, log in to the Riverbed Technical Support site located at <https://support.riverbed.com>.

## Online Documentation

The Riverbed documentation set is periodically updated with new information. To access the most current version of Riverbed documentation and other technical information, consult the Riverbed Technical Support site located at <https://support.riverbed.com>.

## Riverbed Support Knowledge Base

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 key words and strings.

To access the Riverbed Knowledge Base, log in to the Riverbed Technical Support site located at <https://support.riverbed.com>.

## Related Reading

To learn more about network administration, consult the following books:

- *Microsoft Windows 2000 Server Administrator's Companion* by Charlie Russell and Sharon Crawford (Microsoft Press, 2000)
- *Common Internet File System (CIFS) Technical Reference* by the Storage Networking Industry Association (Storage Networking Industry Association, 2002)
- *TCP/IP Illustrated, Volume I, The Protocols* by W. R. Stevens (Addison-Wesley, 1994)
- *Internet Routing Architectures (2nd Edition)* by Bassam Halabi (Cisco Press, 2000)

---

## Contacting Riverbed

This section describes how to contact departments within Riverbed.

### Internet

You can find out 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 Technical Support or your channel partner who provides support. To contact Riverbed Technical Support, please open a trouble ticket at <https://support.riverbed.com> or call 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States.

### Professional Services

Riverbed has a staff of professionals who can help you with installation assistance, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services go to <http://www.riverbed.com> or email [proserve@riverbed.com](mailto:proserve@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 1 Overview of RSP

This chapter describes Riverbed Services Platform. This chapter includes the following sections:

- [“Overview of RSP,”](#) next
- [“RSP Packages”](#) on page 13
- [“Virtual Network Interfaces”](#) on page 15
- [“RSP Watchdog”](#) on page 17
- [“New RSP Features in RiOS Version 5.5.4”](#) on page 18
- [“Next Steps”](#) on page 18

This guide assumes that you installed and configured the Steelhead appliances. For detailed information about the Steelhead appliance, see the *Steelhead Appliance Installation and Configuration Guide*, *Steelhead Management Console User’s Guide*, and the *Steelhead Appliance Deployment Guide*.

---

**Note:** RSP requires RiOS software v5.5 or higher. To upgrade from a version prior to v5.5 to v5.5 with RSP, you must first upgrade to v4.1.7d, v4.1.8, v5.0.5b, v5.0.6 or later, and then upgrade to v5.5 with RSP.

---

---

**Tip:** Riverbed recommends you configure RSP using the Management Console. For detailed information, see the *Steelhead Management Console User’s Guide*.

---

---

## Overview of RSP

This section describes RSP, its components, and the process for deploying RSP.

In RiOS v5.5.x, RSP offers branch-office-in-a-box services with the following benefits:

- A VMware-based virtualization platform provides the benefits of the most commonly deployed and advanced virtualization tool set.
- Support for running up to five different additional services simultaneously on a single Steelhead appliance, depending on the service and Steelhead appliance model.

- Support for more services and types of services. These include in-band packages that sit in-line with optimization such as the Universal Threat Management (UTM) security services, proxy solutions such as video or network monitoring services, and improved support for out-of-band packages such as Windows Active Directory, DNS and DHCP management software, and print services.
- A comprehensive, integrated, user interface that provides granular control of RSP, including setup, reporting, and the definition of the data flow between services.

---

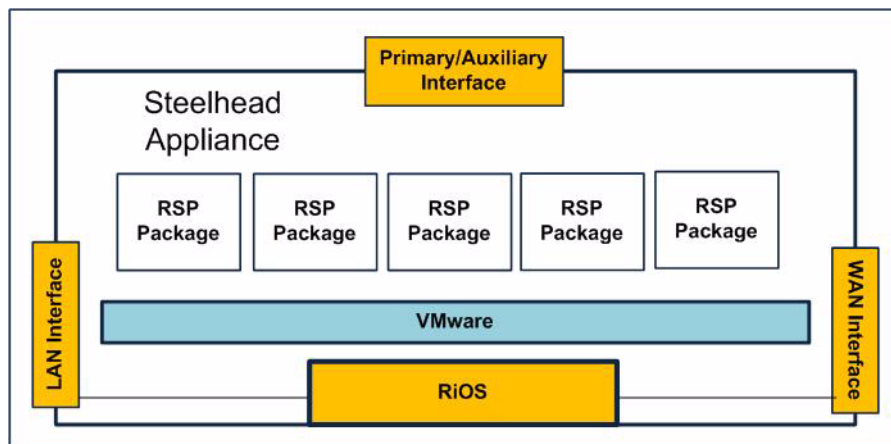
**Note:** RSP is supported on Steelhead appliance models 250, 520, 550, 1020, 1050, 1520, 2020, 2050, 3020, 3520, 5050, and 6050.

---

RSP in RiOS v5.5.x uses VMware Server v2.0 as the virtualization platform. Both 32 and 64-bit versions of the RSP installation image are available.

The following figure illustrates the RSP setup on the Steelhead appliance.

**Figure 1-1. The RSP Platform**



After installing the RSP installation image, you can add packages to run additional services and applications. RSP includes configuration options that enable you to determine the data flow to and from a package, and the ability to chain packages together.

RSP enables the following types of services:

- **Windows Print.** Provides local Windows print services.
- **Basic Branch Services.** Provides local services such as IP address management (IPAM) and package deployment tools.
- **Security.** Provides local security services for in-band packages that sit in-line with optimization, such as Universal Threat Management (UTM).
- **Microsoft Windows Active Directory Server.** Provides local Windows Active Directory service.
- **Proxy Solutions.** Provides services such as live or on-demand video, and HTTP Web proxies.
- **Networking Performance Monitoring.** Provides local network and application performance monitoring.

In addition to configuring RSP packages out-of-path on the primary interface (for example, out-of-path on the primary or auxiliary interface) RiOS v5.5.x also enables you to configure an RSP package in-path on the LAN- or WAN-side of the network.

---

## RSP Packages

Before installing the RSP package, you must install the RSP installation image and start the RSP service. For detail on installing the RSP installation image using the Management Console, see [“Installing the RSP Installation Image” on page 20](#). For details on installing the RSP installation image using the CLI, see [“Basic Steps for Installing and Configuring RSP” on page 37](#).

A package can be:

- a VM created by a third-party vendor that also contains configuration files specific to the RSP implementation.
- a VM created by Riverbed.
- a VM created internally within your organization.

You can download any number of packages to the Steelhead appliance, but you can only run up to five packages at a time. The exact number depends on the package size, the amount of resources available, and your Steelhead appliance model.

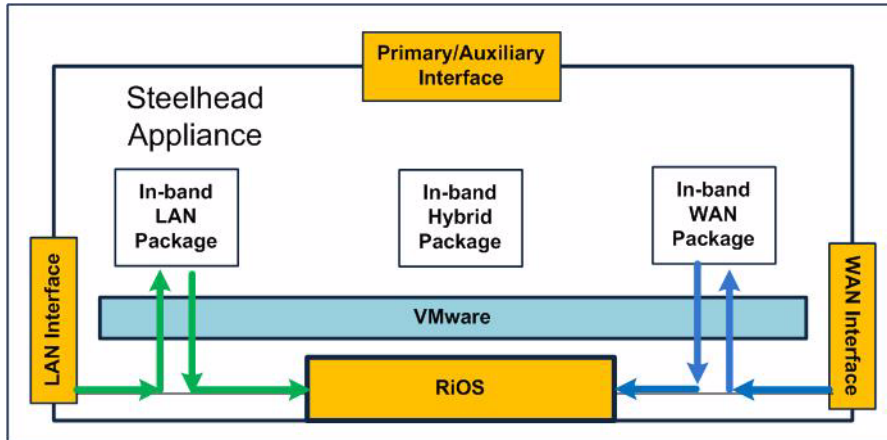
RSP packages contain the service or applications in the virtual machine. RSP packages also contain Riverbed configuration files including the package VNIs. For details about VNIs, see [“Virtual Network Interfaces” on page 15](#). RSP packages include a `.vmx` file and one or more `.vmdk` files. You need not open or modify any of the files in the package. The package files can be quite large and can take up several GBs of disk space.

RSP provides the following packages:

- **In-band packages.** In-band packages work in conjunction with the Steelhead appliance optimization services. You can use the following in-band packages:
  - **In-band LAN packages.** In-band LAN packages intercept data on the Steelhead appliance LAN interface before or after the data flows through RiOS, depending on the traffic direction. Examples of this type of package include Intrusion Detection System or Intrusion Prevention System packages.
  - **In-band WAN packages.** In-band WAN packages intercept data on the Steelhead appliance WAN interface before or after the data flows through RiOS, depending on the traffic direction. Examples of this type of package include firewall, content filtering, and VPN packages.
  - **In-band hybrid packages.** In-band hybrid packages intercept data on both the LAN interface and the WAN interface of the Steelhead appliance. Typically, in-band hybrid packages are network monitoring packages.

The following figure illustrates in-band RSP packages on the Steelhead appliance

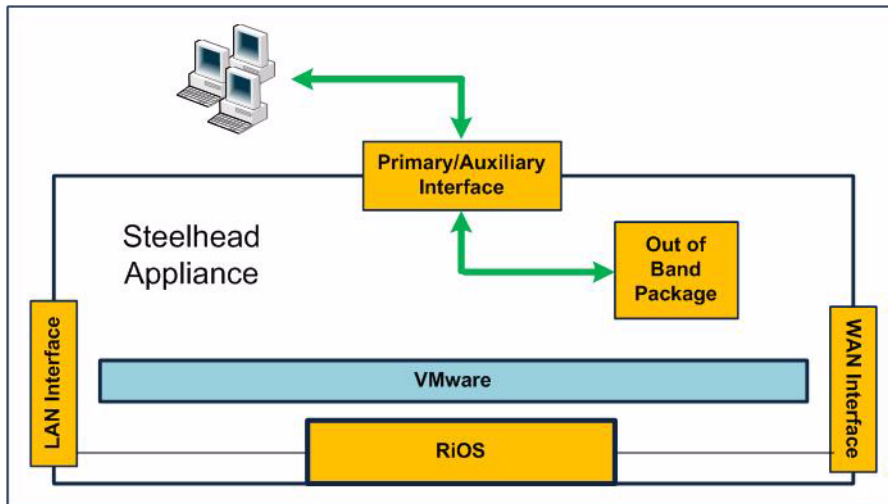
**Figure 1-2. In-Band RSP Packages**



- Out-of-band packages.** Out-of-band packages are not required to work in conjunction with the Steelhead appliance optimization service. Typically, out-of-band packages are located on the Steelhead appliance primary interface. Examples of this type of package include IPAM, print, DNS, and DHCP.

The following figure illustrates an out-of-band RSP package on the Steelhead appliance.

**Figure 1-3. Out-of-Band RSP Packages**



When you install an RSP package you must select an RSP *slot*. A slot is a directory on disk. When you install a package into a slot, the system unpacks the VM into the directory. When you remove a package, the system deletes the files from the slot.

For details about creating an RSP package for a Windows Server, see [“Creating an RSP Package for a Windows Server”](#) on page 63.



## Virtual Network Interfaces

RSP packages use their own virtual network interfaces (VNIs), equivalent to VMware network interfaces, to communicate with the network. These network interfaces are matched to the physical intercept points that create VNIs. VNIs are network taps that enable data flow in and out of the RSP packages. VNIs are available on the LAN, WAN, primary, and auxiliary interfaces of the Steelhead appliance.

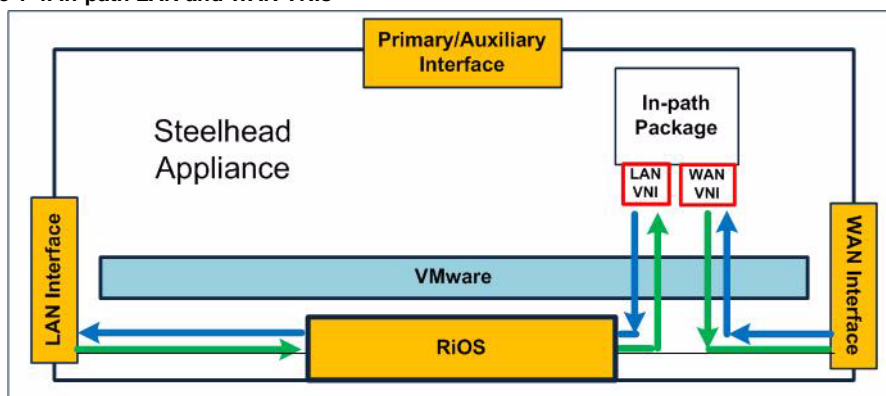
Each package can have ten RSP network interfaces, which enables each package to support ten VNIs. VNIs provide a great deal of configuration flexibility. VNIs also provide the basis for controlling the flow of data through packages in a multiple package scenario.

You can use the following types of VNIs:

- **Optimization VNIs.** Optimization VNIs are used with in-band packages. Optimization VNIs are part of the optimized data flow on either the LAN- or WAN-side of RiOS. There are several types of optimization VNIs:
  - **In-path.** In-path VNIs are used for packages such as security packages. The following types of in-path optimization VNIs are available:
    - **LAN.** LAN VNIs forward packets from the LAN-side to the virtual machine, to the WAN-side, or both. LAN VNIs unconditionally forward packets from the virtual machine to the LAN-side. LAN VNIs cannot receive packets from the WAN-side.
    - **WAN.** WAN VNIs forward packets from the WAN-side to the virtual machine, to the LAN-side, or both. WAN VNIs unconditionally forward packets from the virtual machine to the WAN-side. WAN VNIs cannot receive packets from the LAN-side.

The following figure illustrates in-path LAN and WAN VNIs on the Steelhead appliance.

Figure 1-4. In-path LAN and WAN VNIs



- **Virtual-in-path.** Virtual-in-path VNIs are used for packages that need redirection to intercept traffic. The types of virtual-in-path VNIs are:
  - **DNAT.** Destination Network Address Translation (DNAT) VNIs are used for proxy-based solutions, such as video proxies.
  - **Mirror.** Mirror VNIs are used for network monitoring-based solutions and acts like a SPAN port.
- **Management VNIs.** Management VNIs reside on the Steelhead appliance primary or auxiliary port. Management VNIs are used as a management interface for in-band packages. Management VNIs are the primary communication path for out-of-band packages.

## VNI Rules

VNI rules determine what the VNI does with the traffic it receives. The redirection can be controlled by rules based on IP or port. VNI rules can perform one of the following actions:

- Redirect the packets to the VM.
- Pass the packets along the data flow to the next VNI.
- Pass the packets along the data flow and send a copy of the packets to the VM.

## Default VNI Rules

RSP provides two default rules to direct traffic that does not match any other rules:

- LAN-to-WAN rule
- WAN-to-LAN rule

The default rules are listed after all other rules and you cannot delete them. Riverbed provides the following default rules to direct traffic for optimization VNIs.

Optimization VNI Type	Data Flow Action on IP Traffic	Data Flow Action on Non-IP Traffic
LAN	Pass	Pass
WAN	Pass	Pass
Virtual in-path	L2 switch	L2 switch

Riverbed recommends that you use the Steelhead Management Console to manage RSP rules. For details, see the *Steelhead Management Console User's Guide*.

### Example—Using VNI Rules to Chain Packages Together

For example, if you installed a video streaming package, a security package, and a VPN package on the Steelhead appliance. You can define rules to invoke the following data path:

1. Flash video traffic coming from the LAN Steelhead appliance is redirected to a video proxy solution.
2. All other traffic goes directly to RiOS and is optimized.
3. After RiOS optimizes the traffic, it is redirected to the security package on the WAN-side of the Steelhead appliance that checks the data (or, if it is a VPN solution, encrypts it), and sends it back out of the WAN. You can control the data redirection using rules based on IP or port.

## DNAT Rules

Destination Network Address Translation (DNAT) rules are used for in-path proxy-based solutions. You can only add DNAT rules for a virtual in-path optimization VNIs.

By default, DNAT is disabled. When DNAT is enabled, it translates the network address of packets that match the source and destination IP and the port (or port range) to the target IP and, optionally, the target port. It then routes them to the correct device, host, or network.

For example, you can install an RSP package for live video streaming and add a DNAT rule (using the IP address, port number, or both) that transparently proxies all traffic redirected to the local RSP video instance.

Consequently, the local RSP video instance responds to the local clients on behalf of the original server, simultaneously communicating with the original server in the background over the WAN. This process streamlines the number of requests over the WAN, resulting in time and bandwidth savings.

The RSP rule that determines which traffic is network address translated is provided in the data flow rules for the virtual in-path VNI.

## Usage Notes

Use the following guidelines when you define data flow and DNAT rules:

- Data flow rules are per VNI.
- Data flow rules are unidirectional. For example, typically you have a LAN-to-WAN rule for the LAN VNI, and a reverse WAN-to-LAN rule for the WAN VNI. WAN VNIs do not see data coming from the LAN, and LAN VNIs do not see packets coming from the WAN.
- For a WAN VNI, only WAN-to-LAN rules are applicable.
- For a LAN VNI, only LAN-to-WAN rules are applicable.
- You must create WAN-to-LAN rules and LAN-to-WAN rules separately.
- You can only add DNAT rules for a virtual in-path VNI.
- You can specify a target port range with DNAT rules.

The following table shows some typical rule actions that you can use to control the data flow for the various VNI types:

Optimization VNI type	Typical Data Flow Rule Actions
LAN	Pass traffic around a VM or redirect it to the VM.
WAN	Pass traffic around a VM or redirect it to the VM.
Virtual In-Path DNAT	Pass traffic to the target IP or redirect it to a target IP.
Virtual In-Path Mirror	Pass traffic along the data flow and copy it for monitoring.

## RSP Watchdog

The RSP watchdog determines what to do with traffic during a package failure. By default, the watchdog sends an email alert and bypasses traffic for failed packages. Traffic that normally flows through an optimization VNI on the RSP package skips the optimization VNI and passes through.

You can (optionally) configure a watchdog to block traffic for failed packages. The RSP package must have the management interface configured before you can configure a watchdog on it. For details on configuring an RSP watchdog using the Management Console, see [“Configuring RSP Data Flow” on page 26](#). For details on configuring an RSP watchdog using the CLI, see [“Configuring an RSP Watchdog” on page 66](#).

You configure an IP address on the virtual machine guest operating system Ethernet interface, and bridge it to one of the management VNIs on the Steelhead appliance. The IP address you configure on the virtual machine guest operating system interface is the IP address that the RSP watchdog pings to verify that the RSP service is running.

---

**Note:** For details about configuring an IP address on the virtual machine guest operating system interface, refer to vendor documentation for the operating system installed on your virtual machine.

---

---

## New RSP Features in RiOS Version 5.5.4

RiOS Version 5.5.4 provides the following new RSP features:

- **Backup CLI command.** Use the RSP backup CLI command to restore the RSP data in case the Steelhead appliance fails. The backup command generates a **.zip** file with a **.bkup** file extension.
- **Enhanced RSP Management Console pages.** The RSP Service and RSP Packages pages provide improved access and use more relevant terminology.

---

## Next Steps

To install and configure RSP using the Management Console, see [Chapter 2, “Installing and Configuring RSP Using the Management Console”](#) . To install and configure RSP using the CLI, see [Chapter 3, “Installing and Configuring RSP Using the CLI”](#) .

## CHAPTER 2 Installing and Configuring RSP Using the Management Console

This chapter describes how to configure Riverbed Services Platform (RSP) for the Steelhead appliance using the Management Console. It includes the following sections:

- [“Basic Steps for Installing and Configuring RSP,”](#) next
- [“Installing the RSP Installation Image”](#) on page 20
- [“Adding RSP Packages”](#) on page 22
- [“Configuring RSP Data Flow”](#) on page 26
- [“Performing RSP Tasks”](#) on page 31
- [“Managing Virtual Machines”](#) on page 34
- [“Viewing RSP Statistics Reports”](#) on page 35

---

### Basic Steps for Installing and Configuring RSP

This section provides an overview of the basic steps to install and configure RSP using the Management Console, followed by detailed procedures.

---

**Important:** Follow these steps in the order given to avoid traffic disruption.

---

Task	Reference
1. Verify that your Steelhead appliance supports RSP requirements.	<a href="#">“Product Dependencies and Compatibility”</a> on page 6
2. Download and install the RSP image, which contains the VMware binary programs and the RSP service. The Steelhead appliance RiOS image does not include the RSP image. You must install the RSP image separately.  RSP is pre-installed on newly manufactured Steelhead appliances if you ordered RSP.	<a href="#">“Installing the RSP Installation Image”</a> on page 20  <b>Note:</b> RSP requires RiOS software v5.5 or higher. To upgrade from a version prior to v5.5 to v5.5 with RSP, you must first upgrade to v4.1.7d, v4.1.8, v5.0.5b, v5.0.6 or later, and then upgrade to v5.5 with RSP.

---

Task	Reference
3. Start the RSP service on the Steelhead appliance	<a href="#">“Installing the RSP Installation Image” on page 20</a>
4. Obtain an RSP package by: <ul style="list-style-type: none"> <li>• using an existing package from Riverbed, a third-party vendor, or from within your organization.</li> <li>• creating your own package.</li> </ul> <p><b>Important:</b> The package files can be quite large and can take up several GBs of disk space.</p>	<a href="#">“Adding RSP Packages” on page 22</a>
5. Assign a package to the slot.	<a href="#">“Installing a Package in a Slot” on page 23</a>
6. Enable the slot.	<a href="#">“Enabling a Slot” on page 24</a>
7. Configure the package.	
8. Disable the slot as a safety precaution while you configure the traffic data flow. <p><b>Note:</b> This step is not required for out-of-band packages.</p>	<a href="#">“Disabling a Slot” on page 24</a>
9. Place the slotted package optimization VNI into the data flow. <p><b>Note:</b> This step is not required for out-of-band packages.</p>	<a href="#">“Configuring RSP Data Flow” on page 26</a>
10. Optionally create and add data flow rules to the VNI. <p><b>Note:</b> This step is not required if you use the default rules for the package.</p>	<a href="#">“Adding Rules to an Optimization VNI” on page 27</a>
11. Enable the slot.	<a href="#">“Enabling a Slot” on page 24</a>
12. Verify your configuration.	<a href="#">“Viewing RSP Statistics Reports” on page 35</a>

## Installing the RSP Installation Image

This section describes the prerequisites and the basic steps to install the RSP installation image using the Management Console.

### Prerequisites and Tips

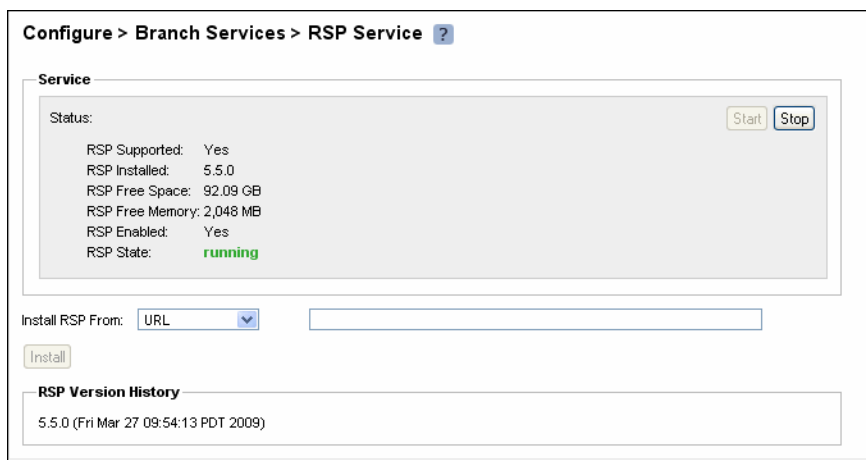
- RSP requires 2 GB of additional memory on the Steelhead appliance. For detailed information, see the *Upgrade and Maintenance Guide*.
- You must have role-based permission for RSP to install RSP. For detailed information about permissions, see the *Steelhead Management Console User’s Guide*.
- Before installing a new RSP image, you must stop the RSP service currently running on the Steelhead appliance.

- RSP requires RiOS software v5.5 or higher. To upgrade from a version prior to v5.5 to v5.5 with RSP, you must first upgrade to v4.1.7d, v4.1.8, v5.0.5b, v5.0.6 or later, and then upgrade to v5.5 with RSP.
- If you have previously installed RSP for RiOS v5.0.x, you must reinstall the RSP image for RiOS v5.5 and later. RSP for RiOS v5.0.x is not compatible with RSP for RiOS v5.5.
- Installing a new RSP image replaces the previously installed image (the virtual machine packages are unmodified).
- For details on Steelhead appliance RSP support for guest operating systems, see the product specification sheets at: <http://www.riverbed.com/products/appliances/>

## To install the RSP image

1. Choose Configure > Branch Services > RSP Service to display the RSP Service page.

Figure 2-1. RSP Service Page



2. Click the Install RSP From drop-down menu and complete the configuration as described in the following table.

Control	Description
URL	Select this option and type the URL to the RSP image in the text box next to the drop-down menu.
Local File	Select this option and type the pathname in the text box next to the drop-down menu, or click <b>Browse</b> to navigate to the local file directory.
Existing Image	Select an image that you uploaded to the Steelhead appliance using the Riverbed CLI. For details, see the <i>Riverbed Command-Line Interface Reference Manual</i> .

3. Click **Install** to download and install RSP on your system.
4. Click **Start** to start RSP.

## Adding RSP Packages

The RSP package contains the service or application in the virtual machine and RSP-specific configuration files. See “RSP Packages” on page 13 for an overview of RSP packages. Before installing a package, you must install the RSP image. See “Installing the RSP Installation Image” on page 20. After installing the RSP image, you can download and install packages.

### To add an RSP package

1. Choose Configure > Branch Services > RSP Packages to display the RSP Packages page.

Figure 2-2. RSP Packages Page

**Configure > Branch Services > RSP Packages ?**

**Packages:**

<input type="checkbox"/>	Local Name	Package Name	Version	Description
<input type="checkbox"/>	Win2k3_AD.zip	Windows 2003 Server AD	1	<none>
<input type="checkbox"/>	m0n0wall.pkg	m0n0wall	1.0	m0n0wall firewall

**Slots:**

Slot	Power	Status	Name	Description
1	on	enabled	Windows 2003 Server AD	<none>

Number of CPUs: 1  
 VMware Tools: running  
 Memory Footprint: 512 MB  
 Watchdog: not watching  
 Watchdog IP:  empty for no watchdog IP  
 Watchdog Frequency: 1 a positive integer  
 Watchdog Timeout: 10 a positive integer

**Optimization Virtual Network Interfaces:**

Name	Type	Vlan	MAC
No Optimization Virtual Network Interfaces			

**Management Virtual Network Interfaces:**

Name	Physical Interface	MAC
1:windows_2003_server_AD_mgmt0	<input checked="" type="radio"/> primary <input type="radio"/> aux	00:0c:29:91:80:a1

[ Launch VM Console ]

2. Under Packages, complete the configuration as described in the following table.

Control	Description
Fetch a Package	Displays the controls to obtain an RSP package.
Name	Optionally, type a descriptive name for the package (up to eight characters).
From URL	Select this option and type the URL to the RSP package image. For third-party packages, get the URL directly from the vendor.



Control	Description
From Local File (for packages less than 2 GB in size)	Click this option and type the path or click <b>Browse</b> to navigate to the local file directory.  <b>Important:</b> You cannot use this option to upload a package file that is larger than 2 GB. If the file is larger than 2 GB you can use SCP or FTP to transfer it using the CLI.
Remove Selected Packages	Click the check box next to the name and click <b>Remove Selected Packages</b> .

**Tip:** To view the VNIs and watchdog settings for a package, click the local name of the package.

## Installing a Package in a Slot

You can install one package per slot. By default, the RSP slots are numbered 1 to 5, although you can change a slot name to make it more descriptive.

### To install an RSP package in a slot

1. Choose Configure > Branch Services > RSP Packages to display the RSP Packages page.

To install an RSP package in an occupied slot, you must first uninstall the package for that slot. Installing a package into a slot and uninstalling that particular slot affects only the slot directory, not the package itself.

2. Under Slots, click the slot name and complete the configuration as described in the following table.

Control	Description
Slot Name	Optionally, type a unique descriptive name for the slot (up to eight characters). <b>Note:</b> The slot must be empty before you can change its name.
Package File Name	Select the package name from the drop-down list.
Update Slot	Adds the package to the slot and updates the configuration. <b>Note:</b> This step can take five minutes or longer to complete.

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

**Important:** Riverbed recommends you configure an RSP watchdog that blocks traffic in the event an in-path security package such as a firewall, fails. For more information, see [“Configuring RSP Data Flow” on page 26](#).

**Note:** To disable a package, click the slot number and then click **Disable Package**.

## Enabling a Slot

After you install a package in a slot, you can enable it.

### To enable a slot

1. Choose Configure > Branch Services > RSP Packages to display the RSP Packages page.

The screenshot shows the 'Configure > Branch Services > RSP Packages' page. It features a 'Packages' section with a table of installed packages and a 'Slots' section with a table of slot configurations. Slot 3 is selected, and its configuration details are shown below the table. An arrow points to the '3' in the slot table, labeled 'click to select the slot'. Another arrow points to the 'Enable Slot' button at the bottom of the configuration panel, labeled 'click to enable the slot'.

**Configure > Branch Services > RSP Packages** ?

**Packages:**

+ Fetch a Package    - Remove Selected Packages

<input type="checkbox"/>	Local Name	Package Name	Version	Description
<input type="checkbox"/>	Win2k3_AD.zip	Windows 2003 Server AD	1	<none>
<input type="checkbox"/>	m0n0wall.pkg	m0n0wall	1.0	m0n0wall firewall

**Slots:**

Slot	Power	Status	Name	Description
1	on	enabled	Windows 2003 Server AD	<none>
2	on	enabled	m0n0wall	m0n0wall firewall
3	off	slot disabled	m0n0wall	m0n0wall firewall

click to select the slot

Number of CPUs: 1  
 VMware Tools: unknown  
 Memory Footprint: 128 MB  
 Watchdog: not watching  
 Watchdog IP:   
 Watchdog Frequency: 1  
 Watchdog Timeout: 10

**Optimization Virtual Network Interfaces:**

Name	Type	Vlan	MAC
3:m0n0wall-lan	Lan	none	
3:m0n0wall-wan	Wan	none	

**Management Virtual Network Interfaces:**

Name	Physical Interface	MAC
3:m0n0wall-mgmt	primary aux	

Update Slot    Enable Slot    Uninstall

click to enable the slot

2. Under Slots, click the slot name and click **Enable Slot** to enable the slot.
3. The slot status changes to enabled.
4. Click **Save** to save your settings permanently.

## Disabling a Slot

You can disable an enabled slot.

## To disable a slot

1. Choose Configure > Branch Services > RSP Packages to display the RSP Packages page.

The screenshot shows the 'Configure > Branch Services > RSP Packages' page. It features two main sections: 'Packages' and 'Slots'.

**Packages:** This section includes a '+ Fetch a Package' button and a '- Remove Selected Packages' button. Below is a table with columns: Local Name, Package Name, Version, and Description.

Local Name	Package Name	Version	Description
Win2k3_AD.zip	Windows 2003 Server AD	1	<none>
m0n0wall.pkg	m0n0wall	1.0	m0n0wall firewall

**Slots:** This section displays a table of slots. The first slot is selected (checked).

Slot	Power	Status	Name	Description
1	on	enabled	Windows 2003 Server AD	<none>

Below the slot table, there are configuration options for the selected slot, including:
 

- Number of CPUs: 1
- VMware Tools: running
- Memory Footprint: 512 MB
- Watchdog: not watching (dropdown)
- Watchdog IP: (input field) *empty for no watchdog IP*
- Watchdog Frequency: 1 *a positive integer*
- Watchdog Timeout: 10 *a positive integer*

There are also sections for 'Optimization Virtual Network Interfaces' (currently empty) and 'Management Virtual Network Interfaces' (showing one interface: 1:windows\_2003\_server\_AD\_mgmt0, primary aux, MAC 00:0c:29:91:80:a1).

At the bottom, there is a '[ Launch VM Console ]' link and two buttons: 'Update Slot' and 'Disable Slot'. A callout points to the 'Disable Slot' button with the text 'click to disable the slot'. Another callout points to the slot name '1' in the table with the text 'click to select the slot'.

2. Under Slots, click the slot name and click **Disable Slot** to disable the slot.
3. The slot status changes to disabled.
4. Click **Save** to save your settings permanently.

## Viewing Slot Status

Choose Configure > Branch Services > RSP Packages to display the RSP Packages page. This page displays all occupied RSP slots and lists the current VM and slot status as described in the following table:

Power	Slot Status	Description
Off	<blank>	VM is off, a package is not installed in the slot, and the watchdog is not in use.
On	Enabled	VM is on, the slot is enabled, and the watchdog is not watching.

Power	Slot Status	Description
On	Healthy	VM is on, the slot is enabled, and the watchdog is watching.
Off	Blocked	VM is off, slot is enabled, and the watchdog has triggered block on failure mode for the traffic affected by the package.
Off	Bypass	VM is off, slot is enabled, and the watchdog has triggered bypass on failure mode for the traffic affected by the package.
Off	Enabled	VM is off, slot is enabled. To troubleshoot, review the VMware server host ID log messages using the Riverbed Command-Line Interface. For details, see the <i>Riverbed Command-Line Interface Reference Manual</i> .
Off	Disabled	VM is off, slot is disabled and the watchdog is not watching.
Off	Slot Disabled	VM is off, slot is installed but not enabled, and the watchdog is watching.
Other	Other	Incorrect state. To troubleshoot, review the VMware server host ID log messages using the Riverbed Command-Line Interface. For details, see the <i>Riverbed Command-Line Interface Reference Manual</i> .

## Configuring RSP Data Flow

This section describes how to add a Virtual Network Interface (VNI) to your RSP data flow and how to add a rule to the VNI.

### Adding a VNI to the Data Flow

After you install and configure RSP, you can add VNI to your configuration. See [“Virtual Network Interfaces” on page 15](#) for an overview of VNIs.

## To add a VNI to the data flow

1. Choose Configure > Branch Services > RSP Data Flow to display the RSP Data Flow page.

Figure 2-3. RSP Data Flow Page

<input type="checkbox"/>	Position	Type	VNI Name	Slot	Package	State	# Rules
<input type="checkbox"/>	null		LAN0_0	null	null	null	null
<input type="checkbox"/>	1		RIOS0_0	null	null		0
<input type="checkbox"/>	2		Rsp0In	1	centospkg		0
<input type="checkbox"/>	3		Rsp0Out	1	centospkg		0
<input type="checkbox"/>	null		WAN0_0	null	null	null	null

Legend:

- LAN NIC
- WAN NIC
- RIOS
- V-Inpath
- LAN VNI
- WAN VNI
- Unknown Type VNI

2. Under Data Flow for <interface>, complete the configuration as described in the following table.

Control	Description
Add a VNI	Displays the controls to add a VNI.
Interface	Select an in-path interface from the drop-down list.
Data Flow Position	Select one of the following from the drop-down list. <ul style="list-style-type: none"> <li>• <b>start.</b> Locates the VNI next to the LAN. A packet coming from the Steelhead appliance LAN interface goes to this VNI first.</li> <li>• <b>end.</b> Locates the VNI next to the WAN. A packet coming from the Steelhead appliance WAN interface goes to this VNI first.</li> <li>• <b>order number.</b> Specifies the VNI order number. A lower number locates the VNI closer to the LAN. A higher number locates the VNI closer to the WAN.</li> </ul>
Add	Adds the VNI to the data flow.
Removed Selected VNIs	Click the check box next to the name and click <b>Remove Selected VNIs</b> .
Move Selected VNIs	Moves the selected VNIs. Click the arrow next to the desired VNI position; the VNI moves to the new position.

The next step is to add rules to configure the traffic flow, unless you use the default rules for the package. For more details on the package data flow, refer to the package documentation.

## Adding Rules to an Optimization VNI

VNI rules determine what an optimization VNI does with the traffic it receives. After you install a package and add it to a slot, you need to add rules to configure the data flow for the package unless you use the default rules for the package. For a WAN VNI, you add WAN-to-LAN rules to direct traffic. For a LAN VNI, you add LAN-to-WAN rules to direct traffic.

See “VNI Rules” on page 16 for an overview of VNI rules.

Use the following tips when you create dataflow rules:

- Place the VNI in the dataflow only for in-band packages.
- You can either use the default IP rules or non IP rules per VNI (customizable by each package vendor).
- Add rules to control traffic (such as in-path rules) per VNI and perform the following actions:
  - Redirect the packets to the VM.
  - Pass the packets along the data flow to the next VNI.
  - Pass the packets along the data flow and send a copy of the packets to the VM.
- Data flow rules are unidirectional.
- For a WAN VNI, only WAN-to-LAN rules apply.
- For a LAN VNI, only LAN-to-WAN rules apply.
- You can only add DNAT rules for a virtual in-path VNI.
- You can specify a target port range with DNAT rules.

#### To add a LAN-to-WAN or WAN-to-LAN rule to a VNI

1. Choose Configure > Branch Services > RSP Data Flow to display the RSP Data Flow page.
2. In the VNI list, click the VNI name.
3. Complete the rule properties under LAN to WAN Rules or WAN to LAN Rules, as described in the following table.

Control	Description
Add a Rule	Displays the controls to add a rule.
Rule Number	Optionally, type a number ( <b>0 - 65535</b> ) to replace the default rule number.
Protocol	Optionally, select <b>All</b> , <b>TCP</b> , <b>UDP</b> , or a specify a protocol number ( <b>1-254</b> ). The default setting is <b>All</b> .
Source Network	Optionally, specify the source subnet of the packet; for example, <b>1.2.3.0/24</b> , or leave it blank to specify all subnets.
Source Port	Optionally, specify a single source port value or a port range of <b>port1-port2</b> , where <b>port1</b> must be less than <b>port2</b> . Leave it blank to specify all ports. <b>Note:</b> You can only specify a port when the protocol is either <b>TCP</b> or <b>UDP</b> .
Destination Network	Optionally, specify the destination network or leave it blank to specify all destination networks.
Destination Port	Optionally, specify the destination port of the packet, either a single port value or a port range of <b>port1-port2</b> , where <b>port1</b> must be less than <b>port2</b> . <b>Note:</b> You can only specify a port when the protocol is either <b>TCP</b> or <b>UDP</b> .
Vlan	Optionally, specify a VLAN identification number or leave it blank to specify all VLANs.
Redirect Traffic to Slot	Click to redirect the packet to a VM.
Pass Traffic Around Slot	Click to pass the packet along the data flow, bypassing the VM.
Copy Traffic to Slot	Click to copy the packet to the VM and also pass it along the data flow.

Control	Description
Add	Adds the rule to the VNI.
Removed Selected Rules	Click the check box next to the name and click <b>Remove Selected Rules</b> .
Move Selected Rules	Moves the selected rules. Click the arrow next to the desired rule position; the rule moves to the new position.

## Changing the Default VNI Rules

The LAN-to-WAN and WAN-to-LAN rule tables include default rules to direct traffic that does not match any other rules. The tables always list these default rules last and you cannot delete them. Riverbed supplies the following default rules to direct traffic for optimization VNIs.

Optimization VNI Type	Data Flow Action on IP Traffic	Data Flow Action on Non-IP Traffic
LAN	Pass	Pass
WAN	Pass	Pass
Virtual in-path	L2 switch	L2 switch

### To edit the default VNI rule settings

1. Choose Configure > Branch Services > RSP Data Flow to display the RSP Data Flow page.
2. In the VNI list, click the VNI name.
3. Under either Default IP Policy or Default Non-IP Policy, click one of the following data flow options:
  - **Pass Traffic Around Slot.** Click to redirect the packet to a VM.
  - **Redirect Traffic to Slot.** Click to pass the packet along the data flow, bypassing the VM.
  - **Copy Traffic to Slot.** Click to copy the packet to the VM and also pass it along the data flow.
  - **Use L2 switching.** Click to use L2 switching.
4. Click **Apply**.
5. Click **Save** to save your changes permanently.

### To add a DNAT rule to a virtual in-path VNI

1. Choose Configure > Branch Services > RSP Data Flow to display the RSP Data Flow page.
2. In the VNI list, click the VNI name.
3. Complete the rule properties under Destination NAT Rules, as described in the following table.

Control	Description
Add a Rule	Displays the controls to add a rule.
Rule Number	Optionally, type a number (0 - 65535) to replace the default rule number.

Control	Description
Protocol	Optionally, select <b>All</b> , <b>TCP</b> , <b>UDP</b> , or specify a protocol number (1-254). The default setting is <b>All</b> .
Source Network	Optionally, specify the source subnet of the packet; for example, <b>1.2.3.0/24</b> , or leave it blank to specify all subnets.
Source Port or Range	Optionally, specify a single source port value or a port range of <b>port1-port2</b> , where <b>port1</b> must be less than <b>port2</b> . Leave it blank to specify all ports.
Original Destination Network	Optionally, specify the destination network or leave it blank to specify all destination networks.
Original Destination Port or Range	Optionally, specify the destination port of the packet, either a single port value or a port range of <b>port1-port2</b> , where <b>port1</b> must be less than <b>port2</b> .
Target Destination Address	Optionally, specify the target address or leave it blank to specify all target addresses.
Target Destination Port or Range	Specify the target destination port of the packet, either a single port value or a port range of <b>port1-port2</b> , where <b>port1</b> must be less than <b>port2</b> . Leave it blank to specify all target ports.
Add	Adds the rule to the VNI.
Removed Selected Rules	Click the check box next to the name and click <b>Remove Selected Rules</b> .
Move Selected Rules	Moves the selected rules. Click the arrow next to the desired rule position; the rule moves to the new position.

---

**Tip:** To remove the data flow configuration for an interface, click **Remove Configuration**.

---

## Bridging a Management VNI to an Interface

When you want to enable a package watchdog, you must bridge one of the management VNIs on the Steelhead appliance to a virtual machine interface. You can bridge a management VNI to either the auxiliary or primary interface to connect the management VNI to the respective physical Ethernet adapter on the Steelhead appliance. For detailed information on RSP watchdogs, see [“Configuring RSP Data Flow” on page 26](#).

### To bridge a management VNI to an interface

1. Choose **Configure > Branch Services > RSP Packages** to display the RSP Packages page.
2. Under **Slots**, click the package slot number.
3. Under **Management Virtual Network Interfaces**, after the VNI name, click **Primary** or **Aux**.
4. Click **Save** to save your settings permanently.



## Performing RSP Tasks

After you install and configure RSP, you can perform the following tasks using RSP:

- [“Updating VLAN Settings,”](#) next
- [“Configuring an RSP Watchdog”](#) on page 31
- [“Configuring RSP Alarm Settings”](#) on page 32

## Updating VLAN Settings

You can add or update the VLAN setting for an optimization VNI in the RSP Packages page.

### To update VLAN settings for an optimization VNI

1. Choose **Configure > Branch Services > RSP Packages** to display the RSP Packages page.
2. Under **Slots**, click the package slot number.
3. Under **Optimization Virtual Network Interfaces**, click the VNI name.
4. After **VLAN**, click **trunk**, **none**, or the third radio button to specify a VLAN tag identification number.
5. Click **Update VNI**.
6. Click **Save** to save your settings permanently.

## Configuring an RSP Watchdog

You can optionally configure an RSP watchdog to determine what to do with traffic during a package failure. The RSP package must have the management interface configured before you can configure a watchdog on it. For an overview of the RSP watchdog feature, see [“RSP Watchdog”](#) on page 17.

### To configure an RSP watchdog

1. Choose **Configure > Branch Services > RSP Packages** to display the RSP Packages page.
2. Under **Slots**, click the slot number.
3. Complete the configuration as described in the following table.

Control	Description
Watchdog	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Not watching.</b> Specifies that the watchdog takes no action if a package fails.</li> <li>• <b>Block on failure.</b> Specifies that the watchdog blocks traffic if a package fails.</li> <li>• <b>Bypass on failure.</b> Specifies that the watchdog bypasses traffic if a package fails.</li> </ul>
Watchdog IP	Specify an IP address of the management VNI to ping.

Control	Description
Watchdog Frequency	Specify the number of seconds between <b>pings</b> to determine whether the package is responsive, for example, 60. You must enter a positive integer.
Watchdog Timeout	Specify the number of seconds to wait for a <b>ping</b> response from the package before the watchdog considers it inactive and stops. You must enter a positive integer.  <b>Note:</b> Specify a larger number of seconds for the watchdog timeout than for the watchdog frequency to ensure that the watchdog attempts enough <b>pings</b> , for example, 180.
Update Slot	Click to apply your configuration to the slot.

4. Bridge one of the management VNIs to a virtual machine interface. For details, see [“Managing Virtual Machines” on page 34](#).

## Configuring RSP Alarm Settings

You can optionally set alarms in System Settings > Alarms page of the Management Console.

## To set RSP alarm parameters

1. Choose Configure > System Settings > Alarms to display the Alarms page.

Figure 2-4. Alarms Page

**Configure > System Settings > Alarms** ?

**Enable Alarms**

- CPU Utilization
  - Rising Threshold (%):
  - Reset Threshold (%):
- Temperature
  - Rising Threshold (°C):
  - Reset Threshold (°C):
- Data Store Wrap Frequency
  - Threshold (days):
- Network Interface Duplex Errors
- Network Interface Link Errors
- Fan Error
- Memory Error
- Extended Memory Paging Activity
- System Disk Full
- Software Version Mismatch
- Asymmetric Routes
- Secure Vault
- Expiring SSL Certificates
- SSL Peering Certificate SCEP Automatic Re-enrollment
- Certificate Revocation List

**Connection Forwarding**

- Connection Forwarding Ack Timeout
- Connection Forwarding Connection Failure

2. Under Enable Alarms, complete the configuration as described in the following table.

Control	Description
RSP License is Close to Expiration	Enables an alarm if an RSP license is due to expire within seven days. By default, this alarm is enabled.
RSP License is Expired	Enables an alarm when an RSP license has expired. By default, this alarm is enabled.

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

---

## Managing Virtual Machines

This section describes how to open a virtual machine (VM) console for an RSP package and how to change the memory footprint for a VM.

### Opening a VM Console

After installing an RSP package, you can open the VM console for the package from the RSP Packages page.

#### To open the VM console for a package

1. Choose **Configure > Branch Services > RSP Packages** to display the RSP Packages page.
2. Under **Slots**, click the package slot number.
3. Click **Launch VM Console**. When the VMware console login screen appears, log in and open the VM console connection to the package.

### Changing the Memory Footprint for a VM

You can optionally change the memory footprint for a VM in the **Configure > Branch Services > RSP Packages** page. Riverbed recommends using the default amount of memory provided for the VM by the vendor.

#### To change the memory footprint for a VM

1. Choose **Configure > Branch Services > RSP Packages** to display the RSP Packages page.
2. Under **Slots**, click the slot number.
3. Complete the configuration as described in the following table.

Control	Description
Memory Footprint	Specify how many megabytes of memory to allocate to the VM. The value must be a multiple of 4.
Update Slot	Updates the slot information.

4. Restart the VM.

## Viewing RSP Statistics Reports

The RSP VNI IO report provides a utilization graph for a package and a VNI for the time period specified. It contains the following table of statistics that summarize RSP VNI activity.

Field	Description
LAN In	Specifies the byte count or number of packets coming into the LAN.
LAN Out	Specifies the byte count or number of packets going out of the LAN.
WAN In	Specifies the byte count or number of packets coming into the WAN.
WAN Out	Specifies the byte count or number of packets going out of the WAN.
Package In	Specifies the byte count or number of packets coming into the package.
Package Out	Specifies the byte count or number of packets going out of the package.

### What This Report Tells You

- How much traffic is coming in and going out the LAN direction?
- How much traffic is coming in and going out the WAN direction?
- How much traffic is coming in and going out of a package?

### About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as GBs of bandwidth, percent (%) of data reduction, connection counts, and the like.

Three triangles near the top margin of the graph point to the value on the x-axis (the time) at which the peak occurred.

The right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

### About Report Data

The Riverbed system polls bandwidth and connection metrics every second and reports on performance for periods up to one month. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

### To view the RSP VNI IO report

1. Choose Reports > Branch Services > RSP VNI IO to display the RSP VNI IO page.

Figure 2-5. RSP VNI IO Page

2. Use the controls to customize the report as described in the following table.

Control	Description
Period	Select a period of <b>Last Minute</b> , <b>Last 5 Minutes</b> , <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , <b>Last Month</b> , or <b>Custom</b> from the drop-down list.  For <b>Custom</b> , enter the <b>Start Time</b> and <b>End Time</b> and click <b>Go</b> . Use the following format: <b>YYYY/MM/DD HH:MM:SS</b>
Slot	Select a slot from the drop-down list.
VNI	Select a VNI from the drop-down list (you must select a slot first).
Data	Select either <b>Bytes</b> or <b>Packets</b> .
Refresh	Select a refresh rate from the drop-down list: <ul style="list-style-type: none"> <li>• To refresh the report every 10 seconds, select <b>10 seconds</b>.</li> <li>• To refresh the report every 30 seconds, select <b>30 seconds</b>.</li> <li>• To refresh the report every 60 seconds, select <b>60 seconds</b>.</li> <li>• To turn refresh off, click <b>Off</b>.</li> </ul>
Go	Displays the report.

3. To print the report, choose **File > Print** in your Web browser to open the Print dialog box.

## CHAPTER 3    Installing and Configuring RSP Using the CLI

This chapter describes how to install and configure RSP using the command line interface on the Steelhead appliance. It includes the following sections:

- [“Basic Steps for Installing and Configuring RSP,”](#) next
- [“Installing the RSP Installation Image”](#) on page 39
- [“Adding RSP Packages”](#) on page 42
- [“Configuring RSP Data Flow”](#) on page 48
- [“Performing RSP Tasks”](#) on page 52
- [“Using RSP Backups”](#) on page 56
- [“Managing Virtual Machines”](#) on page 57
- [“Verifying Your Configuration”](#) on page 58

---

### **Basic Steps for Installing and Configuring RSP**

This section provides an overview of the basic steps to install and configure RSP using the Riverbed CLI, followed by detailed procedures. You must perform each step in the order given to avoid traffic loss.

---

**Important:** Follow these steps in the order given to avoid traffic disruption.

---

Task	Reference
1. Verify that your Steelhead appliance supports RSP requirements.	<a href="#">“Product Dependencies and Compatibility” on page 6</a> <a href="#">“Verifying RSP Requirements” on page 39</a>
2. Download and install the RSP image, which contains the VMware binary programs and the RSP service. The Steelhead appliance RiOS image does not include the RSP image. You must install the RSP image separately.  RSP is pre-installed on newly manufactured Steelhead appliances if you ordered RSP.	<a href="#">“Downloading the RSP Installation Image” on page 40</a> <a href="#">“Uploading the RSP Installation Image on the Steelhead Appliance” on page 40</a>  <b>Note:</b> RSP requires RiOS software v5.5 or higher. To upgrade from a version prior to v5.5 to v5.5 with RSP, you must first upgrade to v4.1.7d, v4.1.8, v5.0.5b, v5.0.6 or later, and then upgrade to v5.5 with RSP.
3. Start the RSP service on the Steelhead appliance.	<a href="#">“Starting RSP” on page 41</a>
4. Obtain an RSP package by: <ul style="list-style-type: none"> <li>• using an existing package from Riverbed, a third-party vendor, or from within your organization.</li> <li>• creating your own package.</li> </ul> <b>Important:</b> The package files can be quite large and can take up several GBs of disk space.	<a href="#">“Adding RSP Packages” on page 42</a>
5. Assign a package to the slot.	<a href="#">“Installing a Package Into a Slot” on page 44</a>
6. Enable the slot.	<a href="#">“Enabling a Slot” on page 44</a>
7. Configure the package. For example, to install a Windows package you would need to configure an IP address for the interface.	<a href="#">“Configuring an IP Address for an RSP Package” on page 47</a> For details about configuring services for your RSP package, refer to the documentation for the package.
8. Disable the slot as a safety precaution while you configure the traffic data flow.	<a href="#">“Disabling a Slot” on page 45</a>
9. Place the slotted package optimization VNI into the data flow.  <b>Note:</b> This step is not required for out-of-band packages.	<a href="#">“Configuring RSP Data Flow” on page 48</a>  Out-of-band packages do not require that you add the package VNI into the data flow.
10. Optionally, create and add RSP package rules to the VNI.  <b>Note:</b> This step is not required if you use the default rules for the package.	<a href="#">“Adding a Rule to the VNI” on page 49</a>
11. Enable the slot.	<a href="#">“Enabling a Slot” on page 44</a>
12. Verify your setup.	<a href="#">“Verifying Your Configuration” on page 58</a>



## Installing the RSP Installation Image

This section describes how to download the RSP installation image on to your computer and then upload it and install it on the Steelhead appliance.

The RSP installation image contains the VMware binary programs and the RSP service. You must install the RSP installation image before you install RSP packages.

### Prerequisites and Tips

Use the following guidelines when you install the RSP installation image:

- Riverbed recommends you use the Steelhead Management Console to install and configure RSP.
- Review hardware, software and system dependencies. For details, see [“Product Dependencies and Compatibility” on page 6](#).
- Ensure you have role-based permission for RSP.
- Ensure you have an RSP service license.
- Before installing a new RSP installation image, stop the RSP service currently running on the Steelhead appliance.
- RSP requires RiOS software v5.5 or higher. To upgrade from a version prior to v5.5 to v5.5 with RSP, you must first upgrade to v4.1.7d, v4.1.8, v5.0.5b, v5.0.6 or later, and then upgrade to v5.5 with RSP.
- Even if you previously installed RSP for RiOS v5.0.x, you must install the RSP installation image for RiOS v5.5 or later. RSP for RiOS v5.0.x is not compatible with RSP for RiOS v5.5.
- Installing a new RSP installation image replaces the previously installed installation image (the virtual machine packages are unmodified).

For details on RSP support for guest operating systems, see the product specification sheets at: <http://www.riverbed.com/products/appliances/>

### Verifying RSP Requirements

Use the following steps to verify that your system supports RSP, has sufficient disk space for RSP use (depending on the package), and has at least 2 GB of additional free memory to run the virtual machine in the slot.

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands to verify your system meets RSP requirements:

```
enable
configure terminal
show rsp
```

For example:

```
riverbed (config) # show rsp
Supported:   Yes
Installed:   No
Release:     5.5.4
Enabled:     No
State:       Off
Disk Space:  10.78 GB used / 195.92 GB free / 206.70 GB total
```

```
Memory:      1.55 GB used / 3.04 GB free / 4.58 GB total
riverbed (config) #
```

If there is not enough free memory available, an error message appears.

You can try reducing the memory footprint for the virtual machine, or reducing it for a virtual machine in another slot. For details, see [“Changing the Memory Footprint for a VM” on page 58](#).

## Downloading the RSP Installation Image

To download the RSP installation image on to your computer:

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands at the system prompt:

```
enable
configure terminal
rsp image fetch <URL>
```

or

```
rsp image fetch scp://<username>:<password>@<hostname>/<path>/<filename>
```

Parameter	Description
<username>	Specify the user name to log in to the host.
<password>	Specify the password to log in to the host.
<hostname>	Specify the name of the source machine on which the installation image file resides.
<path>	Specify the full path for the installation image file on the host.
<filename>	Specify the installation image file name.

## Uploading the RSP Installation Image on the Steelhead Appliance

After you download the RSP installation image on your computer, you must upload and install it on the Steelhead appliance.

### To upload and install the RSP installation image on the Steelhead appliance

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following set of commands at the system prompt:

```
enable
configure terminal
rsp image fetch <image URL>
```

or

```
scp <imagename> <username>@<steelheadname>:/rsp/images/
```

Parameter	Description
<image name>	Specify the full path for the installation image file to load on the Steelhead appliance.
<username>	Specify the user name to log into the Steelhead appliance.
<steelhead name>	Specify the name of the target Steelhead appliance on which the installation image should be loaded.

3. Enter the following command to install the image:

```
rsp image install <rsp image filename>
```

For example:

```
sh-1 > enable
sh-1 # configure terminal
sh-1 (config) # no rsp enable
sh-1 (config) # rsp image fetch http://www.example.com/rsp-image.img
sh-1 (config) # rsp image install rsp-image.img
Installing RSP image . . . . .done.
sh1 (config) # show rsp
  Supported:  Yes
  Installed:  Yes
  Release:    5.5.4
  Enabled:    No
  State:      Off
  Disk Space: 11.26 GB used / 195.44 GB free / 206.70 GB total
  Memory:     1.55 GB used / 3.04 GB free / 4.58 GB total
sh1 (config) #
```

## Starting RSP

After you download and install RSP, you can start RSP as follows:

1. Enter the following commands:

```
enable
configure terminal
rsp enable
write memory
```

2. Enter the following command to verify your system meets RSP requirements:

```
show rsp
```

You are ready to install and configure the RSP package.

## Deleting the RSP installation Image File

To release disk space, you can delete the installation file that you used to install RSP on the Steelhead appliance. Deleting the RSP installation file does not delete RSP functionality.

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
```

```
rsp image delete <rsp image filename>
```

---

## Adding RSP Packages

This section describes how to install RSP packages on the Steelhead appliance using the Riverbed CLI. The RSP package contains the service or application in the virtual machine and RSP-specific configuration files. See [“RSP Packages” on page 13](#) for an overview of RSP packages.

## Obtaining an RSP Package

You obtain an RSP package by either:

- Downloading an existing package from Riverbed, a third-party vendor, or from within your organization. To obtain an RSP package from Riverbed, go to:  
**<https://support.riverbed.com>**
- Creating a package using VMware Server v2.0 or VMware ESX to create the virtual machine, and the RSP Package Generator Wizard to convert the virtual machine into an RSP package.

For details about creating an RSP package for a Windows Server, see [“Creating an RSP Package for a Windows Server” on page 63](#).

---

**Note:** The RSP package files can be quite large and can take up several GBs of disk space.

---

## Prerequisites and Tips

Use the following guidelines when you install and configure the RSP package:

- Riverbed recommends that you use the Steelhead Management Console to install and configure RSP.
- Check that your system meets hardware and software requirements. For details, see [“Product Dependencies and Compatibility” on page 6](#).
- Install an RSP installation image on the Steelhead appliance. For details, see [“Basic Steps for Installing and Configuring RSP” on page 37](#).
- Ensure you have role-based permission for RSP to add a package.
- Ensure you have an RSP license for third party RSP packages.
- Ensure your RSP package is available on an **ftp** or **scp** server, an **HTTP** server, or a laptop.
- If you have a management interface configured, Riverbed recommends that you configure (optional) an RSP watchdog to block traffic in the event that an in-path security package fails.
- VMware Tools users have read-only access to prevent changes to the virtual machine without the knowledge of the Steelhead appliance.
- If you previously installed RSP for RiOS v5.0.x, you must reinstall the RSP installation image for RiOS v5.5 or later. RSP for RiOS v5.0.x is not compatible with RSP for RiOS v5.5.
- For details on Steelhead appliance RSP support for guest operating systems, see the product specification sheets at:

<http://www.riverbed.com/products/appliances/>

- Complete all of the following steps, unless noted as optional, in the order provided.

## Downloading the RSP Package

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp package fetch <URL>
```

or

```
rsp package fetch scp://<username>:<password>@<hostname>/<path>/<filename>
```

Parameter	Description
<username>	Specify the user name to log in to the host.
<password>	Specify the password to log in to the host.
<hostname>	Specify the name of the host machine on which the package file resides.
<path>	Specify the full path for the package file on the host.
<filename>	Specify the package file name.

**Important:** If you fetch a package that is larger than 2 GB you must use **ftp** or **scp**. Due to an Apache limitation, HTTP fails.

## Uploading the RSP Package on the Steelhead Appliance

You can load the RSP package image on the Steelhead appliance in one of the following ways:

- Using a Web browser. For details, see the *Steelhead Management Console User's Guide*.
- Placing the image on a Web server and configuring the Steelhead appliance to download it from the Web server. For details, see the *Steelhead Management Console User's Guide*.
- Using a program such as SCP (secure copy) to load the image in the `/rsp/images` directory, if the image is greater than 2GB.

### To load the RSP package image on the Steelhead appliance

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Open a shell and enter the following command:

```
rsp package fetch <URL>
```

or (if the package is greater than 2 GB):

```
scp <packagename> <username>@<steelheadname>:/rsp/packages/
```

Parameter	Description
<package name>	Specify the full pathname for the package file to push to the Steelhead appliance.
<username>	Specify the user name to log in to the Steelhead appliance.
<steelhead name>	Specify the name of the target Steelhead appliance to push the package to.

3. Log in using the Steelhead appliance password.

## Installing a Package Into a Slot

When you install an RSP package, you select an RSP *slot*. A slot is a directory on the disk. When you install a package into a slot, the system unpacks the virtual machine into the slot directory. When you remove a package, the system deletes the files from the slot.

You can install one package per slot. By default, the RSP slots are numbered 1 to 5. You can change a slot name to more make it more descriptive.

After you load the RSP package, you can install it into a slot on the Steelhead as follows:

Enter the following commands:

```
enable
configure terminal
rsp slot <slot name> install package <package filename>
```

---

**Note:** Installing the package can take five minutes or more.

---

For example:

```
sh-1 (config) # rsp slot 1 install package inpathbridge_v7
This command may take five minutes or more to complete.
Slot "1" is successfully installed.
```

## Enabling a Slot

After you assign an RSP package to a slot, you must enable the slot as follows:

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp slot <slot name> enable
```

3. At the system prompt, enter the following command to verify your system meets RSP memory requirements:

```
show rsp
```

Verify that enough free memory is still available to run the virtual machine in the slot. If there is not enough free memory available you receive an insufficient memory error message, and the slot is not enabled. You can try reducing the memory footprint for the virtual machine, or reducing it for a virtual machine in another slot.

---

**Note:** RSP requires 2 GB additional memory on the Steelhead appliance. If the amount of available memory is less than the memory footprint for the virtual machine you are installing, you receive an insufficient memory error message. For detailed information about installing additional memory, see the *Upgrade and Maintenance Guide*.

---

## Disabling a Slot

Before you uninstall an RSP package, you must disable the slot that contains the package.

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
no rsp slot <slot name in which the package is installed> enable
```

## Setting Slot Priority

You can set a high, normal, or priority for a slot in RSP relative to other slots. RSP allocates CPU resources based on their priority. Slots with the same priority level receive equal CPU access.

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp slot <slot name> priority <priority level>
```

Parameter	Description
<b>priority &lt;priority level&gt;</b>	<p>Specify the priority level for the slot:</p> <ul style="list-style-type: none"> <li>• <b>high.</b> Specifies a higher priority relative to other slots.</li> <li>• <b>normal.</b> Specifies normal priority relative to other slots.</li> <li>• <b>low.</b> Specifies low priority relative to other slots.</li> </ul> <p>For example: <b>priority normal</b></p> <p>The default priority setting is <b>Normal</b>. In the event of CPU contention, CPU resources are allocated to the slots according to the priority specified. Slots with the same priority level receive equal access to the CPU.</p>

## Renaming a Slot

Before you rename an RSP slot, ensure that it is empty.

### To rename an RSP slot

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp slot <slot name> rename <new name>
```

## Uninstalling an RSP Package From a Slot

Before you uninstall an RSP package from a slot, disable the slot in which the RSP package resides.

### To uninstall an RSP package from a slot

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
no rsp slot <slot name> enable
rsp slot <slot name> uninstall
```

## Deleting an RSP Package Installation File

You can delete an RSP package installation file to release disk space. Deleting the RSP package installation file removes the file used to install the package into a slot. It does not uninstall the package from the system. To install the package again, you must download the package and then install it into a slot.

### To delete an RSP package installation file

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp package delete <rsp package name>
```

## Renaming an RSP Package

After you load an RSP package on the Steelhead appliance, you can rename the package.

### To rename an RSP package

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp package move <package name> to <new package name>
```



## Upgrading the RSP Image

---

**Important:** You must manually stop RSP when you upgrade the RSP installation image. Consider upgrading during non-peak hours.

---

You need not uninstall the previous RSP installation image or packages before you upgrade to a newer version.

### To upgrade the RSP image

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp image fetch <URL or scp://username:password@hostname/path/filename>
no rsp enable
rsp image install <rsp image filename>
rsp enable
```

If you use SCP to load the RSP installation image on the Steelhead appliance, use the following destination path: `/rsp/images`.

## Configuring an IP Address for an RSP Package

Use the following steps to configure an IP address for an RSP Windows Server package.

---

**Note:** For details about configuring your RSP package, refer to the documentation for the package.

---

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:
 

```
enable
configure terminal
show rsp slot <slot name>
```
3. Copy and paste the console URL into a Web browser to display the VMware console log in screen.
4. Type your Steelhead appliance user name and password to display the VMware console.
5. Log in to the package using your Windows virtual machine user name and password.
6. In the Windows virtual machine, go to **Start > Control Panel > Network Connections**.
7. Right-click the VMware network interface icon, and select **Properties**.
8. Select **General**, scroll down, and select **Internet Protocol (TCP/IP)**.
9. Select **Properties**, and type the IP address information for the interface and click **OK**.

## Configuring RSP Data Flow

This section describes how to add a Virtual Network Interface (VNI) to your RSP data flow and how to add a rule to the VNI.

### Adding a VNI to the Data Flow

After you install and configure RSP, you can add VNI to your configuration. See [“Virtual Network Interfaces” on page 15](#) for an overview of VNIs.

#### To add a VNI to the data flow

1. Enter the following commands:

```
enable
configure terminal
rsp dataflow <data flow name> add opt-vni <slot name>:<VNI name> vni-num <order number in rule list>
write memory
```

Parameter	Description
<b>dataflow &lt;data flow name&gt;</b>	Specify the data flow name. The data flow name is the name of the in-path interface. For example: <b>dataflow inpath0_0</b>  In the above example, data flow <b>inpath0_0</b> represents and controls the flow of data through the <b>lan0_0</b> , <b>inpath0_0</b> , and <b>wan0_0</b> interfaces.
<b>opt-vni &lt;slot name&gt;:&lt;VNI name&gt;</b>	Specify the optimization VNI name. VNI names have the following format: <b>&lt;SlotName&gt;:&lt;RSPinterfaceName&gt;</b>  For example: <b>wowzaSlot:Rsp0In, 1:LanRSPInf</b>  VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<b>vni-num &lt;order in rule list&gt;</b>	Specify the order number of the VNI in the rule list. The order number in the rule list determines which VNI a packet goes to first, second, third, fourth, and last. <ul style="list-style-type: none"> <li>• <b>start.</b> Locates the VNI next to the LAN. A packet coming from the Steelhead appliance LAN interface goes to this VNI first.</li> <li>• <b>end.</b> Locates the VNI next to the WAN. A packet coming from the Steelhead appliance WAN interface goes to this VNI first.</li> <li>• <b>Order number of the VNI in the rule list.</b> Lower numbers locate the VNI closer to the LAN. Higher numbers locate the VN closer to the WAN.</li> </ul> For example: <b>vni-num start</b>

For example:

```
rsp dataflow inpath0_0 add opt-vni 1:lan0 vni-num start
```

---

**Note:** You must save your changes to memory for them to take effect.

---

2. Enter the following command to enable the RSP slot.

```
rsp slot <slot name> enable
```

3. Enter the following command to verify your system meets RSP memory requirements:

```
show rsp
```

4. Enter the following command to verify your setup:

```
show rsp slot <slot name>
```

5. Copy and paste the console URL into a Web browser to display the VMware console login screen.
6. Type your Steelhead appliance user name and password to display the VMware console and verify your setup.

## Adding a Rule to the VNI

This section describes how to add a rule to the VNI using the CLI. Riverbed recommends that you use the Steelhead Management Console to manage your RSP rules. For details, see [“Configuring RSP Data Flow” on page 26](#).

See [“VNI Rules” on page 16](#) for an overview of VNI rules. Use the following tips when you create dataflow rules:

- Place the VNI in the dataflow only for in-band packages.
- You can either use the default IP rules or non IP rules per VNI (customizable by each package vendor).
- Add rules to control traffic (such as in-path rules) per VNI and perform the following actions:
  - Redirect the packets to the VM.
  - Pass the packets along the data flow to the next VNI.
  - Pass the packets along the data flow and send a copy of the packets to the VM.
- Data flow rules are unidirectional.
- For a WAN VNI, only WAN-to-LAN rules apply.
- For a LAN VNI, only LAN-to-WAN rules apply.
- You can only add DNAT rules for a virtual in-path VNI.
- You can specify a target port range with DNAT rules.

### To add a rule to a VNI

1. Enter the following commands. For example, if you are configuring a LAN-to-WAN rule:

```
enable
configure terminal
```

```
rsp opt-vni <slot name>:<VNI name> rule lan-to-wan action redirect
write memory
```

Parameter	Description
<b>opt-vni &lt;slot name&gt;:&lt;VNI name&gt;</b>	Specify the optimization VNI name. VNI names have the following format: <b>&lt;SlotName&gt;:&lt;RSPinterfaceName&gt;</b> For example: <b>wowzaSlot:Rsp0In, 1:LanRSPInf</b> VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<b>rule &lt;rule type&gt;</b>	Specify the rule type, either <b>lan-to-wan</b> , or <b>wan-to-lan</b> . For example: <b>rule lan-to-wan</b>
<b>action &lt;action type&gt;</b>	Specify the action type: <ul style="list-style-type: none"> <li>• <b>pass</b>. Specifies to redirect the packet to a virtual machine.</li> <li>• <b>redirect</b>. Specifies to pass the packet along the data flow, bypassing the virtual machine.</li> <li>• <b>copy</b>. Specifies to copy the packet to the virtual machine and also pass it along the data flow.</li> </ul> For example: <b>action redirect</b>

**Note:** You must save your changes to memory for them to take effect.

2. Enter the following command to verify your setup:

```
show rsp slot <slot name>
```

3. Copy and paste the console URL into a Web browser to display the VMware console log in screen.
4. Type your Steelhead appliance user name and password to display the VMware console.

## Bridging a Management VNI to an Interface

You bridge a management VNI to either the primary or auxiliary interface to connect the management VNI to the respective physical Ethernet adapter on the Steelhead appliance. The management VNI becomes part of the network connected to the physical primary or auxiliary port of the Steelhead appliance. If you want to use an RSP watchdog you must bridge a management VNI on the Steelhead appliance to a virtual machine interface.

### To bridge a management VNI to an interface

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp mgmt-vni <slot name>:<VNI name> interface <interface type>
```

Parameter	Description
<b>mgmt-vni</b> <slot name>:<VNI name>	Specify the management VNI name. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: <b>testSlot:Rsp0In, 1:LanRSPIf</b> VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<b>interface</b> <interface type>	Specify the interface type, either <b>aux</b> or <b>primary</b> . For example: <b>interface primary</b>

---

**Note:** For details about Riverbed CLI commands, see the *Riverbed Command-Line Interface Reference Manual*.

---

- Verify your setup by entering the following command:

```
show rsp slot <slot name>
```

- Copy and paste the console URL into a Web browser to display the VMware console log in screen.
- Type your Steelhead appliance user name and password to display the VMware console.

## Verifying VNI Statistics

You can view optimization VNI statistics for specified periods of time based on a VNI or based on an interface.

### To view RSP statistics for optimization VNIs

- Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
- Enter the following commands: to view RSP statistics for all optimization VNIs:

```
enable
configure terminal
```

- Enter the following command to view RSP statistics for all optimization VNIs:

```
show stats rsp all-opt-vnis period <time period>
```

or,

Enter the following command to view RSP statistics for a specific optimization VNI:

```
show stats rsp opt-vni <slot name>:<VNI name> period <time period>
```

Parameter	Description
<code>opt-vni &lt;slot name&gt;:&lt;VNI name&gt;</code>	Specify the optimization VNI name. VNI names have the following format: <code>&lt;SlotName&gt;:&lt;RSPinterfaceName&gt;</code>  For example: <code>wowzaSlot:Rsp0In, 1:LanRSPInf</code>  VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<code>period &lt;time period&gt;</code>	Specify the time period, either <b>1min</b> , <b>5min</b> , <b>hour</b> , <b>day</b> , <b>week</b> , or <b>month</b> . For example: <code>period month</code>

4. Enter the following command to view RSP statistics for a specified interface on an optimization VNI:

```
show stats rsp opt-vni <slot name>:<VNI name> side <side type> period <time period>
```

Parameter	Description
<code>opt-vni &lt;slot name&gt;:&lt;VNI name&gt;</code>	Specify the optimization VNI name. VNI names have the following format: <code>&lt;SlotName&gt;:&lt;RSPinterfaceName&gt;</code>  For example: <code>testSlot:Rsp0In, 1:LanRSPInf</code>  VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<code>side &lt;side type&gt;</code>	Specify the side type, either <b>lan</b> , <b>wan</b> , or <b>package</b> . For example: <code>side wan</code>

For example:

```
show stats rsp opt-vni 1:LanRSPInf side wan period hour
```

## Performing RSP Tasks

After you install and configure RSP, you can perform the following tasks using RSP:

- [“Updating VLAN Settings,”](#) next
- [“Configuring an RSP Watchdog”](#) on page 53
- [“Configuring Fail-to-Block for an Interface”](#) on page 54
- [“Configuring Email Alerts”](#) on page 55

## Updating VLAN Settings

You update VLAN settings only to in-band/virtual in-band VNI and not the management VNI.

### To update VLAN settings for an optimization VNI

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

2. Enter the following commands:

```
enable
configure terminal
rsp opt-vni <slot name>:<VNI name> vlan <VLAN type>
```

Parameter	Description
<b>opt-vni &lt;slot name&gt;:&lt;VNI name&gt;</b>	Specify the optimization VNI name. VNI names have the following format: <b>&lt;SlotName&gt;:&lt;RSPinterfaceName&gt;</b>  For example: <b>wowzaSlot:Rsp0In, 1:LanRSPInf</b>  VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<b>vlan &lt;VLAN type&gt;</b>	Specify the VLAN type: <b>none</b> , <b>trunk</b> , or a VLAN number ( <b>0-4094</b> ). For example: <b>vlan trunk</b>  The default value is <b>none</b> .

For example, the following sets the VNI named *lan*, located in slot 2, to **trunk**:

```
rsp opt-vni 1:lan vlan trunk
```

## Configuring an RSP Watchdog

You can optionally configure an RSP watchdog to determine what to do with traffic during a package failure. For an overview of the RSP watchdog feature, see [“RSP Watchdog” on page 17](#).

### To configure an RSP watchdog

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp slot <slot name> watchdog ip <IP address of the management VNI to ping>
rsp slot <slot name> watchdog frequency <seconds>
rsp slot <slot name> watchdog timeout <seconds>
rsp slot <slot name> watchdog enable
```

Parameter	Description
<b>watchdog ip &lt;IP address of the management VNI to ping&gt;</b>	Specify the IP address of the management VNI to ping. For example: <b>watchdog ip 999.999.999.999</b>
<b>watchdog frequency &lt;seconds&gt;</b>	Specify the amount of time, in seconds, between pings. For example: <b>watchdog frequency 60</b>
<b>watchdog timeout &lt;seconds&gt;</b>	Specify the amount of time, in seconds, to wait for a ping response before RSP is considered down. The time-out parameter should be several times greater than the frequency parameter to ensure that enough pings are attempted. For example: <b>watchdog timeout 180</b>

---

**Note:** You must disable and enable the slot for the changes to take effect. The watchdog configuration takes effect immediately.

---

## Configuring Fail-to-Block for an Interface

The fail-to-block mode is useful during a firewall package failure. If the Steelhead appliance loses power or otherwise fails, traffic is allowed through the interface. You can also disable the fail-to-block mode on the package interface. For details about which interfaces support disabling fail-to-block, see the *Network Interface Card Installation Guide*.

### To configure fail-to-block for an interface

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp slot <slot name> watchdog block
write memory
```

---

**Note:** You must save your changes to memory for them to take effect.

---

### To disable fail-to-block for an interface

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
no interface inpathX_Y fail-to-block enable
```



```
write memory
```

---

**Note:** You must save your changes to memory for them to take effect.

---

## Configuring Email Alerts

You can configure an RSP watchdog to send an email and alert you when a package fails.

### To configure email alerts

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
email notify failures enable
write memory
```

---

**Note:** You must save your changes to memory for them to take effect.

---

---

## Using RSP Backups

Use the RSP backup command to restore the RSP data in case the Steelhead appliance fails. The backup command generates a **.zip** file with a **.bkup** file extension. The default backup filename is **<steelheadname>-<slotname>-<date>.bkup**.

You need not shut down the VM before you run the backup command. To optimize the backup feature using the Steelhead appliance, ensure that the data traffic passes through the Steelhead.

---

**Important:** You must restore an RSP backup into the same slot in which it was previously installed on the same Steelhead appliance model.

---



---

**Note:** You can use the RSP backup command only through the Steelhead CLI. It is not available in the Management Console.

---

### To create a backup file

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
rsp slot <slot-name> backup create [nocompress]
```

You can use the **nocompress** option to create uncompressed backup files. This enables you to transfer the backup file efficiently using the Steelhead deduplication feature.

3. After you create an RSP backup file, enter the following commands:

```
rsp backup upload <backup filename> remote <backup URL>
rsp backup fetch <backup URL> [as <backup filename>]
rsp slot <slot-name> backup restore <backup filename>
rsp backup delete <backup filename>
```

Command	Description
<b>rsp slot &lt;slot-name&gt; backup create [nocompress]</b>	Creates a backup file in the specified slot. Use the nocompress option to create uncompressed backup files.
<b>rsp backup upload &lt;backup-filename&gt; remote &lt;backup URL&gt;</b>	Uploads the backup file onto a remote server or another Steelhead appliance using the HTTP, FTP, or SCP URL you specify. For example, you can enter: <code>scp://username:password@host/path</code> .
<b>rsp backup fetch &lt;backup URL&gt; [as &lt;backup filename&gt;]</b>	Obtains the backup file from the server using the HTTP, FTP, or SCP URL and optionally saves it using the filename you specify. For example, you can enter: <code>scp://username:password@host/path</code> .

Command	Description
<code>rsp slot &lt;slot-name&gt; backup restore &lt;backup filename&gt;</code>	Replaces a file in the specified slot with its backup file. You must specify the same slot in which the backup was previously installed.
<code>rsp backup delete &lt;backup filename&gt;</code>	Deletes the backup file from the Steelhead appliance.

## Verifying Your RSP Backup Configuration

Enter the following command on the Steelhead CLI to verify your RSP backup configuration:

```
show rsp backups
```

## Managing Virtual Machines

This section describes how to open a virtual machine (VM) console for an RSP package and how to change the memory footprint for a VM.

### Opening a VMware Console for an Installed VM

After installing an RSP package, you can open a VM console for the package. A VM is an RSP package installed and enabled on the Steelhead appliance.

#### To open a VMware console for an installed virtual machine

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
show rsp slot <slot name>
```

Slot 1:

```
Package:
  Name: minimal package
  Description:
    this package is minimal; it contains a small 1MB harddisk and no interfaces...
```

```
Enabled:          yes
Power State:     on
Priority:         normal
VMware Tools State: unknown
Memory Size:     256 (MB)
Number of CPUs:  1
Watchdog:        unused
  Frequency:     1
  Timeout:       10
IP:              0.0.0.0
Fail-to-Block:  no
Optimization VNIs:
  No optimization VNIs.
Management VNIs:
  No management VNIs.
```

```
Console URL:  
https://www.example.com:8333/ui/?wsUrl=http://localhost:8222/  
sdk&mo=VirtualMachine|16&inventory=none&tabs=hide_
```

3. Copy and paste the console URL into a Web browser to display the VMware console log in screen.
4. Type your Steelhead appliance user name and password to display the VMware console.

## Changing the Memory Footprint for a VM

Riverbed recommends that you use the default amount of memory provided by the vendor. However, if your VM supports a greater or lesser number of services such as printers or Windows user logins, you can optionally increase or decrease the VM memory size.

### To change the memory footprint for a VM

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

2. Enter the following commands:

```
enable  
configure terminal  
no rsp slot <slot name> enable  
rsp slot <slot name> vm memory-size <new memory size in MB>  
rsp slot <slot name> enable
```

3. At the system prompt, enter the following command to verify your system meets RSP requirements:

```
show rsp
```

4. Verify that enough free memory remains available to run the virtual machine in the slot. If there is not enough free memory available you receive an insufficient memory error message, and the slot is not enabled. You can try reducing the memory footprint for the virtual machine, or reducing it for a virtual machine in another slot.

---

**Note:** RSP requires 2 GB additional memory on the Steelhead appliance. If the amount of available memory is less than the memory footprint for the virtual machine you are installing, you receive an insufficient memory error message.

---

5. Disable the slot and enable it again for the changes to take effect.

## Verifying Your Configuration

After you install and configure RSP, verify your configuration on the Steelhead CLI as follows:

1. Enter the following command:

```
show rsp slot <slot name>
```

For example:

```
Slot 1:  
Package:
```

```
Name: minimal package
Description: this package is minimal; it contains a small 1MB harddisk and no interfaces...

Enabled:          yes
Power State:      on
Priority:          normal
VMware Tools State: unknown
Memory Size:      256 (MB)
Number of CPUs:   1
Watchdog:         unused
  Frequency:      1
  Timeout:        10
  IP:             0.0.0.0
  Fail-to-Block: no
Optimization VNIs:
  No optimization VNIs.
Management VNIs:
  No management VNIs.
Console URL:
  https://sh-1.lab.nbttech.com:8333/ui/?wsUrl=http://localhost:8222/
  sdk&mo=VirtualMachine|16&inventory=none&tabs=hide_
```

2. Copy and paste the console URL into a Web browser to display the VMware console log in screen.
3. Type your Steelhead appliance user name and password to display the VMware console and verify your RSP setup.



## CHAPTER 4 Using VMware Infrastructure Software

This chapter explains how to manage your virtual machine (VM) using VMware Infrastructure software. A VM is an RSP package installed and enabled on the Steelhead appliance.

---

### Using VMware Infrastructure Software

This section describes how to manage virtual machines on your Steelhead appliance using VMware Infrastructure software. A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. For more details on virtual machines, see the VMware documentation at <http://www.vmware.com>.

Using VMware Infrastructure software, you can:

- create snapshots for your virtual machines.
- open a console connection for a specific virtual machine.
- view the status of all or your virtual machines.
- get performance reports for the virtual machine:
  - CPU.
  - disk.
  - memory.
  - system.

---

**Note:** For security and administrative reasons, Riverbed has disabled other VMware Infrastructure functionality.

---

There are two versions of VMware Infrastructure software that you can use to manage virtual machines on your Steelhead appliance: VMware Infrastructure Web Access and VMware Infrastructure Client (for Windows).

### Using the VMware Infrastructure Client (for Windows)

To use VMware Infrastructure Client (for Windows) you must download it and install it on a PC running Microsoft Windows.

VMware Infrastructure Client (for Windows) might provide better performance than VMware Infrastructure Web Access when you interact with VMware Server 2.0 running on the Steelhead appliance. You can download VMware Infrastructure Client (for Windows) from the Steelhead appliance on which you have installed RSP.

### To download VMware Infrastructure Client (for Windows)

1. Connect to the Steelhead CLI. For details, see the *Riverbed Command-Line Interface Reference Manual*.
2. Enter the following commands:

```
enable
configure terminal
show rsp vmware vi-access
```
3. Copy and paste the download URL address into a Web browser and download the installation image.
4. Double-click the installation package to start the installation after the download completes. Follow the wizard prompts and install the VMware Infrastructure Client (for Windows).

## Using VMware Infrastructure Web Access and Windows Client

To use VMware Infrastructure Web Access you need a Web browser.

### To open VMware Infrastructure Web Access

1. In a Web browser, browse to the virtual machine and type:  
**http://<Steelhead appliance IP Address>:8222**  
or  
**https://<Steelhead appliance IP Address>:8333**  
For example: **https://xxx.xxx.xxx.xxx:8333**
2. Type the Steelhead appliance user name and password and click **Log In**.
3. Select a virtual machine from the list of virtual machines in the left panel.

### To open VMware Infrastructure Client (for Windows)

1. Double-click the VMware Infrastructure Client (for Windows) icon to open the application.
2. In VMware Infrastructure Client (for Windows), type the following for **host**:  
**<Steelhead appliance IP Address>:8333**  
For example: **xxx.xxx.xxx.xxx:8333**
3. Type the Steelhead appliance user name and password and click **Log In**.
4. Select a virtual machine from the list of virtual machines in the left panel.



## CHAPTER 5    Creating an RSP Package for a Windows Server

This chapter describes how to create an RSP package for a Windows Server for use on the Steelhead appliance. This section describes how to use VMware Server v2.0 and the Riverbed RSP Package Generator Wizard to create the RSP package for a Windows Server. It includes the following sections:

- [“Installing the Windows Package,”](#) next
- [“Overview of RSP Package Creation”](#) on page 64
- [“Hardware and Software Dependencies”](#) on page 64
- [“Basic Steps for Creating an RSP Package”](#) on page 65
- [“Creating the Virtual Machine”](#) on page 66
- [“Installing Windows Server on the Virtual Machine”](#) on page 69
- [“Installing VMware Tools on the Virtual Machine”](#) on page 70
- [“Configuring Services on the Virtual Machine”](#) on page 71
- [“Reconfiguring the Virtual Machine for RSP”](#) on page 71
- [“Converting the Virtual Machine into an RSP Package for a Windows Server”](#) on page 72

---

### Installing the Windows Package

For the Steelhead xx50 model appliances, Riverbed also provides an option to purchase fully-licensed OEM Microsoft Windows 2008 Standard package. The RSP package is already installed on the Steelhead appliance with a Certificate of Authenticity (COA) sticker containing your license key attached to the appliance. To obtain the package, simply browse for it and the file **ms\_windows\_2008\_standard<version>.pkg** appears. The package name varies based on the version installed.

You can assign a package to a slot using the instructions [“Installing a Package in a Slot”](#) on page 23.

You can also create your own RSP Windows package (see [Chapter 5, “Creating an RSP Package for a Windows Server.”](#)) and use your Windows license to deploy it on any Steelhead appliance that supports RSP.

---

## Overview of RSP Package Creation

To create an RSP package, create a virtual machine and then convert it into an RSP package using the Riverbed Package Generator Wizard to convert the virtual machine into an RSP package.

You can create the virtual machine using VMware Server v2.0, VMware ESX, or VMware Workstation. Install the VMware application on a workstation and create the virtual machine on the workstation. Also, use the VMware application to install VMware Tools on the virtual machine, and reconfigure the virtual machine for RSP.

VMware Server v2.0 does not need a separate license.

---

**Note:** The instructions in this document are for VMware Server v2.0.

---

For the most recent VMware Server v2.0 documentation, see the *VMware Server User's Guide* at:

<http://www.vmware.com>.

After you create the virtual machine, install a guest operating system (in this case, the guest operating system is the Windows Server) and configure services on the virtual machine.

After you install a guest operating system and configure services on the virtual machine, use the Riverbed Package Generator Wizard to convert the virtual machine into an RSP package. You can use the Package Generator Wizard to create all types of RSP packages.

Download the Package Generator Wizard from the Riverbed Technical Support Web site located at

<https://support.riverbed.com>.

Install the Package Generator Wizard on a workstation and convert the virtual machine into an RSP package on the workstation.

The Package Generator Wizard creates the RSP package which contains the **.vmx** file, **.vmdk** files, and Riverbed configuration files, including the package VNIs. The package files can be quite large, and can take up several GBs of disk space.

You do not need to edit any of the files in the RSP package.

The Package Generator Wizard runs on Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista or Redhat Enterprise Linux 4.0.

---

## Hardware and Software Dependencies

The following table summarizes the system specifications for Package Generator Wizard.

RSP Package Generator	
Operating System	Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, or Redhat Enterprise Linux 4.0
CPU	1.0 GHz
Memory	512 MB

## RSP Package Generator

Virtual Processors	<ul style="list-style-type: none"> <li>Verify that the Steelhead appliance model on which you are installing RSP supports the number of processors you assign to your virtual machine.</li> <li>The total number of virtual processors on your virtual machine must be equal to or less than the number of physical processors on the Steelhead appliance.</li> </ul>
Virtual Hardware	<p>Virtual hardware Generation 4, 6, 7, or 8.</p> <p>You can use VMware Server v2.0, VMware ESX, or VMware Workstation software to create the virtual machine.</p> <p><b>Important:</b> Ensure that your virtual machine has virtual hardware Generation 4, 6, 7, or 8. For details, see the <i>Virtual Machine Mobility Planning Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>

## Basic Steps for Creating an RSP Package

This section provides the basic steps to create an RSP package for a Windows Server. It also lists the tools and software you use for each step. As you proceed through the detailed steps in the following sections, refer back to the list in the following table.

**Important:** Follow these steps in the order given.

Task	Reference
1. Install the VMware application on a workstation.	<ul style="list-style-type: none"> <li>Use VMware Server v2.0, VMware ESX, or VMware Workstation.</li> </ul> <p>For VMware Server v2.0 documentation, see the <i>VMware Server Installation Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>
2. Create the virtual machine.	<p><a href="#">“Creating the Virtual Machine” on page 66</a></p> <ul style="list-style-type: none"> <li>Use VMware Server v2.0, VMware ESX, or VMware Workstation.</li> </ul> <p><b>Note:</b> The virtual hardware must be Generation 4, 6 or 7.</p> <p>For VMware Server v2.0 documentation, see the <i>VMware Server User’s Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>
3. Install the Windows Server guest operating system on the virtual machine.	<p><a href="#">“Installing Windows Server on the Virtual Machine” on page 69</a></p> <p>For details about the operating systems supported by VMware Server v2.0, see the <i>Guest Operating System Installation Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>
4. Install VMware Tools on the virtual machine.	<p><a href="#">“Installing VMware Tools on the Virtual Machine” on page 70</a></p> <ul style="list-style-type: none"> <li>Use VMware Server v2.0, VMware ESX, or VMware Workstation.</li> <li>The VMware Tools contain drivers that improve your virtual machine performance.</li> </ul> <p>For the most recent VMware Server v2.0 documentation, see the <i>VMware Server User’s Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>

Task	Reference
5. Configure services on the virtual machine guest operating system.	<p><a href="#">“Configuring Services on the Virtual Machine” on page 71</a></p> <p>You can configure services on the Windows Server, such as print, DHCP, DNS, Active Directory, and streaming media.</p> <p>For details about other applications and services, refer to the documentation for the application you are installing on the virtual machine.</p> <p><b>Note:</b> You can configure services on the virtual machine application you install the virtual machine on the Steelhead appliance.</p>
6. Reconfigure the virtual machine for RSP.	<p><a href="#">“Reconfiguring the Virtual Machine for RSP” on page 71</a></p> <ul style="list-style-type: none"> <li>• Use VMware Server v2.0, VMware ESX, or VMware Workstation.</li> </ul> <p>For the most recent VMware Server v2.0 documentation, see the <i>VMware Server User’s Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>
7. Enable serial support if you need serial access from the Riverbed CLI.	<p><a href="#">“Enabling a Named-Pipe Serial Support” on page 72</a></p> <ul style="list-style-type: none"> <li>• Use VMware Server v2.0, VMware ESX, or VMware Workstation.</li> </ul> <p>For the most recent VMware Server v2.0 documentation, see the <i>VMware Server User’s Guide</i> at <a href="http://www.vmware.com">http://www.vmware.com</a>.</p>
8. Convert the virtual machine into a Riverbed RSP package.	<p><a href="#">“Converting the Virtual Machine into an RSP Package for a Windows Server” on page 72</a></p> <ul style="list-style-type: none"> <li>• You must use the Riverbed Package Generator Wizard.</li> </ul>

For details about VMware Server v2.0, see the *VMware Server User’s Guide* at <http://www.vmware.com>.

## Creating the Virtual Machine

This section describes how to create a virtual machine using VMware Server v2.0. This section assumes that you have installed VMware Server v2.0 on your workstation.

You can use VMware Server v2.0, VMware ESX, or VMware Workstation to create the virtual machine. The virtual hardware version must be Generation 4, 6, 7, or 8.

For details about VMware Server v2.0, go to <http://www.vmware.com>.

### Prerequisites and Tips

- VMware Server v2.0 is installed on your workstation.
- Ensure that your virtual hardware is Generation 4, 6 or 7; otherwise, an error message appears and you cannot install the package.
- Verify that the Steelhead appliance model on which you are installing RSP supports the number of processors you assign to your virtual machine. The total number of virtual processors on your virtual machine must be equal to or less than the number of physical processors on the Steelhead appliance.
- Allocate all the necessary disk space when you create the virtual machine because RSP does not support the *grow* option. Disk space size is ideally not greater than 12 GB (unless you are leveraging the entire RSP disk space for a single package).
- Disable the following in your package:
  - logging.

- external adaptors, such as sound cards, USB interfaces, and floppy adapters.
- Before you create the virtual machine, verify the requirements for the guest operating system you are installing on the virtual machine. For details, see the *VMware Guest Operating System Installation Guide* at <http://www.vmware.com>.
- For details on Steelhead appliance RSP support for guest operating systems, see the product specification sheets at:  
<http://www.riverbed.com/products/appliances/>
- Install VMware Tools on your virtual machine.
- Enable serial support if you need serial access from the Riverbed CLI.
- Complete the following steps in the same order.

---

**Note:** Create the virtual machine on a workstation. You cannot create the virtual machine on the Steelhead appliance.

---

### To create a new virtual machine

1. Double-click the VMware Server Home Page icon on your workstation desktop to open VMware Infrastructure Web Access.
2. Log in using your workstation user name and password to open VMware Infrastructure Web Access.

---

**Note:** If you are remotely accessing a workstation to create the virtual machine, see the *VMware Server User's Guide* at <http://www.vmware.com>.

---

3. Place your cursor at the root directory in the Inventory panel, click the Summary tab, and select **Create Virtual Machine** to display the Name and Location page.
4. On the Name and Location page:
  - Enter the name of the virtual machine. The virtual machine name is used in the list of available virtual machines. The name is also used for the automatically created subfolder in the data store. The subfolder contains all the files associated with the virtual machine.
  - Select a data store from the list of available data stores.
  - Click **Next** to display the Guest Operating System page.
5. On the Guest Operating System page:
  - Select **Windows operating system**.
  - Select the Windows operating system version from the drop-down list.
  - Optionally, expand **Product Compatibility** to select the virtual machine hardware version.
  - Click **Next** to display the Memory and Processors page.
6. On the Memory and Processors page:

**Important:** Verify that the Steelhead appliance model on which you are installing RSP supports the number of processors you assign to your virtual machine. The total number of virtual processors on your virtual machine must be equal to or less than the number of physical processors on the Steelhead appliance.

---

- Optionally, adjust the memory settings as necessary. The default memory setting is sufficient for most configurations. Increase the memory setting if your virtual machine has an application that uses large amounts of memory.
  - Select 1 from the number of processors for the virtual machine from the drop-down list and click **Next** to display the Hard Disk page.
7. On the Hard Disk page, select **Create a New Virtual Disk** to display the Properties page.
8. On the Properties page:
- Specify the hard disk size and location.
  - Expand **File Options** and specify **Allocate all disk space now**.
  - Expand **Disk Mode** and specify **Persistent**.
  - Expand **Virtual Device Node** and:
    - select an adapter from the drop-down list.
    - select 0 (zero) from the device number drop-down list.
  - Expand **Policies** and select one of the following:
    - Optimize for safety.
    - Optimize for performance.

---

**Note:** If your guest operating system supports journaling file systems, and the RSP package is not business critical (for example, the service does not impact network connectivity), use the **Optimize for performance** option. Otherwise use the **Optimize for safety** option. Also, note that the guest operating system does its own caching.

---

- Click **Next** to display the Network Adapter page.
9. On the Network Adapter page, select **Add a Network Adapter**. This option adds a network adapter to your virtual machine.
- Select **Bridged** from the type of network drop-down list.
  - Select **Connect at Power On**.
  - Click **Next** to display the Home page.
10. On the CD/DVD Drive page, select **Use a Physical Drive** or **Use an ISO Image** to provide the guest operating system access to a physical CD or DVD drive on the host system. You use this drive to install the guest operating system and VMware Tools.
- Select the CD/DVD drive from the drop-down list.
  - If you do not want this drive to be connected when you power on the virtual machine, deselect **Connect at Power On**.
  - Click **Next** to display the Floppy Drive page.

11. On the Floppy Drive page, select **Don't Use a Floppy Drive**.
  - Click **Next** to display the USB Controller page.
12. On the USB Controller page, select **Don't Add a USB Controller**.
  - Click **Next** to display the Ready to Complete page.
13. On the Ready to Complete page, verify your setup and click **Finish** to create the virtual machine. The wizard:
  - Creates the files and hardware for your virtual machine.
  - Saves the files using the filename you previously specified in the virtual machine. On a Windows operating system, the virtual machine is saved in the **C:\Virtual Machines** folder.
  - Displays the virtual machine under the Inventory panel.

You are now ready to install Windows on the virtual machine.

---

**Note:** To resume work later, double-click the VMware Server v2.0 icon on your desktop, open the application, and select your virtual machine from the Inventory panel.

---

---

## Installing Windows Server on the Virtual Machine

This section describes how to install Windows Server 2003 on the virtual machine using VMware Server v2.0.

### Prerequisites and Tips

- You need a complete Windows Server 2003 installation CD to complete the installation.
- Your virtual machine must be configured with a CD-ROM drive.

### To install Windows on the virtual machine

1. Insert the Windows Server 2003 CD into the CD-ROM drive and power on the virtual machine.
2. If you are using the virtual BusLogic SCSI driver downloaded from the VMware Website, do the following:
  - As the Windows Server 2003 installer loads, press the **F6** key and select the additional SCSI driver required for installation.
  - Press **S** to specify the additional driver.
  - Specify the SCSI driver and press **Enter** to continue with the setup.
3. Follow the remaining installation steps as you do for a physical machine.

---

**Important:** Remove any CD/DVD drives from the virtual machine after you install the operating system and VMware tools.

---

You are now ready to install VMware Tools into your virtual machine.

---

**Note:** To resume work later, double-click the VMware Server v2.0 icon on your desktop, open the application, and select your virtual machine from the Inventory panel.

---

---

## Installing VMware Tools on the Virtual Machine

This section describes how to install VMware Tools onto a virtual machine using VMware Server v2.0. The VMware Tools contain drivers that improve your virtual machine performance.

---

**Note:** You need a CD drive installed on the virtual machine to install VMware Tools. After you install VMware Tools, remove the CD drive from the virtual machine.

---

---

**Note:** If your guest operating system is Windows NT, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista, you must log in as an administrator to install VMware Tools. If your guest operating system is Windows 95, Windows 98, or Windows Me, any user can install VMware Tools.

---

### To install or upgrade VMware Tools onto the virtual machine

1. Double-click the VMware Server v2.0 icon on your desktop to open the application.
2. Verify that the virtual machine Power State is **Powered On** in the Status section of the virtual machine Summary tab.
3. Click **Install VMware Tools** in the Status section of the virtual machine Summary tab.
4. Click the Console tab.
  - If **autorun** is enabled in the guest operating system, the system prompts you to install VMware Tools.
    - Click **Yes** to launch the Install Shield wizard and follow the instructions.
  - If autorun is not enabled, select **Start > Run** and type:  
**D:\setup\setup.exe**, where D: is your first virtual CD/DVD drive.
5. If prompted, reboot the virtual machine.
6. Verify that the VMware Guest Service is running on the Windows guest operating system. In the Windows guest operating system, go to **Start > Control Panel > Administrative Tools/Services** and verify that the status for VMware Guest Service is **Started**.

---

**Note:** The VMware Guest Service must be running on the guest operating system to use VMware Tools.

---



The changes you made are automatically saved in the virtual machine using the filename you previously specified. On a Windows operating system, the virtual machine is saved in the **C:\Virtual Machines** folder.

You are now ready to install an application into your virtual machine. If you are not installing an application, proceed to [“Reconfiguring the Virtual Machine for RSP”](#).

---

## Configuring Services on the Virtual Machine

Refer to the documentation for the application you are installing on the virtual machine. In this example, you configure services on the Windows Server, such as print services, DHCP, and DNS.

---

**Note:** You can configure services on the virtual machine application after you install the virtual machine on the Steelhead appliance.

---

You are now ready to reconfigure your virtual machine for use in an RSP package.

---

## Reconfiguring the Virtual Machine for RSP

This section describes how to configure the virtual machine for RSP using VMware Server v2.0.

### To reconfigure the virtual machine for RSP

1. Double-click the VMware Server v2.0 icon on your desktop to open the application.
2. In the Inventory panel, select the virtual machine.
3. Verify that the virtual machine is off.
4. Under the Summary - Hardware tab, select the floppy drive, click **Remove** and **Yes**. The floppy drive is removed.
5. Under the Summary - Hardware tab, select the CD-ROM, click **Remove** and **Yes**. The CD-ROM is removed.
6. Under the Summary - Hardware tab, select the USB, click **Remove** and **Yes**. The USB is removed.
7. To disable logging, under the Summary - Commands tab do the following:
  - Select **Configure VM**.
  - Click the **Advanced** tab.
  - Under Settings, deselect **Enable Logging** to disable logging, and click **OK**.

The changes you made are automatically saved in the virtual machines using the filename you previously specified in the virtual machine. On a Windows operating system, the virtual machine is saved in the **C:\Virtual Machines** folder.

You are now ready to add a named-pipe serial port to your virtual machine.

## Enabling a Named-Pipe Serial Support

This section describes how to add a named-pipe serial port to the virtual machine using VMware Server v2.0.

### To add a named-pipe serial port to the virtual machine

1. Double-click the VMware Server v2.0 icon on your desktop to open the application.
2. Start the VMware Add Hardware wizard and select the virtual machine from the Inventory panel.
3. Verify that the virtual machine is powered off. If the virtual machine is on, shut down the guest operating system and click **Power Off** on the tool bar.
4. In the Summary - Commands tab, click **Add Hardware** to display the Add Hardware wizard.
5. In the Add Hardware wizard:
  - Select **Serial Port** and **Use Named Pipe**.
  - Enter the pathname and filename for the pipe using the following format:
    - On Windows hosts: `\\.\pipe\<namedpipe>`.
    - On Linux hosts: `/tmp/<socket>` or another UNIX socket name of your choice.
  - For **Near End**, accept the default setting **Is a server**.
  - For **Far End**, select **Is an application**.
  - Click **Yes** to select **Connect at Power On** (the default) to connect to the named-pipe when you power on the virtual machine.
  - Optionally, you can select **Yield CPU on poll** by expanding the I/O Mode. The target virtual machine kernel uses the virtual serial port in polled mode, not interrupt mode.
  - Click **Next**.
6. Verify your configuration summary and click **Finish**.

The changes you made are automatically saved in the virtual machines using the filename you previously specified in the virtual machine. On a Windows operating system, the virtual machine is saved in the **C:\Virtual Machines** folder.

You are now ready to use the Riverbed Package Generator Wizard to convert your virtual machine into an RSP package for a Windows Server.

---

## Converting the Virtual Machine into an RSP Package for a Windows Server

This section describes how to use the Riverbed Package Generator Wizard to convert the virtual machine you created into an RSP package for a Windows Server. This section assumes that you have created a virtual machine.

You must use the Riverbed Package Generator Wizard to create RSP packages.

Before you convert your virtual machine into an RSP package, check that your configuration meets the prerequisites listed in the section, “[Hardware and Software Dependencies](#)” on page 64.

### To create the RSP package

1. Download the Package Generator Wizard to your workstation from:  
<https://support.riverbed.com>.

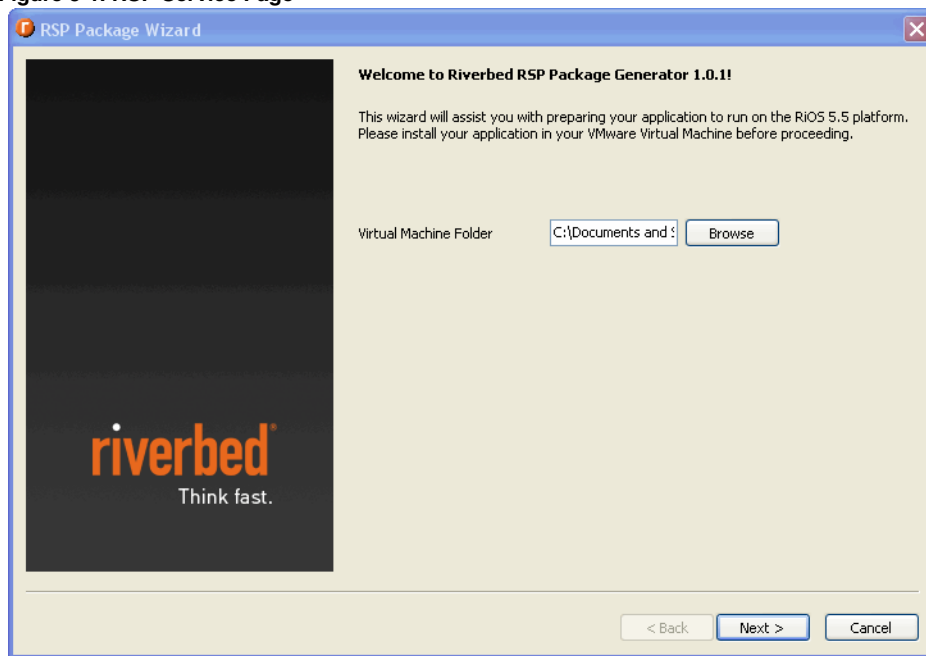
---

**Note:** The Package Generator Wizard can run from any directory and does not require installation or configuration.

---

2. Start the Package Generator Wizard. The Welcome page appears.

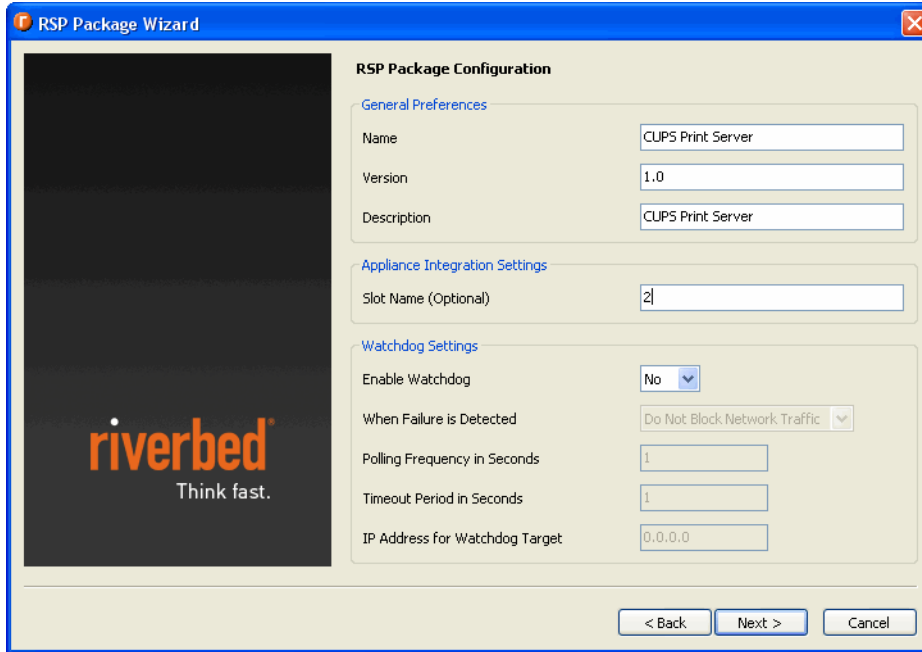
**Figure 5-1. RSP Service Page**



3. Browse to the folder that contains the virtual machine you created. For example, on a Windows operating system, the virtual machine is located in the **C:\virtual machines** folder.

- Click **Next** to display the RSP Package Configuration page.

**Figure 5-2. RSP Package Configuration Page**



- Configure the package as described in the following table.

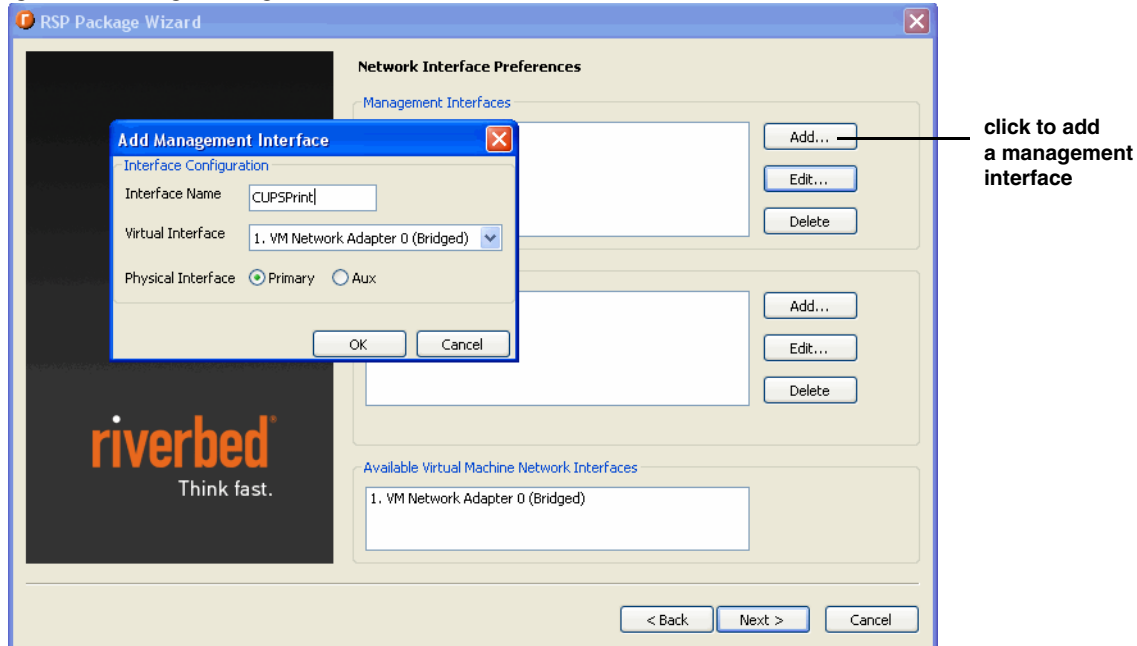
	Field	Description
General Preferences	Name	Specify the name of the package.
	Version	Specify the version of the package.
	Description	Specify a description for the package.

	Field	Description
Watchdog Settings	Enable Watchdog	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Yes.</b> Enables the watchdog. If an RSP package fails, the RSP watchdog sends an email alert and bypasses traffic destined for failed packages. Traffic that normally flows through an optimization VNI on the RSP package now skips the optimization VNI, and is allowed through.</li> <li>• <b>No.</b> Disables the watchdog. If an RSP package fails, the RSP watchdog takes no action.</li> </ul>
	When Failure is Detected	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Block Network Traffic.</b> Enables fail-to-block mode for the package interface. In fail-to-block mode, if the Steelhead appliance has an internal software failure or power loss, the Steelhead appliance LAN and WAN ports power down and stop bridging traffic.</li> <li>• <b>Bypass Network Traffic.</b> Enables fail-to-wire mode for the package interface. In fail-to-wire mode, if the Steelhead appliance has an internal software failure or power loss, the Steelhead appliance LAN and WAN ports become internally connected as if they were the ends of a crossover cable, thereby providing uninterrupted transmission of data over the WAN.</li> </ul>
	Polling Frequency in Seconds	Specify the amount of time, in seconds, between <b>pings</b> .
	Timeout Period in Seconds	Specify the amount of time, in seconds, to wait for a <b>ping</b> response before the package is considered down. The time-out parameter must be several times more than the frequency parameter to ensure that enough <b>pings</b> are attempted.
	IP Address for Watchdog Target	Specify the IP address of the management VNI to <b>ping</b> .

6. Click **Next** to display the Network Interface Preferences page.

The available virtual machine network interfaces appear under **Available Virtual Machine Network Interfaces**.

**Figure 5-3. Adding a Management Interface**



7. Configure the management interface as described in the following table.

---

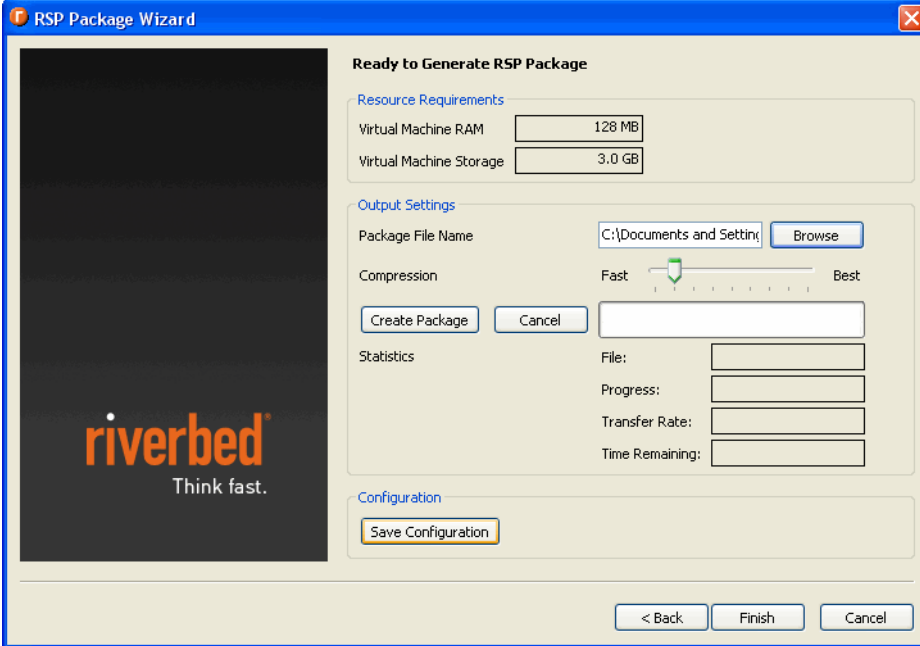
**Note:** For the Windows Server package creation, you do not need to configure optimization interfaces.

---

Field	Description
Management Interface	<p><b>Add.</b> Displays the Add Management Interface dialog box.</p> <ul style="list-style-type: none"> <li>Enter the interface name. This name appears in the Management Console GUI as the virtual network interface (VNI) name. The name must have between 1 and 30 alphanumeric characters (0-9, a-z, A-Z), spaces, dashes (-), and underscores (_).</li> <li>Select an available virtual interface from the Virtual Machine Network Interfaces list and click <b>OK</b>. The virtual interface is removed from Available Virtual Machine Network Interfaces list.</li> </ul> <p><b>Edit.</b> Select a Management Interface and click <b>Edit</b> to modify the Management Interface.</p> <p><b>Delete.</b> Select a Management Interface and click <b>Delete</b> to remove the Management Interface. The virtual interface is displayed under the Available Virtual Machine Network Interfaces list.</p>
Available Virtual Machine Network Interfaces	Lists available virtual machine network interfaces.

- Click **Next** to display the Ready to Generate RSP Package page.

**Figure 5-4. Ready to Generate RSP Package Page**



- Click **Browse** to locate the folder in which to store the RSP package.
- Enter a name for the RSP package or select an existing file (the file is overwritten). Do not include spaces in the filename. Riverbed recommends the extension **.pkg**.
- Under Compression, set the compression level:
  - Fast.** This is the lowest compression level, providing the fastest compression. However, the file size is larger than files compressed at higher compression levels.
  - Best.** This is the highest compression level, providing the smallest file size. However, it can be much slower than files compressed at lower compression levels.
- Click **Create Package**. As the Riverbed Package Generator Wizard creates the RSP package, it displays the package creation progress under Statistics:
  - File.** The name of the file currently compressed.
  - Progress.** The amount (in megabytes) processed and the total size of the archive.
  - Transfer Rate.** The speed at which input files are read and compressed.
  - Time Remaining.** Approximate amount of time remaining to complete the process. The amount of time varies, depending on the input data.
- Under Configuration, click **Save Configuration** to permanently save the configuration.
- Click **Finish** to close the Package Generator Wizard.
- Upload the RSP package to an **ftp** or **scp** server. You can also use an **HTTP** server or a laptop if your RSP package is not larger than 2 GB.

You are now ready to install the RSP Package on the Steelhead appliance.

To install and configure RSP using the Management Console, see [Chapter 2, “Installing and Configuring RSP Using the Management Console”](#). To install and configure RSP using the CLI, see [Chapter 3, “Installing and Configuring RSP Using the CLI”](#).

## Troubleshooting Error Messages

The following table lists and describes the Package Generator Wizard error messages. It also provides a recommendation to work around the error.

Error Message	Description
Unable to open the VMware virtual machine. Virtual hardware version of disk connected to <b>scsi0:0</b> is <b>9</b> . RiOS platform supports virtual hardware version <b>4, 6, 7, and 8</b> . Please use VMware Server v2.0 when creating a virtual machine.	The disk image was created with an unsupported version of VMware.  Recommendation: Use VMware Server v2.0, VMware ESX, or VMware Workstation to recreate the virtual machine and its corresponding disk image.
Unable to open the VMware virtual machine. Found virtual CD/DVD-ROM device connected to <b>ide0:0</b> . Virtual CD/DVD-ROM devices are not supported on the RiOS platform.	Virtual machine was configured with a virtual CD-ROM. RSP does not support this configuration.  Recommendation: Remove CD-ROM device from the virtual machine.
Unable to open the VMware virtual machine. The virtual disk that is connected to <b>ide0:0</b> points to a disk image outside the VM directory.	The disk image is not inside the virtual machine directory. RSP does not support this configuration.  Recommendation: Configure the virtual machine so that the virtual disk file is inside the virtual machine directory.
Unable to open the VMware virtual machine. The virtual machine was configured with a virtual floppy drive. Virtual floppy drives are not supported on the RiOS platform.	The virtual machine was configured with a virtual floppy drive. RSP does not support this configuration.  Recommendation: Remove floppy drive from the virtual machine.
Unable to open the VMware virtual machine. Unable to determine the hardware version of the virtual disk connected to <b>ide0:0</b> . Verify that the disk image exists in the VM directory. Also, try using VMware Server v2.0 to create the virtual machine.	Either the virtual machine contains a corrupted disk image, the disk image format is not recognized, or the disk image was deleted after the virtual machine was created.  Recommendation: Use VMware Server v2.0, VMware ESX, or VMware Workstation to re-create the virtual machine and its corresponding disk image.
Unable to open the VMware virtual machine. The virtual disk connected to <b>ide0:0</b> is not pointing to the disk image file.	The virtual machine contains a corrupted <b>.vmtx</b> file.  Recommendation: Use VMware Server v2.0, VMware ESX, or VMware Workstation to recreate the virtual machine and its corresponding disk image.
Unable to open the VMware virtual machine. The virtual disk connected to <b>ide0:0</b> has to be pre-allocated. Growing virtual disks are not supported on the RiOS platform.	The virtual machine was configured with the growing disk image functionality. RSP does not support this feature.  Recommendation: Configure the virtual machine with a pre-allocated disk image size.



# Acronyms and Abbreviations

**AAA.** Authentication, Authorization, and Accounting.

**ACL.** Access Control List.

**ACK.** Acknowledgment Code.

**ACS.** (Cisco) Access Control Server.

**AD.** Active Directory.

**ADS.** Active Directory Services.

**AES.** Advanced Encryption Standard.

**APT.** Advanced Packaging Tool.

**AR.** Asymmetric Routing.

**ARP.** Address Resolution Protocol.

**BDP.** Bandwidth-Delay Product.

**BW.** Bandwidth.

**CA.** Certificate Authority.

**CAD.** Computer Aided Design.

**CDP.** Cisco Discovery Protocol.

**CHD.** Computed Historical Data.

**CIFS.** Common Internet File System.

**CLI.** Command-Line Interface.

**CMC.** Central Management Console.

**CPU.** Central Processing Unit.

## Acronyms and Abbreviations

**CRM.** Customer Relationship Management.

**CSR.** Certificate Signing Request.

**CSV.** Comma-Separated Value.

**DC.** Domain Controller.

**DES.** Data Encryption Standard.

**DID.** Deployment ID.

**DMZ.** Demilitarized Zone.

**DER.** Distinguished Encoding Rules.

**DES.** Data Encryption Standard.

**DHCP.** Dynamic Host Configuration Protocol.

**DNS.** Domain Name Service.

**DR.** Data Replication.

**DSA.** Digital Signature Algorithm.

**DSCP.** Differentiated Services Code Point.

**ECC.** Error-Correcting Code.

**ERP.** Enterprise Resource Planning.

**ESD.** Electrostatic Discharge.

**FDDI.** Fiber Distributed Data Interface.

**FIFO.** First in First Out.

**FIPS.** Federal Information Processing Standards.

**FSID.** File System ID.

**FTP.** File Transfer Protocol.

**GB.** Gigabytes.

**GMT.** Greenwich Mean Time.

**GRE.** Generic Routing Encapsulation.

**GUI.** Graphical User Interface.

**HFSC.** Hierarchical Fair Service Curve.

**HSRP.** Hot Standby Routing Protocol.

**HSTCP.** High-Speed Transmission Control Protocol.

**HTTP.** HyperText Transport Protocol.

**HTTPS.** HyperText Transport Protocol Secure.

**ICA.** Independent Computing Architecture.

**ICMP.** Internet Control Message Protocol.

**ID.** Identification Number.

**IETF.** Internet Engineering Task Force.

**IGP.** Interior Gateway Protocol.

**IOS.** (Cisco) Internetwork Operating System.

**IKE.** Internet Key Exchange.

**IP.** Internet Protocol.

**IPMI.** Intelligent Platform Management Interface.

**IPSec.** Internet Protocol Security Protocol.

**ISL.** InterSwitch Link. Also known as Cisco InterSwitch Link Protocol.

**L2.** Layer-2.

**L4.** Layer-4.

**LAN.** Local Area Network.

**LED.** Light-Emitting Diode.

**LRU.** Least Recently Used.

**LZ.** Lempel-Ziv.

**MAC.** Media Access Control.

**MAPI.** Messaging Application Protocol Interface.

**MDI, MDI-X.** Medium Dependent Interface-Crossover.

**MEISI.** Microsoft Exchange Information Store Interface.

**MIB.** Management Information Base.

**MOTD.** Message of the Day.

## Acronyms and Abbreviations

**MS GPO.** Microsoft Group Policy Object.

**MS SMS.** Microsoft Systems Management Server.

**MS-SQL.** Microsoft Structured Query Language.

**MSFC.** Multilayer Switch Feature Card.

**MSI Package.** Microsoft Installer Package.

**MTU.** Maximum Transmission Unit.

**MX-TCP.** Max-Speed TCP.

**NAS.** Network Attached Storage.

**NAT.** Network Address Translate.

**NFS.** Network File System.

**NIS.** Network Information Services.

**NSPI.** Name Service Provider Interface.

**NTLM.** Windows NT LAN Manager.

**NTP.** Network Time Protocol.

**OSI.** Open System Interconnection.

**OSPF.** Open Shortest Path First.

**PAP.** Password Authentication Protocol.

**PBR.** Policy-Based Routing.

**PCI.** Peripheral Component Interconnect.

**PEM.** Privacy Enhanced Mail.

**PFS.** Proxy File Service.

**PKCS12.** Public Key Cryptography Standard #12.

**PRTG.** Paessler Router Traffic Grapher.

**PSU.** Power Supply Unit.

**QoS.** Quality of Service.

**RADIUS.** Remote Authentication Dial-In User Service.

**RAID.** Redundant Array of Independent Disks.

**RCU.** Riverbed Copy Utility.

**ROFS.** Read-Only File System.

**RPC.** Remote Procedure Call.

**RSA.** Rivest-Shamir-Adleman Encryption Method by RSA Security.

**RSP.** Riverbed Services Platform.

**SA.** Security Association.

**SAP.** System Application Program.

**SCP.** Secure Copy Program.

**SCPS.** Space Communications Protocol Standards.

**SDR.** Scalable Data Referencing.

**SEL.** System Event Log.

**SFQ.** Stochastic Fairness Queuing.

**SMB.** Server Message Block.

**SMI.** Structure of Management Information.

**SMTP.** Simple Mail Transfer Protocol.

**SNMP.** Simple Network Management Protocol.

**SPAN.** Switched Port Analyzer.

**SQL.** Structured Query Language.

**SSH.** Secure Shell.

**SSL.** Secure Sockets Layer.

**SYN.** Synchronize.

**SYN/ACK.** Synchronize/Acknowledgement.

**TA.** Transaction Acceleration.

**TACACS+.** Terminal Access Controller Access Control System.

**TCP.** Transmission Control Protocol.

**TCP/IP.** Transmission Control Protocol/Internet Protocol.

**TP.** Transaction Prediction.

## Acronyms and Abbreviations

**TTL.** Time to Live.

**ToS.** Type of Service.

**U.** Unit.

**UDP.** User Datagram Protocol.

**UNC.** Universal Naming Convention.

**URL.** Uniform Resource Locator.

**UTC.** Universal Time Code.

**VGA.** Video Graphics Array.

**VLAN.** Virtual Local Area Network.

**VoIP.** Voice over IP.

**VWE.** Virtual Window Expansion.

**WAN.** Wide Area Network.

**WCCP.** Web Cache Communication Protocol.

**XOR.** Exclusive OR logic.

# Glossary

**Acceleration Policy.** An acceleration policy contains optimization rules for accelerating the WAN traffic for endpoint clients. An acceleration policy is required for optimization to occur.

**ACK.** A packet message used in the TCP to acknowledge receipt of a packet.

**ARP.** Address Resolution Protocol. An IP protocol used to obtain a node's physical address.

**Assignment.** An assignment occurs when an endpoint or an acceleration policy is matched to a deployment ID (DID).

**Bandwidth.** The upper limit on the amount of data, typically in kilobits per second (kbps), that can pass through a network connection. Greater bandwidth indicates faster data transfer capability.

**Bit.** A Binary digit. The smallest unit of information handled by a computer; either 1 or 0 in the binary number system.

**Blade.** One component in a system designed to accept some number of components (blades).

**Bridge.** Device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame.

**Cache.** A temporary storage area for frequently or recently accessed data.

**CIFS.** Common Internet File System. CIFS is the remote file system access protocol used by Windows servers and clients to share files across the network.

**Correct Addressing.** A packet addressing method in which the source IP addresses and port numbers are used in the header fields.

**Database Cursor.** A record pointer in a database. When a database file is selected and the cursor is opened, the cursor points to the first record in the file. Using various commands, the cursor can be moved forward, backward, to top of file, bottom of file, and so forth.

**Deduplication.** A method of reducing storage space by eliminating redundant data. It stores only one unique instance of the data. It replaces redundant data with a pointer to the unique data copy.

**Deduplication factor.** The ratio of expanded bytes to the deduplicated bytes of the volume.

**Default Gateway.** The default address of a network or Web site. It provides a single domain name and point of entry to the network or site.

**Deployment ID.** The deployment ID (DID) is used to apply policies and policy updates to groups of endpoint clients. The DID is associated with the endpoint client upon installation of a MSI package. The Steelhead Mobile Controller uses the DID to identify the client and provide their assigned policies and policy updates.

**DHCP.** Dynamic Host Configuration Protocol. Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network.

**DMZ.** Demilitarized Zone. A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and DNS servers.

**DNS.** Domain Name Service. A system used in the Internet for translating names of network nodes into IP addresses. A Domain Name Server notifies hosts of other host IP addresses, associating host names with IP addresses.

**Domain.** In the Internet, a portion of the Domain Name Service (DNS) that refers to groupings of networks based on the type of organization or geography.

**Endpoint.** An endpoint is a client computer. For example, a PC or laptop.

**Endpoint Policy.** An endpoint policy specifies machine-specific software settings for endpoint clients, such as the data store size. An endpoint policy is required for optimization to occur.

**Ethernet.** The most widely used Local Area Network (LAN) access method.

**Fat Client.** A client computer which provides large size applications independently of the central server.

**FDDI.** Fiber Distributed Data Interface. A set of American National Standards Institute (ANSI) protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for Wide Area Networks (WANs).

**File Cluster.** Two or more filers that provide high availability and load balancing.

**Filer.** An appliance that attaches to a computer network and is used for data storage.

**Full Address Transparency.** A packet addressing method in which the client and server IP addresses and port numbers are used in the header fields.

**Gateway.** A computer that acts as an intermediate device for two or more networks that use the same protocols. The gateway functions as an entry and exit point to the network. Transport protocol conversion might not be required, but some form of processing is typically performed.

**Gigabit Ethernet.** An Ethernet technology that raises transmission speed to 1 Gbps (1000 Mbps).

**Hashing.** Producing hash values for accessing data or for security. A hash value is a number generated from a string of text. The hash is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text produces the same hash value.



**Heartbeat.** A repeating signal transmitted from one appliance to another to indicate that the appliance is operating.

**Heuristic.** A method of problem solving using exploration and trial and error methods. Heuristic program design provides a framework for solving the problem in contrast with a fixed set of algorithmic rules that cannot vary.

**Host.** A computer or other computing device that resides on a network.

**Host address.** The IP address assigned to each computer attached to the network.

**Host name.** Name given to a computer, usually by DNS.

**HSRP.** Hot Standby Routing Protocol. HSRP is a routing protocol from Cisco that provides backup to a router in the event of failure. Using HSRP, several routers are connected to the same segment of an Ethernet, FDDIs or token-ring network and work together to present the appearance of a single virtual router on the LAN. The routers share the same IP and MAC addresses, therefore in the event of failure of one router, the hosts on the LAN are able to continue forwarding packets to a consistent IP and MAC address. The process of transferring the routing responsibilities from one device to another is transparent to the user.

**HTTP.** Hypertext Transport Protocol. The protocol used by Web browsers to communicate with Web servers.

**HTTPS.** Hypertext Transport Protocol Secure. The protocol for accessing a secure Web server. Using HTTPS directs the message to a secure port number to be managed by a security protocol.

**Interface.** The point at which a connection is made between two elements, systems, or devices so that they can communicate with one another.

**Internet.** The collection of networks tied together to provide a global network that use the TCP/IP suite of protocols.

**IP.** Internet Protocol. Network layer protocol in the TCP/IP stack that enables a connectionless internetwork service.

**IP address.** In IP version 4 (IPv4), a 32-bit address assigned to hosts using the IP protocol. Also called an Internet address.

**IPsec.** Internet Protocol Security protocol. A set of protocols to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. For IPsec to work, the sending and receiving devices must share a public key.

**Kerberos.** A computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner.

**Latency.** Delay between a request being issued and its response being received.

**Layer 2.** The communications protocol (called the data link layer or MAC layer) that contains the physical address of a client or server inspected by a bridge or switch. Layer 2 processing is faster than layer 3 processing, because less analysis of the packet is required.

**Layer 3.** The communications protocol (called the network layer) that contains the logical address of a client or server station that is inspected by a router which in turn forwards it through the network. Layer 3 contains a type field so that traffic can be prioritized and forwarded based on message type as well as network destination. The IP network layer (Layer 3) accepts packets from the TCP or UDP transport layer (Layer 4), adds its own header and delivers a datagram to the data link layer protocol (Layer 2).

**Layer-4.** A communications protocol (called the transport layer) responsible for establishing a connection and ensuring that all data has arrived safely. The application delivers its data to the communications system by passing a stream of data bytes to the transport layer along with the socket (the IP address of the station and a port number) of the destination machine.

**MAC address.** Unique serial number or physical station address burned into Ethernet and Token Ring adapters to identify that network card from all others.

**MAPI.** Messaging API. A programming interface from Microsoft that enables a client application to send and receive mail from Exchange Server or a Microsoft Mail (MS Mail) messaging system. Microsoft applications such as Outlook, the Exchange client, and Microsoft Schedule use MAPI.

**Microsoft Exchange.** Messaging and groupware software for Windows from Microsoft. The Exchange server is an Internet-compliant messaging system that runs under Windows systems and can be accessed by Web browsers, the Windows In-box, Exchange client, or Outlook. The Exchange server is also a storage system that can hold anything that needs to be shared.

**MSI Package.** An MSI package is the Microsoft Software Installer (MSI) used to install Mobile Client software onto endpoint clients.

**Multiprotocol Filer.** Filer that supports both the NFS and CIFS protocols.

**Netmask.** A 32-bit mask which shows how an Internet address is divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are used for the network and subnet parts, and zeros for the host part. The mask must contain at least the standard network portion (as determined by the class of the address), and the subnet field should be contiguous with the network portion.

**Neural Network.** A modeling technique based on the observed behavior of biological neurons and used to mimic the performance of a system. It consists of a set of elements that start out connected in a random pattern, and, based upon operational feedback, are molded into the pattern required to generate the required results. It is used in applications such as robotics, diagnosing, forecasting, image processing, and pattern recognition.

**NFS.** Network File System. The file sharing protocol in a UNIX network.

**NIS.** Network Information Services. A naming service that allows resources to be easily added, deleted, or relocated.

**Opportunistic Lock.** Also known as oplock. A lock requested by a client on a file that resides on a remote server. To prevent any compromise to data integrity, the Steelhead appliance only optimizes data where exclusive access is available (in other words, when locks are granted). When an oplock is not available, the Steelhead appliance does not perform application-level latency optimizations but still performs Scalable Data Referencing and compression on the data as well as TCP optimizations. Therefore, even without the benefits of latency optimization, Steelhead appliances still increase WAN performance, but not as effectively as when application optimizations are available.

**OSPF.** Open Shortest Path First. An interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (which keeps track of routes to particular network destinations) that describes the state of its own links. It also sends the complete routing structure (topography).

**Packet.** A unit of information transmitted, as a whole, from one device to another on a network.

**Policy.** Routing and Quality of Service (QoS) scheme that forwards data packets to network interfaces based on user-configured parameters.

**Port.** A pathway into and out of the computer or a network device such as a hub, switch, or router. On network devices, the ports are for communications, typically connecting Ethernet cables or other network devices.

**Port Transparency.** A packet addressing method in which the server port number is used in the header fields.

**Probe.** A small utility program that is used to investigate, or test, the status of a system, network, or Web site.

**Proxy.** An entity that acts on behalf of a network client. In a network, a client is an entity that makes a network request and a server is an entity that responds to the request. For example, your Web browser is a client which requests Web content from a Web server. A proxy can take the place of the client, meaning the client never communicates directly with the server. Instead, the client makes a connection to the proxy and the proxy makes the connection to the server, receives any responses from the server, and relays them back to the client.

**Router.** A device that forwards data packets from one LAN or WAN to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Routers work at Layer-3 in the protocol stack, whereas bridges and switches work at Layer-2.

**SDR.** Scalable Data Referencing. Process that uses a proprietary algorithm to divide data into small chunks, then references and stores the data chunks on the Steelhead appliance.

**Server Virtualization.** Process that uses multiple virtual filers on a single filer hardware.

**Share.** Mechanism of making a directory on a volume an IP network entity. Clients connect to shares. A share can point to any directory, even the root directory. A volume can have many shares. A share can point only to one directory in a volume. A share is not a storage management entity.

**SMB.** Server Message Block. A message format used by DOS and Windows to share files, directories, and devices. There are also a number of products that use SMB to enable file sharing among different operating system platforms. A product called Samba, for example, enables UNIX and Windows machines to share directories and files.

**SNMP.** Simple Network Management Protocol. A network protocol that provides a way to monitor network devices, performance, security, and manages configurations and collects statistics.

**SPAN.** Switched Port Analyzer. A method of monitoring network traffic. SPAN is also called port mirroring. If SPAN is enabled, the switch sends a copy of all network packets seen on one port (or the entire VLAN) to another port, where the packet can be analyzed.

**Socket.** The method of directing data to the appropriate application in a TCP/IP network. A socket is made up of the IP address of the station and a port number.

**Spanning Tree Protocol.** An OSI layer-2 protocol that ensures a loop-free topology for a bridged LAN.

**Switch.** A network device that filters and forwards frames based on the destination address of each frame. The switch operates at Layer-2 (data link layer) of the Open System Interconnection (OSI) model.

**SYN.** A synchronize packet in TCP.

**SYN-ACK.** To establish a connection TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to a port to open it for connections (a passive open). After the passive open is established, a client can initiate an active open. To establish a connection, the three-way handshake occurs: 1) the active open is performed by the client sending a SYN to the server, 2) in response, the server replies with a SYN-ACK, 3) finally, the client sends an ACK back to the server.

**TCP.** Transmission Control Protocol. The error correcting Transport layer (Layer-4) in the TCP/IP protocol suite.

**TCP/IP.** Transmission Control Protocol/Internet Protocol. The protocol suite used in the Internet, intranets, and extranets. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. TCP/IP is a routable protocol, and the IP part of TCP/IP provides this capability.

**Throttle.** To adjust the CPU speed.

**VIF.** Virtual Interface. A logical interface created for the physical interface. Like a physical Ethernet interface, each VIF can have multiple addresses assigned to it.

**VLAN.** Virtual Local Area Network. A VLAN is an administratively configured LAN or broadcast domain. Instead of going to the wiring closet to move a cable to a different LAN, network administrators can remotely configure a port on an 802.1Q-compliant switch to belong to a different VLAN. A 802.1Q VLAN enables network administrators to move end stations to different broadcast domains by setting membership profiles for each port on centrally managed switches.

**Virtual Filer.** Independent network entity that has its own set of IP addresses and routing tables, DNS names, and domain membership.

**Virtual Server.** Network entity that uses its own name and IP address to serve data just like a physical server. It mounts volumes from external filers and exports shares that you can mount and access. Multiple virtual servers can share physical resources and run concurrently on the same appliance.

**Volume.** A partition on the filer disk. A volume is not an IP network entity; you cannot ping or connect to a volume. Volumes belong to virtual servers. The volume administrator can create shares for various directories on the volume. Volumes contain shares you can export and access. When a virtual server fails over to another filer, volumes follow the virtual server.

**WAN Visibility Mode.** Pertains to how packets traversing the WAN are addressed.

**XOR.** Exclusive OR logic or exclusive disjunction logic. It yields true if exactly one (but not both) of two conditions is true. XOR hardware logic is used in RAID engines designed to perform complex parity calculations.

# Index

## A

Alarm thresholds, setting 32

## B

Basic steps for creating an RSP package 65

Basic steps for installing and configuring RSP 37

## D

DNAT rules, overview of 16

Documentation, contacting 9

## F

Fail-to-block, enabling on an interface 54

Fail-to-bypass, disabling on an interface 54

## I

In-band hybrid packages, overview of 13

In-band LAN packages, overview of 13

In-band packages, overview of 13

In-band WAN packages, overview of 13

IP address, configuring on an RSP Windows Server package 47

## K

Knowledge Base, accessing 8

## M

Management VNIs, overview of 15

Memory footprint in RSP 34

## O

Online documentation, accessing 8

Online notes 8

Optimization VNIs, overview of 15

Out-of-band packages, overview of 14

## P

Package

adding to a slot 23

removing from RSP 23

Primary interface

bridging a management VNI to 30

Professional services, contacting 9

## R

Related reading 8

Release notes 8

Reports

RSP 35

Riverbed Package Generator Wizard 64, 72

## RSP

basic steps for installing and configuring 37

configuring 37

configuring services on a virtual machine 71

converting the virtual machine into an RSP package 72

creating a virtual machine 67

downloading the RSP image 40, 43

enabling a named-pipe serial support on a virtual machine 72

hardware and software

dependencies 6

image versions 12

image, installing 39

image, prerequisites for installing 39

installing 37

installing from local file 21

installing from pre-uploaded image 21

installing VMware Tools onto a virtual machine 70

installing Windows Server onto a virtual machine 69

launching a VM console 57

overview of 11

package watchdog 34

partition, requirements for 7

reconfiguring the virtual machine for 71

rules 27

service license for 39

slot, overview of 14

statistics for all optimization VNIs 51

Steelhead appliance models that support 6

types of services provided 12

VNI IO report 35

VNI rules, default settings 16

VNI rules, overview of 16

## RSP packages

configuring a watchdog for 53

configuring an IP address for Windows Server 47

creating, hardware and software dependencies 64

## Index

- creating, overview of 64
- deleting installation files 46
- obtaining 42
- overview of 13
- renaming 46
- uninstalling from a slot 46

## S

### Setting

- alarm thresholds 32

### Slots

- adding 23

## T

- Technical support, contacting 9

## V

### Virtual machine

- configuring services on the 71
- converting into an RSP package 72
- creating 67
- creating, prerequisites for 66
- enabling a named-pipe serial support on the 72
- installing VMware Tools onto the 70
- installing Windows Server onto the 69
- reconfiguring for RSP 71

### VLAN

- setting a tag for a VNI 31

### VM console 34

### VM package in RSP 13

### VMware Server, overview of 12

### VNI rules 27

- default settings 16
- example of 16
- overview of 16

### VNIs

- adding rules to 49
- bridging to an interface 50
- DNAT rules for 15
- in-path rules for 15
- management, overview of 15
- mirror, overview of 15
- optimization, overview of 15
- overview of 15
- updating VLAN settings for 52
- virtual-in-path, overview of 15

## W

### Watchdog

- configuring 53
- configuring an email alert 55
- configuring fail-to-block for 54
- default setting for 17

### Watchdog for RSP package 34