

# PacketShaper Release Notes

PacketWise Version 9.2.6

June, 2014

**BLUE COAT**

P/N 20-0260-926 Revision A

---

© 2014 Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUGH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, technical services, and any other technical data referenced in this document are subject to U.S. export control AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

SNMP Research SNMP Agent Resident Module Version 14.2.1.7. Copyright 1989-1997 SNMP Research, Inc.

This product includes software developed by the University of California, Berkeley and its contributors. Portions Copyright © 1982, 1983, 1986, 1989, 1990, 1993 by The Regents of the University of California. All rights reserved.

Portions Copyright © 1996 by Internet Software Consortium.

Portions Copyright © 1993 by Digital Equipment Corporation.

Portions Copyright © 1990 by Regents of the University of Michigan. All rights reserved.

This product includes software developed by the University of California, Berkeley and its contributors. Portions Copyright © 2001 Mike Barcroft. Portions Copyright © 1990, 1993 by The Regents of the University of California. All rights reserved.

This product incorporates software for zipping and unzipping files.

UnZip 5.42 of 14 January 2001, by Info-ZIP.

Zip 2.3 (November 29th 1999).

Copyright © 1990-1999 Info-ZIP

Portions copyright 1994, 1995, 1996, 1997, 1998, by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health. Portions copyright 1996, 1997, 1998, by Boutell.Com, Inc. GIF decompression code copyright 1990, 1991, 1993, by David Koblas (koblas@netcom.com). Non-LZW-based GIF compression code copyright 1998, by Hutchison Avenue Software Corporation (<http://www.hasc.com/>, [info@hasc.com](mailto:info@hasc.com)).

Portions Copyright © 2006 Narciso Jaramillo. <nj\_flex@rictus.com>

TACACS+ software Copyright 2000,2001 by Roman Volkov.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

Fisheye Component v0.1 Copyright © 2006 by Ely Greenfield

ActionScript Library 3.0 (as3corelib v0.9) BSD 2.0 Copyright © 2008, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of California, Berkeley nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

## U.S. Government Restricted Rights

Blue Coat software comprises “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212 (SEPT 1995) and is provided to the United States Government (i) for acquisition by or on behalf of civilian agencies, consistent with the policy set forth in 48 C.F.R. 12.212; or (ii) for acquisition by or on behalf of units of the Department of Defense, consistent with the policies set forth in 48 C.F.R. 227-7202-1 (JUN 1995) and 227.7202-3 (JUN 1995). Blue Coat software is provided with “RESTRICTED RIGHTS.” Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR 52.227-14 and DFAR 252.227-7013 et seq. or their successors. Use of Blue Coat products or software by the U.S. Government constitutes acknowledgment of Blue Coat’s proprietary rights in them and to the maximum extent possible under federal law, the U.S. Government shall be bound by the terms and conditions set forth in Blue Coat’s end user agreement.

---

---

**Blue Coat Systems, Inc.**

420 N. Mary Avenue

Sunnyvale, CA 94085

<http://www.bluecoat.com>

**Revision History**

November, 2012	PacketWise 9.2.1
July, 2013	PacketWise 9.2.2
August, 2013	PacketWise 9.2.3
February, 2014	PacketWise 9.2.4
April, 2014	PacketWise 9.2.5
June, 2014	PacketWise 9.2.6


---

## Introduction

These release notes include the changes to PacketWise 9.2.6 only. If you are upgrading from an earlier version of PacketWise, you can learn about other new features and software changes by consulting the release notes for the versions between your current software and v9.2.6.

Acrobat PDF files of all versions of release notes are available in the Documents section of each PacketGuide version:

<https://bto.bluecoat.com/packetguide/version.htm>

 **Note:** This document reflects current information at the time the release notes were finalized. The Blue Coat support website may contain additional late-breaking information: <http://bluecoat.com/support>

See the following sections for specific information:

Automatic Notification of New Software Releases .....	page 2
What's New in PacketWise 9.2.6.....	page 3
Resolved Issues in PacketWise 9.2.6 .....	page 4
Backing Up Software Configurations .....	page 5
Upgrading to PacketWise 9.2.6.....	page 10
Known Issues in PacketWise 9.2.6 .....	page 16
Known Issues in Xpress.....	page 22
Additional Information for PacketWise 9.2 .....	page 23
Additional Information for Xpress .....	page 24

---

## Automatic Notification of New Software Releases

To be automatically notified when new PacketShaper software releases are available, you can subscribe to the PacketShaper product channel in the Knowledge Base:

1. Log in to the BTO Knowledge Base (<https://kb.bluecoat.com>).
2. In the Knowledge Base, go to: **Product Information > Products > PacketShaper**  
[https://kb.bluecoat.com/index?page=content&cat=PACKETSHAPER&channel=PRODUCT\\_INFORMATION](https://kb.bluecoat.com/index?page=content&cat=PACKETSHAPER&channel=PRODUCT_INFORMATION)
3. Click **Subscribe**.


You will then receive email messages to let you know when new software releases are available for download. Click the link in the email to view the KB article. The article will provide you with the following types of information for the new release: the release number, the date the software was posted, highlights of the release, and links to release notes and other related documentation and training materials.

---

## What's New in PacketWise 9.2.6

This section describes the new features in PacketWise 9.2.6. For more information, see PacketGuide at:

<https://bto.bluecoat.com/packetguide/9.2/index.htm>

 **Note:** It's very important to back up your configuration before upgrading to PacketWise 9.2.6. This has always been a recommended best practice when upgrading to a new release.

### Ability to Load External SSL Certificate

The new **setup https load** CLI command allows you to load an external SSL certificate to use for secure access to the browser interface.

```
setup https load <cert_file> [<key_file>]
```

where <cert\_file> is the filename containing the certificate (and possibly the private key). If the private key is in a separate file, you must also specify the <key\_file> filename of the RSA private key.

 **Note:** You must FTP the file(s) to the PacketShaper before issuing the **setup https load** command.

PacketShaper supports only one certificate. Loading a new certificate will replace the existing certificate. Certificate and key files must be in PEM-encoded format. Certificates must be in X.509 format and keys must be in OpenSSL RSA format. If the certificate and key are in the same file, .pkcs12 format is not supported.

If you later downgrade to a previous PacketWise version, an SSL certificate you imported in PacketWise 9.2.6 will be retained.

### Default Values Changed for SSH and SSL Keys


The default key size for SSH key generation is now 2048 bits. To generate 2048-bit SSH key pairs, use the **setup ssh keygen** CLI command.

In addition, self-signed SSL certificate generation now uses 2048-bit keys instead of 1024-bit. To use the new key size, you need to generate an SSL certificate with the **setup https certificate** command.

If you downgrade to a previous PacketWise version, any 2048-bit SSL and SSH keys you generated in PacketWise 9.2.6 will be retained.

### Command Introduced to Reset Schedule Counters

A new CLI command in PacketWise 9.2.6 zeros out the counters for all command schedules configured on the PacketShaper. The counters keep track of the number of times each schedule has been executed since it was created. Use the **schedule reset-counter** command to reset the counters to zero (for example, after resetting the appliance).

 **Note:** Prior to PacketWise 9.1.3, schedule counters were automatically reset to zero after each reboot of the PacketShaper. In PacketWise 9.1.3 and higher, counters accumulate since the schedule was created, not since the appliance was rebooted.

---

## Resolved Issues in PacketWise 9.2.6

The following issues, discovered in previous versions, have been fixed in PacketWise 9.2.6.

- Starting in PacketWise 9.1.3, schedule counters were not reset to zero after the PacketShaper was rebooted. To give users the ability to reset the counters on demand, a new CLI command is offered in PacketWise 9.2.6. See “Command Introduced to Reset Schedule Counters” on page 3. [SR 2-650548912]
- Fixed additional reasons for URL categories not being discovered from SSL traffic.
- PacketShaper sends SNMP traps and syslog alerts (if configured) when a flow matches a Flow Quota based class. When subsequent flows match the same class, PacketShaper no longer sends duplicate traps and alerts.


---

## Backing Up Software Configurations

### Overview

**Important:** Before upgrading to PacketWise 9.2.6, it is imperative to back up your configuration. You may need to use these backup files in case your configuration doesn't load properly after installing the new software or if you decide to revert back to the older version.

For instructions, see the following sections "How Do I Save My Settings?" and "How Do I Back Up Configurations?"

 **Note:** If you are using PolicyCenter, follow the backup instructions in PolicyCenter 9.2.6 Release Notes. In addition, make sure to upgrade to PolicyCenter 9.2.6 before installing PacketWise 9.2.6 on your PacketShapers.

### How Do I Save My Settings?


#### Option 1

Use the **config save** CLI command to save the current configuration's sharable settings in an .ldi file and its nonsharable settings in a .cmd file. The .ldi file contains the traffic tree configuration (including all classes, class IDs, partitions, policies, host lists, and events), as well as all sharable configuration settings, such as packet shaping, traffic discovery, passwords, SNMP, email, SNTP, compression, and Syslog. The .cmd file contains the unit's IP address, gateway, DNS servers, timezone, NIC speed, and other non-shareable settings. If you ever need to restore the configuration, you can issue the **config load** command to load these saved settings.

To save your configuration:

```
config save <filename>
```

where <filename> is the name of the configuration file (such as myconfig). The .ldi and .cmd files (for example, myconfig.ldi and myconfig.cmd) are automatically created in the 9.256/ volume (system disk).

 **Note:** Do not confuse the **config save** .cmd file with the one created using **setup capture** (Option 2 below). The **setup capture** command file is an executable file that contains all the PacketShaper settings; the **config save** command file contains only the non-shareable settings.

#### Option 2

In addition, PacketWise offers a way to capture your traffic configuration and settings in an executable command (.cmd) file. First, use the **setup capture** command to create the command file. Then, if you want to restore the settings you captured, use the **run** command to re-create the configuration.

Note that restoring a configuration by running a command file takes much longer (possibly hours) than loading a configuration (less than a minute). However, Blue Coat recommends that you create and backup the command file as a safeguard in case the configuration fails to load.

To save your settings in a command file, use the following command:

```
setup capture complete <filename>
```

where <filename> is the name of the command file (such as backup.cmd). This file is automatically created in the 9.256/cmd directory.

This command file should be backed up along with your configuration .ldi and .cmd files.

### How Do I Back Up Configurations?

After saving and capturing the unit's configuration as described above, you should copy the configuration files (such as myconfig.ldi and myconfig.cmd) and the command file (such as backup.cmd) to a workstation's hard drive.

To transfer files from the PacketShaper to a workstation:



- 
1. At your workstation's command line, create a directory where the backup files will be stored.
  2. Go to the newly created directory and enter:

```
ftp <ipaddress>
```

where *<ipaddress>* is the PacketShaper's address (for example, *ftp 192.166.0.100*).

When you press Enter, the screen messages indicate that the connection has been made and that the server is ready.

3. Enter a user name (such as *touch*).
4. Enter the unit's *touch* password.
5. Go to the PacketShaper directory where you saved the configuration files. By default, they are saved on the system disk (9.256/).
6. To transfer the configuration files ( *.ldi* and *.cmd*) from the PacketShaper to your local drive, enter:

```
ascii (to go into ASCII mode)
```

```
get <filename>.ldi (where <filename> is the name of the file you saved with config save)
```

```
get <filename>.cmd (this is the .cmd created with config save, not setup capture)
```

7. To transfer the command file you captured with **setup capture**:

```
get <filename>.cmd (where <filename> is the file that was created with setup capture)
```

```
quit
```

## How Do I Restore Configurations?

In the event that your current software configuration becomes corrupt, use the following procedure to restore the unit to the configuration you saved:

1. At your workstation's command line, go to the directory where the backup files were stored.
2. FTP to the PacketShaper.
3. Enter a user name (such as *touch*).
4. Enter the unit's *touch* password.
5. To transfer the configuration files (*.ldi* and *.cmd*) from your workstation's drive to the PacketShaper's system disk, enter:

```
ascii (to go into ASCII mode)
```

```
put <filename>.ldi (where <filename> is the name of the file you saved with config save)
```

```
put <filename>.cmd
```

```
quit
```

6. To reset and load the new configuration, go to the PacketShaper's command-line interface, and type the following commands:

```
config reset
```

```
config load <filename>
```

7. If a configuration won't load or the traffic tree still isn't in place, you can restore the configuration by running the command file you backed up. For example, if you used the **setup capture** command and created a file named *backup.cmd*, you need to FTP the *backup.cmd* file to the PacketShaper and then type **run backup.cmd** at the CLI prompt.

## Reverting to a Backup Image

When you upgrade PacketWise, the newly-installed version becomes the main image, and the previous main image becomes the new backup image.

There are times when you may want to revert to your backup image (that is, replace the main image with the backup image):

- 
- After attempting to load a version of PacketWise that does not support your PacketShaper model.
  - After evaluating a new version of PacketWise, but before deploying the new version.
  - When you observe problems with your PacketShaper that began after loading a different version of PacketWise.

PacketWise offers two manual and one automatic method to revert to the backup image:

- Using the **image revert** command. (See “Revert to the Backup Image Using the CLI” on page 7.)
- Pressing **Ctrl+B** during the boot-up process. (See “Revert to the Backup Image by Pressing Ctrl+B” on page 8.)
- Automatic reversion when a unit repeatedly fails to boot. (See “Automatic Reversion to the Backup Image” on page 8.)

### Considerations When Downgrading

Here are some considerations when downgrading from PacketWise 9.2:

- Because PacketWise 9.x configurations are incompatible with 8.x versions, you must reset the configuration after downgrading to version 8.x. See “Special Procedure for Downgrading to PacketWise 8.x Versions” on page 8.
- There are several issues when downgrading from v9.2.2+ to v9.2.1. (See “Downgrade Issues” on page 16.) Because of these issues, it’s important to back up your configuration *before* upgrading from v9.2.1 to v9.2.2+; you can then load the backed up 9.2.1 configuration if you later decide to downgrade to v9.2.1.
- As is always the case, new features are not recognized by earlier versions. After downgrading, you may want to either load the pre-9.2 class tree that you backed up or delete the classes that use 9.2-specific matching rules. Note that a class with a user-based matching rule becomes a match-all class in pre-9.2 versions.
- Make sure you are aware of the minimum required version for your PacketShaper model:
  - The PacketShaper 12000 model requires 8.6.3 or higher and cannot be reverted to a pre-8.6.3 image.
  - The PacketShaper 10000 model (Revisions A-F) requires 7.0.0 or higher and thus cannot be reverted to a pre-7.0.0 image.
  - The PacketShaper 1700, 3500, 7500, and 10000 (Revision G or higher) models require 7.4 or higher and thus cannot be reverted to a pre-7.4 image.
  - The PacketShaper 900 model requires PacketWise 8.2.x and higher, and thus cannot be reverted to earlier versions.
- If you load any 9.2.x-specific plug-ins and then revert to a pre-9.2.x version, you will see the following error message: *Unknown local type 0 in <plug-in name>*. To eliminate this message, delete the incompatible plug-in file and reset the unit.
- See also “Downgrade Issues” on page 16.

### Clear the Browser Cache After Downgrading

Blue Coat recommends clearing the browser cache after downgrading from PacketWise 9.2 to earlier versions. See “Clear Browser Cache” on page 14 for instructions.

### Revert to the Backup Image Using the CLI

If your PacketShaper has successfully booted, you can revert to the backup image using the CLI:

1. At the command-line interface, revert to the backup image by entering:  
`image revert`
2. Reconnect to your PacketShaper, and wait at least one minute.

---

If the class tree disappeared during the reverting process, run the CMD file you had previously created before upgrading. For example, if you used the **setup capture** command and created a file named `backup.cmd`, you need to FTP the `backup.cmd` file to the PacketShaper and then type **run backup.cmd**. (To see if all the commands executed successfully, type **cat backup.out**.)

### Revert to the Backup Image by Pressing Ctrl+B

If you have attempted to load a version of PacketWise that is not supported by your hardware platform, such as version 8.6.2 on a PacketShaper 12000, your PacketShaper will not boot and will become inaccessible except by console connection. On models that have LCDs, the message `Loading...` will remain on the LCD panel.

To recover the unit, you need to revert to the backup image of PacketWise, which is the image previously installed on the unit before you loaded the unsupported image. The recovery procedure must be performed from a console connection:

1. Using the provided null-modem cable, attach a workstation or PC to the unit's port labeled **CONSOLE**. This cable offers both 9-pin and 25-pin connectors on each end.
2. Start your terminal emulation program (such as HyperTerminal).
3. Verify that you have configured the program with the following values to communicate with the unit's console serial port:
  - 9600 bps, 8 data bits, 1 stop bit, no parity, no flow control
  - If you are using a modem connected to the serial port, the modem must be set to: 9600 bps, 8 data bits, 1 stop bit, no parity, auto-answer (usually ATH1 in the standard Hayes command set), and DTR always on (usually a DIP switch setting). Check the modem manual for details.
4. Power cycle unit.
5. As the unit is attempting to boot, (the message `Loading...` appears on the LCD panel), press **Ctrl+B**. This forces the PacketShaper to reboot using its backup image.

### Automatic Reversion to the Backup Image

If a PacketShaper crashes eight consecutive times, it automatically reverts to the backup image and re-boots. This process can take 20-40 minutes, depending on the PacketShaper model.

### Special Procedure for Downgrading to PacketWise 8.x Versions

Because the 9.x configuration has been upgraded to accept 64-bit values, the 9.x configuration is incompatible with 8.x PacketWise versions. Therefore, if you decide to downgrade to 8.x versions, you must clear the 9.x configuration before loading the configuration you saved from the earlier version.

Follow these steps to downgrade from PacketWise 9.x to an 8.x version:

1. Access the PacketShaper CLI.
2. Save your 9.x configuration:

```
config save <filename>
```

3. If you have a 10,000 class ISP key, clear all the classes:

```
class reset
```

4. Revert to the backup image or load another image:

```
image revert
```

5. Reset the configuration:

```
config reset
```

6. Reset measurement data:

```
measure reset
```

- 
7. Load the 8.x configuration you saved before installing v9.x.

```
config load <filename>
```

---

## Upgrading to PacketWise 9.2.6

### Supported Hardware Platforms

PacketWise 9.2.6 is supported on the following PacketShaper models: 900, 1700, 3500, 7500, 10000, 12000.

PacketWise 9.2.6 is *not* supported on end-of-life PacketShaper models, including: 1200, 1400, 1550, 2500, 6500, 9500, and iShaper 400.

### Adobe Flash Player

Because the Blue Coat Sky user interface is displayed using Adobe Flash Player, you must have Adobe Flash Player 10 (or later) installed on the client system from which you access Sky. If you haven't already installed the latest version, make sure to do so before using Blue Coat Sky. If you aren't sure which version of Adobe Flash Player is installed on your client system, go to:

<http://www.adobe.com/software/flash/about/>

To download the latest version, go to:

<http://www.adobe.com/products/flashplayer/>

If you do not have Flash installed and you attempt to log in to Blue Coat Sky, you will be redirected to the Flash download page.

### BCAAA

PacketShaper uses the Blue Coat Authentication and Authorization Agent (BCAAA) to resolve IP addresses to user names so that it can classify and report on network users and groups. BCAA version 6.1 is required when using the user awareness feature in PacketWise 9.2.2 and higher. If you were using an earlier version of BCAA with PacketWise 9.2.1, you must install the new version for PacketWise 9.2.2.

### Supported Browsers

The Advanced UI and Blue Coat Sky have been tested with the English version of the following web browsers:

- Microsoft Internet Explorer 9 (Note: You may need to enable Compatibility View if any UI screens don't render properly.)
- Mozilla Firefox 20 and 21
- Google Chrome 26 and 27

Others browsers and versions may be compatible, but have not been tested.

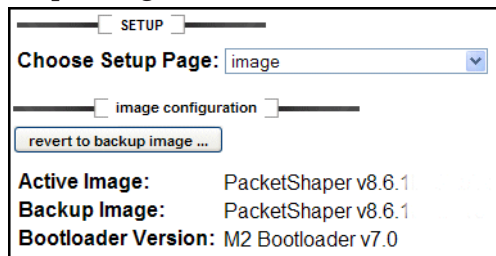
### Remove Obsolete Plug-Ins When Upgrading

When upgrading from PacketWise v8.x to v9.x, it's important to remove any old 8.x plug-ins. Leaving these obsolete plug-ins on the unit could cause the PacketShaper to reboot.


---

## PacketShaper Bootloader Version

PacketWise v8.6 and higher require the PacketShaper to use bootloader version 7.0 or higher. To determine the bootloader version your PacketShaper is using, use the **image show** CLI command or display the **Setup > image** screen.



If your bootloader version is not 7.0 or higher, you need to update the bootloader using the plug-in that has been developed for this purpose.

 **Note:** The Bootloader Update plug-in cannot be executed on the following PacketShaper models: 1200, 1550, 2500, 6500, 9500 and iShaper 400.

If you haven't done so already, follow the steps below to install the Bootloader Update plug-in before upgrading the PacketShaper to v9.2:

1. Download the bootupdt.plg plug-in file: <https://bto.bluecoat.com/sites/default/files/bootupdt.plg>
2. At the command line, change to the directory where you downloaded the plug-in.
3. To open an FTP session to the PacketShaper, type:

```
ftp <ipaddress>
```

where *<ipaddress>* is the IP address of the PacketShaper (for example, *ftp 207.78.98.254*). You can also type the domain name.

When you press Enter, the screen messages indicate that the connection has been made and that the server is ready.

4. Enter a user name (such as *touch*).
5. Enter the PacketShaper's *touch* password.
6. Enter **bin** to go into binary mode.
7. Change to the PLG directory:

```
cd plg
```

8. To transfer the file to the PacketShaper, type:

```
put bootupdt.plg
```

After you press Enter, the file is transferred to your PacketShaper.

9. Exit the FTP session (**quit** or **bye**).

To run the Bootloader Update plug-in, all you need to do is reset the PacketShaper:

1. Open a Telnet window and connect to your PacketShaper.
2. Reset the PacketShaper by entering the following CLI command:

```
reset
```

3. Close the Telnet window, and wait for the boot-up process to complete.

- 
4. To confirm that the bootloader was updated, access the PacketWise software by entering the PacketShaper's IP address in your web browser. After you log in, the Info tab displays a message about the bootloader.

## Upgrading Overview

To upgrade your software, download the new image and load the software onto the PacketShaper. There are two ways to download the software:

- Use the PacketWise browser interface (see **Option 1** below)
- Use the Blue Coat download website (see **Option 2**)

Try downloading the software with the PacketWise browser interface first. If this method doesn't work (perhaps because the corporate LAN is private or because a security policy or firewall is in place), download the image from the Blue Coat download website to a computer that is not subject to these restrictions.

## Option 1

### Use the PacketWise Browser Interface to Upgrade the Software

 **Note:** Your PacketShaper must be running bootloader version 7.0 or higher before you upgrade the image.

To upgrade the PacketWise software image:

1. Make sure you have backed up your configuration files. (See "Backing Up Software Configurations" on page 5.)
2. Make sure the PacketShaper is running bootloader version 7.0 or higher. (See "PacketShaper Bootloader Version" on page 11.)
3. Access the PacketWise software by entering the PacketShaper's IP address in your web browser.
4. Click the **setup** tab.
5. From the **Choose Setup Page** list, select **image**. The *image configuration* window is displayed.
6. In the **Image File Location** field, enter the explicit pathname of the FTP server that holds the software image file. The *Image Configuration* window supplies the default pathname for the latest recommended image on the PacketShaper FTP site:


```
//ftp.packetshaper.com/latest9x.zoo
```

To load a new image file directly from another FTP server, enter:

```
[//<hostname>/]<filename>
```

- [//<hostname>/] is the name of the FTP server. For example:  
`//corp-server.example.com/`
  - <filename> must be the explicit path and filename. For example, `/PWimages/pw911.zoo`
7. Enter a user name to access your FTP server, if required. If you are downloading the latest image file from ftp.packetshaper.com, do not enter a user name.
  8. Enter a password if it is required. If you specified a user name, a password is required. If you are downloading the latest image file from ftp.packetshaper.com, do not enter a password.
  9. Click **load new image** in the *image configuration* window to install the latest software image.

When you load a new image, PacketWise replaces the current backup image with the active image and replaces the current active image with the new image. Also, after the image is loaded, a dialog box prompts you to confirm the unit reset.

 **Note:** If the configuration didn't load properly (for example, the traffic tree disappeared), see "Loading a Traffic Configuration" on page 15.

- 
10. Since user lists can contain user and group names starting in v9.2.2, user names have a **u:** prefix to distinguish them from group names, which have a **g:** prefix. If you had created user lists in v9.2.1, you must use the **ul reformat upgrade** CLI command after upgrading to v9.2.2 or higher. This command inserts **u:** before each user name in the list, making 9.2.1 user lists compatible with 9.2.2 and higher.
  11. Clear the browser cache (see “Clear Browser Cache” on page 14) and, if necessary, reset measurement data (see “Reset Measurement Data” on page 14).

## Option 2

### Download the Software from the Blue Coat Download Website

This method of upgrading the PacketWise software is a three-part process. First, download the software image file from the Blue Coat download website to your client workstation. Second, FTP the file from your client workstation to the PacketShaper. Third, load the new software image.

 **Note:** Your PacketShaper must be running bootloader version 7.0 or higher before you upgrade the image.

To download the latest software image:

1. Make sure you have backed up your configuration files. (See “Backing Up Software Configurations” on page 5.)
2. Make sure the PacketShaper is running bootloader version 7.0 or higher. (See “PacketShaper Bootloader Version” on page 11.)
3. Log in to the BTO site (<https://bto.bluecoat.com>) with your Blue Coat Support username and password.
4. Go to the **Downloads** tab.
5. Select **PacketShaper** from the product list, and then select your model number.
6. In the PacketShaper release list, select the software version you want to download.
7. Verify the file was downloaded successfully.

To copy the new software to the PacketShaper:

1. At the command line, change to the directory where you downloaded the software image.
2. To open an FTP session to the PacketShaper, type:

```
ftp <ipaddress>
```

where *<ipaddress>* is the IP address of the PacketShaper (for example, *ftp 207.78.98.254*). You can also type the domain name.

When you press Enter, the screen messages indicate that the connection has been made and that the server is ready.

3. Enter a user name (such as *touch*).
4. Enter the PacketShaper’s *touch* password.
5. Enter **bin** to go into binary mode.
6. To select the PacketShaper’s data disk as the FTP destination, type:

```
cd 9.258/
```

7. *Optional:* To turn hash printing on, enter **hash**. (With hash enabled, you will see a “#” symbol for every 2K transferred.)
8. To transfer the file to the PacketShaper, type:

```
put <filename>
```

where *<filename>* is the name of the file you are copying to the PacketShaper (for example, *put 9\_1\_1.zoo*). After you press Enter, the file is transferred to your PacketShaper.



- 
9. Exit the FTP session (**quit** or **bye**).

To load the new software image:

1. Make sure the PacketShaper is running bootloader version 7.0 or higher. (See “PacketShaper Bootloader Version” on page 11.)
2. Open a Telnet window and connect to your PacketShaper.
3. To select the PacketShaper’s data disk as the source directory, type:


```
cd 9.258/
```

4. To load the new image, type:

```
image load <filename>
```

where <filename> is the name of the file you copied to the PacketShaper (for example, *image load 9\_1\_1.zoo*). After you press Enter, you are asked to confirm the process. Press Enter to proceed.

5. Close the Telnet window, and wait for the image load/boot-up process to complete.
6. Since user lists can contain user and group names starting in v9.2.2, user names have a **u:** prefix to distinguish them from group names, which have a **g:** prefix. If you had created user lists in v9.2.1, you must use the **ul reformat upgrade** CLI command after upgrading to v9.2.2 or higher. This command inserts **u:** before each user name in the list, making 9.2.1 user lists compatible with 9.2.2 and higher.
7. To confirm that the new version was installed, access the PacketWise software by entering the PacketShaper’s IP address in your web browser. After you log in, the software version number appears in the window.

 **Note:** If the configuration didn’t load properly (for example, the traffic tree disappeared), see “Loading a Traffic Configuration” on page 15.

8. Clear the browser cache and reset measurement data (if necessary). See sections below for details.

## Clear Browser Cache

After upgrading to PacketWise 9.2, you must clear the browser cache to see the new functionality. To clear the cache:

Firefox: **Tools > Clear Recent History > Cache**

Internet Explorer: **Tools > Internet Options > General > Browsing History > Delete > Temporary Internet files**

Chrome: **History > Clear browsing data > Empty the cache**

The steps for clearing the cache may vary, depending on which browser version you are using.

 **Note:** You should also clear the cache after downgrading.

## Reset Measurement Data

Depending on which version you are upgrading from, you may need to reset the measurement engine. PacketWise 9.2.6 does not contain any new measurement variables, so you won’t need to reset measurement data unless you are upgrading from a pre-9.1 version (which did introduce new variables).

To reset measurement data:

1. Click the **setup** tab.
2. From the Choose Setup Page list, choose **unit resets**. The unit resets options appear on the Setup screen.
3. Select the type of measurement data to reset: **Link**.
4. Click **reset measurement data**.

---

## Problems with Upgrading

If you attempt to load the PacketWise 9.2 image on a PacketShaper that doesn't have bootloader v7 or higher, the PacketShaper will not be able to boot successfully. (This is why it is so important to run the Bootloader Update plug-in before upgrading to PacketWise 8.6 or higher.) The Bootloader Update plug-in cannot be executed on the following PacketShaper models: 1200, 1550, 2500, 6500, 9500 and iShaper 400. Also, the bootloader version cannot be manually upgraded to version 7.0 or higher on the following PacketShaper models: 1200, 1550, 2500, 6500, 9500 and iShaper 400.

If the PacketShaper is unable to boot successfully due to an improper bootloader version, you must revert to the backup image of PacketWise, which is the image previously installed on the unit before you loaded the v9.2 image. The recovery procedure must be performed from a console connection:

1. Using a null-modem cable, attach a workstation or PC to the unit's port labeled **CONSOLE**. This cable offers both 9-pin and 25-pin connectors on each end.
2. Start your terminal emulation program (such as HyperTerminal).
3. Verify that you have configured the program with the following values to communicate with the unit's console serial port:
  - 9600 bps, 8 data bits, 1 stop bit, no parity, no flow control
  - If you are using a modem connected to the serial port, the modem must be set to: 9600 bps, 8 data bits, 1 stop bit, no parity, auto-answer (usually ATH1 in the standard Hayes command set), and DTR always on (usually a DIP switch setting). Check the modem manual for details.
4. Power cycle the PacketShaper.
5. As the unit is attempting to boot, (the message **Loading...** appears in your terminal emulation program), press **Ctrl+B**. This forces the PacketShaper to reboot using its backup image.

## Loading a Traffic Configuration

If your configuration didn't load properly after upgrading, you can load a traffic configuration from a previous version. You might also want to load a traffic configuration if you want to use a configuration from another unit. See "How Do I Restore Configurations?" on page 6.

---

## Known Issues in PacketWise 9.2.6

This section lists known issues in PacketWise 9.2.6.

### Downgrade Issues

 **Note:** If you want to downgrade from v9.2 to a 9.1 version, choose 9.1.3 or higher; earlier 9.1 versions had issues that were fixed in 9.1.3.

- Although PacketWise 9.2.1 fixes an upgrade issue that caused the PacketShaper to reboot when the time zone was set to London, downgrading to a previous version can experience this same issue. Blue Coat recommends that if your time zone is set to London, temporarily change the time zone to another zone before downgrading.
- User awareness downgrade issues:
  - User classes become match-all classes when downgrading from 9.2.1 to earlier versions.
  - User group classes become user classes when downgrading from 9.2.2+ to 9.2.1
  - User list classes have undefined matching rules when downgrading from 9.2.2+ to v9.2.1 (and match-all rules when loading a 9.2.2+ configuration on 9.2.1).  
Note that these classes do not show configuration errors. These classes should be deleted manually, or after downgrading, you can restore the old configuration you had previously saved with the **config save** command.
- Downgrading from v9.2.2+ to v9.2.1 can cause the following issues:
  - class reset and config reset operations do not work
  - turning off the **traffic-info** command causes the PacketShaper to reset  
To avoid these issues, issue the **config reset** command prior to downgrading. After downgrading, you can then restore the 9.2.1 configuration you had previously saved with the **config save** command.

### User Awareness Issue

- If there is a match-all class in the root of the traffic tree in addition to the Default match-all class, creating a user list class will cause the PacketShaper to reset. To check for the existence of a match-all class, look for a class with a bucket next to it in the Advanced UI traffic tree; it will appear above the Inbound/Default and/or Outbound/Default class.

### Login Issues

- If the initial page (Info tab in Advanced UI, Dashboard in Sky UI) doesn't display after logging in to the PacketShaper, click the browser's Refresh button. You may need to click the Stop button first.
- You may occasionally receive an "invalid password" message when logging in to the PacketShaper browser interface, even when entering the correct password. This could occur when the PacketShaper is reset when there are multiple Sky UI browser sessions open. The CLI will still work properly during this temporary window of browser inaccessibility.

### WebPulse Classification Issues and Limitations

- Blue Coat is continually fine-tuning the web applications and operations that WebPulse can identify. As these enhancements are incorporated into WebPulse, PacketShaper will automatically take advantage of these improvements. Because of the dynamic nature of web sites, Blue Coat will need to analyze new URLs as they appear and enhance WebPulse to include these updates; during this process, some web applications and operations may temporarily be misclassified.

- 
- If a URL starts its connection using HTTP and then switches to HTTPS, the PacketShaper will not be able to classify the operation over the secure connection.
  - Some of Amazon Instant Video traffic may get classified in the FlashVideo class.
  - PacketShaper passes web traffic while determining its URL category, service, and operation. This means that some content may pass through the PacketShaper before a configured policy is applied. Once the URL classification is verified, PacketShaper applies configured policy on subsequent traffic. Note that the policy application for classes that rely on WebPulse works most of the time when the URL is in the WebPulse cache; when the URL must be looked up in WebPulse, the policy may not be successfully applied in time. In addition, behavior for asymmetrically applied redirect policies is non-deterministic for WebPulse-based classes since WebPulse classification is not part of packet processing. Therefore, when applying never-admit policies with the redirect option, be sure to apply the policy to the WebPulse classes in both directions (Inbound and Outbound).
  - To avoid class tree configuration errors, do not create classes that contain both a category-based rule and a service/service group-based rule. If needed, the recommended way to combine category matching rules with service/service group matching rules is with a parent-child class relationship. For example, use a category-based class as a parent of a service/service group-based class.
  - HTTP traffic may not be classified properly when compression and/or acceleration is enabled. If you experience this issue, save your configuration, issue the **setup reset all** CLI command, and then restore the configuration. HTTP classification will work properly after you do this.

## Browser Issues

- If new functionality isn't showing in the UI after upgrading to or downgrading from PacketWise 9.2, you should clear the browser cache. See "Clear Browser Cache" on page 14.
- You may need to enable Compatibility View in Internet Explorer if any UI screens don't render properly.

## Host Accounting Issue

If you enable host accounting and specify an interval of 0, the PacketShaper may reboot. Valid interval values are 1-1440 minutes; do not enter 0 for *<interval-minutes>*.

## IPv6 in a Direct Standby Topology

Since the introduction of direct standby, IPv6 traffic has been dropped by the Standby port and not copied to the partner unit in a direct standby topology. The new services introduced in v9.1 are affected in the same manner. Therefore, the direct standby feature is not fully functional in an IPv6 network.

## ISP 10000 Key Limitations

- When downgrading to a PacketWise 8.6.x image on a PacketShaper 12000 that has an ISP 10000 key installed, you must replace the ISP 10000 key with a 5000 key before loading the image. If you attempt to load the image when the appliance has the ISP 10000 key, the command will abort and a message will display letting you know that the image is not supported with the currently installed key. The message about the image not being found can be disregarded.
- To avoid a multiple reboot situation, you should issue a **class reset** before downgrading the ISP 10000 key to a key with fewer classes or downgrading the release from v8.7.x to v8.6.x.
- If you are using a demo key and the ISP 10000 key expires, the PacketShaper will reset the class tree to the factory default, institute a 1024 class limit, and automatically reboot. (If the PacketShaper is in shared mode, it will need to reboot two additional times before the tree is reset.) All other configuration settings will be unaffected. Blue Coat recommends saving the configuration with the **class save** command before the key expires; use the **setup show** CLI command to see when the key is set to expire. Note that purchased keys do not expire; this situation affects demo keys only.

---

## PacketShaper 12000 Issues

- The ifSpeed and ifHighSpeed SNMP variables report incorrect values when a link is down on a PS12000.
- Using the pinhole reset on the front panel of the PacketShaper 12000 can cause LEMs to not go into bypass, and traffic will be interrupted for approximately 50 seconds. However, bypass will work as expected during power outages, power cycles, or other types of resets.
- After rebooting the PacketShaper 12000 when a terminal server is connected to the serial console, you may see the Intel Boot Agent Setup Menu, waiting for input. This can happen with terminal servers that have small serial data buffers. If you experience this issue, disable software flow control on the terminal server.

## PacketShaper 12000 and Direct Standby Limitations

- If a PS12000 is in standby mode and you power down to install or replace a LEM, it is possible that the new LEM will not have all devices set to bypass=OPEN. This will result in the confusing banner message *Not enough interfaces for Direct Standby* to appear when the unit is rebooted. If you see this message, issue the following CLI commands:

```
setup bypass open all
setup standby direct
```

Direct standby mode will be restored.

- The PS12000 Standby port supports only the auto-negotiate speed setting. Manual settings can possibly cause the device to reboot.

## Backup Image Lost after Failed Image Load

If a remote image load is aborted (for example, when a corrupted image is detected) and the image load is reattempted, the backup image on the system disk (9.256/bin/backup.zoo) is lost, and the current and backup images on the data disk become the same image version. Therefore, if you revert the image at this point, it will simply revert to the same version as the current one. Blue Coat recommends that once an image load fails because of a corrupted image, do not attempt to load the corrupted file again.

This happens only when you specify an FTP location for the image load path. You can avoid this potential problem by putting the image on the box (using FTP, for example) and then loading it with the **image load** command, specifying the local path to the .zoo file.

## Classification Issues

- Although the UI allows you to create a class based on the Standby port or a LEM that is being used for direct standby, this class will not capture any traffic and should therefore not be created.
- SNMP does not auto-discover in the Localhost class; you must manually create the class if you would like to classify PacketShaper's localhost SNMP traffic.

## Policy Issue

The web redirect policy does not work properly.

## Blue Coat Sky UI Issues and Limitations


- When Blue Coat Sky is the default user interface, neither the Advanced UI nor the Sky UI time out after a period of inactivity. Previously, the Advanced UI would time out after 60 minutes of inactivity and would require you to log in again.
- Blue Coat Sky, in particular its real-time graphing features, can place a high CPU load on the client machine running Sky. To avoid unnecessary CPU load, Blue Coat recommends that you only run real-time graphs when you are actively viewing them. Note that this doesn't impact the performance

---


of the PacketShaper, although it can affect the performance of the client machine. For best Sky performance, the client machine should have the following minimum requirements: Pentium 4 @ 3GHz with 2GB of RAM.

- In configurations with large traffic class trees (more than 2000 classes), performance in Blue Coat Sky may not be optimal. For example, report generation may be slow.
- When Xpress tunnels are configured to run in legacy mode, the status line in Blue Coat Sky may not accurately reflect the current state of compression. For example, the status line may show *Compression on* when, in fact, it is turned off. The status line in the Advanced UI does show the correct compression state.

### Graphing

- If you have a Blue Coat Sky browser session open when the PacketShaper is reset (for example, via a CLI command or by turning the unit off and back on), real-time graphs will stop updating and a *Retry Update?* error message appears. Before resetting the unit, you should close the browser window or manually log out (with the **Log out** link). If you don't, you need to close all open browser windows after resetting the PacketShaper. (Logging out won't be sufficient.)
- Occasionally, each selected class is graphed twice on historic graphs. If you see this behavior, click the **Refresh Class Tree Now**  icon.
- The higher the latency on the network or the higher the load on the PacketShaper, the longer it takes for historical graphs to render in Blue Coat Sky. If a graph fails to display in Sky (in other words, it times out), try creating a similar graph in the Advanced UI.

### Class Tree

- In combined view, when you want to copy a single-direction class (such as Inbound/test) to the other direction (for example, to Outbound), choose Root for the **To** location. After the copy operation, the class then appears in the tree as  (bi-directional).
- Blue Coat Sky copies all children when copying a parent with children, even if you selected only some of the child classes. For example, suppose you have a parent with four child classes. If you select the parent and three of the child classes, Blue Coat Sky copies all four child classes.

### Policy Manager

- After editing or creating a rate policy, you may see the error message, *Policy not bound with class*. However, the policy is still created successfully.
- When creating a "simple match" class, the **Auto-Discovery in Class** option is available for all classes, even when it's not applicable. Blue Coat Sky will, however, display an error message if you inappropriately select the checkbox.
- In combined view, if you create a class in both directions when your PacketShaper is within two classes of its configuration limit, Sky is able to create only one class. The error message indicates that it couldn't create the class, but in fact, it created the Inbound class but couldn't create the Outbound class. (Note: The maximum number of classes in your class tree is actually one less than the configuration limits on your PacketShaper model. For example, the PacketShaper 900 can have up to 255 classes: 256 limit minus 1.)

### Switching Between Sky and Advanced UIs

- If you switch to the Advanced UI and then press the browser's Back button (perhaps because you want to return to Blue Coat Sky), the Login screen displays, giving the appearance that your session has logged out. You have not actually logged out, though: you can press the browser's Forward button to return to Blue Coat Sky at this point. The proper way to switch between the Advanced UI and Sky is to use the **Blue Coat Sky** link in the banner; avoid using the browser's Back button.



- 
- Blue Coat recommends that you have only one Sky session open at a time.

### Service Groups Issues

- While a move operation is in process, some of the selected services might not be moved, even if you get a message that the operation was successful. This might occur if someone else is creating classes in another user session or if you press Ctrl-C to abort the operation while it's in process. If this happens, repeat the move command on the services that weren't moved.
- Prior to deleting a custom group, delete any classes based on that group. If you fail to do this, the class will have a configuration error and you will be unable to delete it in the browser interface. A workaround is to use the **class delete** command in the command-line interface.
- If a class has duplicate matching rules with another class (for example, a local /Inbound/HTTP and an inherited /Inbound/Internet/HTTP), one of these classes will have a configuration error. Until you resolve this error, traffic will still get classified into the errored class.
- Occasionally PacketWise displays the configuration before a service group operation is completed. If the configuration doesn't look correct, try refreshing the browser.

### RADIUS Issue

PAP, CHAP, and version two (v2) of MS-CHAP can be used to authenticate against a RADIUS server; MS-CHAPv1 currently has issues.

### SNMP Issue

If SNMP look and touch community strings are identical, the PacketShaper does not send SNMP traps. Be sure to set unique look and touch community strings.

### Issues with User-Defined Services

- If you delete a user-defined service (UDS), make sure to also delete any traffic classes that are based on this service. If you fail to delete the class, a configuration error results. In addition, the traffic hit count on a class created with a UDS does not get reset after the UDS is deleted. The next UDS created may continue to hit the class previously created by the original UDS.
- If you create a UDS, delete it, and then create another UDS, the new UDS may have the same service ID as the one that was deleted. This can create misinterpretation of Flow Detail Record (FDR) data in third-party FDR collectors.

### Customer Portal Issues

- Do not set a secondary customer portal IP address if using a secure LDAP connection between PolicyCenter and the Directory Server; setting the portal IP address causes LDAP to use the portal IP address instead of the management address.
- When a customer portal IP address is configured, several PacketShaper features use the portal IP address instead of the PacketShaper's management IP address. In particular, SNMP sends the portal IP address as the source address in notify and response packets, and heartbeats are sent from the portal IP. If this is an issue for you, you can clear the portal IP address and have customers log in to the portal with the following URL: **`http://<management-IP>/customer`**.

### Matching Rule Issue

In the Advanced UI, the browser may display a blank screen after you have edited a matching rule and applied the change. This typically happens after you have attempted to edit the rule with an invalid specification (such as duplicate matching rule). If this happens, you need to delete and then recreate the class.

---

## Classes with Duplicate Matching Rules

Typically, PacketWise does not let you create a traffic class with matching rules that duplicate another class. However, PacketWise allows it to happen in the following situation: when a class has a Default child class, you are able to create a class with a different name but with the same matching rules. For example, suppose you have created a class named Internet that classifies traffic for the Internet service group, and class discovery is enabled (which creates a Default child class). PacketWise lets you create another class named MyInternet based on the Internet service group, without displaying an error message or configuration error. Traffic gets classified into only one of the classes (whichever appears first in the class tree).

## Limitations of the VoIP Summary Report

The **Class** drop-down list for the *VoIP Summary* report only lists VoIP classes if the name appears with the exact upper/lower case as the auto-discovered class (RTP-I). If you created the class manually and typed the name differently (such as rtp-i), the name does not appear on the Class drop-down list.

## Config Save Filenames

When providing a filename in the **config save** CLI command, enter a name that is eight characters or less; entering a longer filename displays an error message *No such address*.



---

## Known Issues in Xpress

This section lists known issues with the Xpress feature in PacketWise 9.2.6.

### Classification Issue When Acceleration is Enabled

The classification of Citrix priority tags does not work on accelerated flows. Note that all other types of Citrix classification works on accelerated flows and priority tagging classification works on non-accelerated flows. 112371

### MTU Issue

Acceleration does not respect the MTU imposed by low speed link values (less than 384k). The workaround is to use the **tunnel mtu <mtu>** CLI command to force the desired MTU value.

### Command-Line Interface Issues

- The PacketWise command-line interface is able to complete partial commands if a user enters enough information to specify just a single command. For example, entering just **tr tr** returns the output for the command **traffic tree**. However, the command to determine the value of the measurement engine variable bytes-saved-by-compression, even when typed in full, is also the partial text for the command to determine the value of the bytes-saved-by-compression% variable.
- If you use a single **measure dump** CLI command to determine the value of both the bytes-saved-by-compression and bytes-saved-by-compression% measurement variables, list the bytes-saved-by-compression variable before the bytes-saved-by-compression% variable. If the variables are listed in the opposite order, the bytes-saved-by-compression variable reports the same value as bytes-saved-by-compression%.

### Miscellaneous Xpress Issues

- With short flows (that is, flows containing only a few packets), you may notice a discrepancy in measurement data between direct standby partners. For example, the active PacketShaper may show more compression savings than the passive PacketShaper. This situation occurs in enhanced tunnel mode only.
- If you are having problems controlling VoIP traffic with rate policies and partitions when there is significant competing traffic, you may want to disable packing and compression.
- If two PacketShapers are connected via the direct standby feature, those units may not form a proper acceleration tunnel for asymmetric flows unless the same static local hosts and tunnel passwords are configured on both units.

---

## Additional Information for PacketWise 9.2

This section contains important additional information that will help you better understand and use PacketWise 9.2.

### WebPulse Additional Information

- Because WebPulse classification features require access to a number of outside web servers, you should not completely secure the outside interface. Instead, use the **setup secure outside list** command and add the IP addresses of the following servers to the exception list: the fastest WebPulse service points (use the **setup webpulse show service** command to find the IP addresses), the WebPulse map update server (sitereview.bluecoat.com), the support update server (updates.bluecoat.com), the heartbeat server (hb.bluecoat.com), and the traffic information reporting server (cda.bluecoat.com). If you are using a web proxy, you also need to add this server's IP address to the list if it will be accessible via the outside interface.
- Don't try to compare class hits on category classes with category hits shown in the **setup webpulse show categories** CLI command. A flow can be categorized with up to four categories (for example, a hit on four different categories) but it can only hit one category class in the traffic tree. In addition, class hits can be reset at any time (with the **clear stats** button on the Monitor tab). Category hits accumulate until a **setup webpulse reset** command is issued or until the PacketShaper is reset.
- PacketShaper identifies the service for web traffic before determining its URL category. Therefore, if the service has a policy (such as never-admit), the policy is applied before the traffic gets classified into the category class.
- When URLs using HTTP get redirected, PacketShaper classifies traffic according to the category of the original URL first, and then the redirected URL. With HTTPS, however, PacketShaper classifies traffic according to the category of the redirected page only; it is not able to see the certificate common name of the original URL.
- After disabling WebPulse or turning off discovery of a URL category, classes may continue to be discovered for up to a minute. This could happen if the category reaches the discovery threshold right before the feature is disabled. (The discovery threshold is the number of flows that PacketShaper must see in a one-minute interval before a class is created.) For example, if traffic based on the Real Estate category has already hit the discovery threshold before turning off discovery for that category, a Real\_Estate class will be auto-created. This is expected behavior.

### SNMP Requests

PacketWise 8.3.x and higher supports SNMPv1, SNMPv2c and SNMPv3. If your PacketShaper is configured to respond to SNMPv1 requests and you upgrade that unit to PacketWise 8.3.x or later, the PacketShaper responds to both SNMPv1 and SNMPv2c requests.

### PacketShaper 3500 Fan Speed

On a PacketShaper 3500, which has only one fan, the info tab reports a speed of 0.00Hz for power supply fan two. A speed of zero simply indicates that the fan is not present.

### Unsupported Images

Some PacketShaper models require a specific version of PacketWise software in order to run. For example, the PacketShaper 12000 requires PacketWise 8.6.3 or higher. However, it is possible to overwrite the supported version with an unsupported image of PacketWise. In this case, the unit can not boot, and you need to re-boot the unit using its backup software image.

---

## Additional Information for Xpress

This section contains important additional information that will help you better understand and use the Xpress feature.

### Understanding Acceleration

Acceleration is designed to improve TCP performance in the following three cases:

- On links that have a large bandwidth-delay product, acceleration can provide substantial throughput improvement over TCP for *bulk* data transfers such as FTP transfers of large data files or downloading of large images in a browser.
- On links that have a high loss due to transmission characteristics, as opposed to high loss from congestion, accelerated flows typically perform substantially better than TCP. (TCP sees any kind of loss as congestion and slows down accordingly.)
- For HTTP traffic, acceleration can be configured to prefetch objects on a web page, substantially reducing the time needed to display a page on high-latency links.

Non-TCP traffic is never accelerated. Also, acceleration provides little or no benefit in the following situations:

- *Transaction processing* over a high-latency link will not be improved. Thus, Windows File Sharing (CIFS) which relies on large numbers of transactions transferring small objects will not benefit from acceleration.
- *Low-latency links with only congestion loss*. For example, links with bandwidth-delay products under 100K bytes will see minimal or no performance benefit.

In addition, HTTP prefetch does not uniformly improve all types of web page downloads. Prefetch relies on extra bandwidth being available for prefetched objects. Prefetching is automatically disabled if the PacketShaper is running low on available memory.

### Configuration Options for Acceleration

In order to achieve the benefits of acceleration, PacketShapers need to be properly configured for your network and the flows you wish to accelerate. Some PacketShaper configurations that perform perfectly well without acceleration may actually get poor performance with acceleration, if acceleration is enabled without regard to the issues stated above and without some appropriate configuration changes.

Acceleration uses one of two strategies for transmitting packets. If congestion control is enabled (the default), data is sent at the outbound link or partition rate, and packet loss is treated as congestion; this causes acceleration to slow down. This mechanism is conceptually the same as the congestion control logic used by TCP. If congestion control is disabled, then acceleration relies totally on the outbound link or partition setting; it treats loss as data corruption, not congestion, and does not slow down.

### Preferred Configuration for Acceleration

Acceleration works best when the *available* link rate is fixed, and the PacketShaper outbound link or partition rate can be set to a value which matches this available rate. By “available,” we mean the amount of bandwidth that is available for accelerated TCP flows. For example, if a link is shared between VoIP and FTP file transfers, the available bandwidth is what is left over after accounting for VoIP traffic (which, being UDP-based, is never accelerated). If the available rate is known and relatively steady, then the best performance can be achieved by setting the *outbound* link or partition rate of the sending-side PacketShaper to a value that’s 1-2% smaller than this available limit. In this case, you should disable congestion control.

---

If PacketShapers configured for direct standby are using the acceleration feature to accelerate asymmetric traffic, both direct standby partner PacketShapers must be able to access Inside hosts via the units' Xpress-IP. If Inside hosts are on a different subnet from the Xpress-IP, that PacketShaper must have an Ingress gateway defined. Use the CLI command [tunnel ip configure](#) to configure an Ingress gateway.

## When to Use Congestion Control with Acceleration

By default, PacketShapers uses congestion control when acceleration is enabled. This is a very conservative approach designed to minimize performance problems that might occur if the sending-side PacketShaper's outbound link and partition rates are not properly set. This is also necessary for the (not recommended) configuration in which Inbound policies on the remote PacketShaper(s) are used to control data throughput. Generally speaking, you should enable congestion control for links with wildly varying available rates, for example, what is left over from VoIP. Congestion control may also be necessary for full-mesh networks where you cannot predict the actual bandwidth available between any two end hosts.

Note that since congestion control is a sub-optimal setting for acceleration, any acceleration benefits may vary greatly over time or between different hosts. You must assess performance on your particular network and then decide whether or not it benefits from acceleration.

## ICNA Algorithm

The ICNA plug-in is not necessary when using enhanced tunnel mode because the ICNA algorithm is built into enhanced compression. However, if you are using legacy or migration tunnel mode, you need to install the ICNA plug-in. Note that the ICNA plug-in only loads when you are using legacy or migration mode.

## Limitations in Xpress

- Watch mode is not available with enhanced Xpress tunnels, and can be enabled only when PacketShaper is set to legacy tunnel mode. If watch mode was enabled in 7.x, it will be enabled after the upgrade and the unit will be in legacy mode.
- Because TCP is converted to XTP when acceleration is enabled, the response-time measurement (RTM) variables aren't able to measure a transaction through its complete round trip, and does not account for the portion that is not TCP.
- The `tcp-early-retx-toss-pkts` and `tcp-early-retx-toss-pkts%` variables rely on TCP Rate Control so they won't increment for accelerated connections.
- If only legacy compression tunnels exist between two PacketShapers, and you create an enhanced compression tunnel between those units but then later disable enhanced compression on one or both of those units, the previous legacy compression tunnels do not automatically reform. Delete the enhanced tunnel to reenable the legacy compression tunnels.

## Multicast Compression

Multicast traffic can be compressed in v8.x assuming that the following conditions are met:

- The Class D addresses must be added to remote and/or local host lists using the **tunnel local add** and **tunnel remote add** commands. Unlike unicast compression hosts, multicast hosts are not discovered automatically.
- The tunnel must be static (since only static tunnels can be configured with remote and local hosts.)

Other important points:

- In order for the traffic to get disseminated to multiple recipients, the decompressed multicast traffic must be forwarded to a router. If not, only one host receives the flow.
- Multicast addressees are in the range 224.0.0.0 – 239.255.255.255. For more information about multicast addresses, see:

<http://www.iana.org/assignments/multicast-addresses>

- 
- Multicast traffic cannot be accelerated.

## Asymmetric Flows

For acceleration to work, traffic needs to pass through a single pair of PacketShapers in both directions. If a redundant topology is configured in such a way that a server is reachable through a path that does not first traverse the remote PacketShaper, the asymmetric flow are not accelerated.

In certain circumstances, connections will fail with asymmetric flows:

- When packets from the client to the server pass through both a client-side and server-side PacketShaper, but return packets bypass either of these PacketShapers.
- When routing changes cause TCP packets to not go through their near-side PacketShaper
- When routing changes cause XTP packets to pass through an accelerating PacketShaper that is not the original partner.

If Xpress is unable to successfully complete an accelerated connection to a particular host (perhaps because the flow was asymmetric), Xpress remembers this on a per-destination basis for a period of time and does not try to intercept additional connections for the failed destination.

If PacketShapers configured for Direct Standby are using the acceleration feature to accelerate asymmetric traffic, both Direct Standby partner PacketShapers must be able to access Inside hosts sourced via XTP. If the XIP hosts are on a different subnet (so there is a router connected to the Inside port of the PacketShaper, that PacketShaper must have a defined Ingress gateway.

## Xpress-IP Configuration for Units on the Same Subnet

When two PacketShapers are configured with Xpress-IP addresses on the same subnet, the Xpress-IP gateway must be set to *none* on both PacketShapers, if either of the following is true:

acceleration is off

or

all of the end hosts in the network are also on that same subnet.

This setup is most common in network configurations used for testing, demonstrations, and training where the PacketShapers and hosts being used are all on the same subnet. It may also be found in cases where networks are bridged over a WAN.

## Localhost Traffic Doesn't Get Tunneled

Localhost traffic doesn't get compressed or packed because Xpress doesn't tunnel flows that have a PacketShaper as the endpoint. In other words, when you access your PacketShaper via Telnet, web browser, or FTP, this traffic does not get tunneled.

## Acceleration Notes

Important notes about acceleration:

- The site router must be set to *none* when you are using acceleration.
- For best performance, Blue Coat recommends that shaping be enabled when using acceleration.
- If a PacketShaper is reset while there are active accelerated connections, those connections are terminated.
- For tunnels using dynamic host discovery, connections to destinations that are not already in the remote host list are not accelerated. New connections started after discovery of the host are accelerated.

