

Cascade Pilot for Steelhead and Whitewater

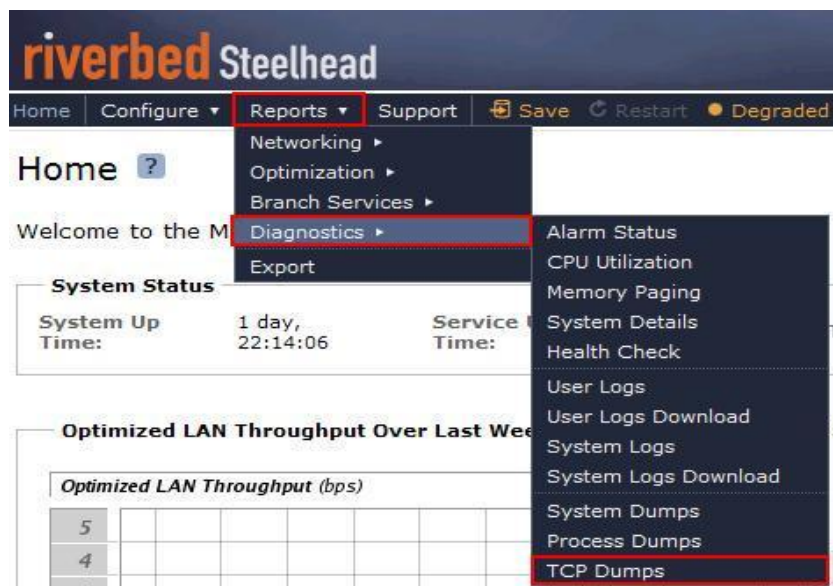
Improving Network Analysis for the Steelhead, Steelhead Mobile and Whitewater

Cascade Pilot is an extremely powerful tool for analyzing and reporting on packet capture data. In many sites, Steelheads and Steelhead Mobile are broadly deployed and provide an excellent platform for capturing traffic of interest without additional expense or deployment complexity. In fact, Steelheads, Steelhead Mobile Controller (SMC) and Whitewater can be used as remote sniffers to capture traffic when there are problems that might be difficult to diagnose otherwise. This document describes the process for initiating a packet capture on Steelhead, Steelhead Mobile Controller (SMC) and Whitewater and for bringing it into Cascade Pilot for detailed analysis.

Note: This document was prepared using the Steelhead version 6.5.0, Steelhead Mobile Controller (SMC) 3.0 and Whitewater 1.0.2. Older Steelhead, Steelhead Mobile Controller (SMC) and Whitewater versions might have different command syntax for capturing packets. Consult the online help if the version you are using does not correspond to these instructions.

Enabling Packet Capture on Steelhead

On the Steelhead, packet capture is configured using the Reports → Diagnostics → TCP Dumps menu item, as shown in the screen shot below:



SOLUTION BRIEF: Cascade Pilot for Steelhead and Whitewater

The TCP Dumps screen has an area for managing previously generated capture files and for viewing currently active TCP dumps. The top of the TCP Dumps page displays a list of existing TCP trace dumps (if any). The bottom of the page has controls to create a new trace dump or stop a currently running job. It also has a list that displays the trace dumps that are currently running. This list includes both TCP trace dumps started manually and also any dumps that were scheduled previously and are now running.

Note: You may need to manually refresh the screen to see changes, such as when errors are posted or to know when capture jobs are finished.

The screen shot below shows this screen when there are no existing capture files and no currently running TCP dumps.

Reports > Diagnostics > TCP Dumps ?

Stored TCP Dumps:

Download Link	Timestamp	Size
No stored TCP dumps.		

TCP Dumps Currently Running:

Running Capture Name	Start Time
No TCP dumps currently running.	

The red highlight indicates where to click to create a new capture job. This exposes a configuration area for specifying exactly how the capture job should be configured. Remember that the options shown here might appear in a different order depending on the version of software in use. The initial options are shown below.

TCP Dumps Currently Running:

Name

Capture Name:

Endpoints

Capture traffic between:

IPs:

Ports:

and:

IPs:

Ports:

Capture Name: Allows the user to specify an identifier for the capture file. The full file name consists of the hostname of the Steelhead appliance, followed by the interface selected for the trace (for example, lan0_0, wan0_0), and is terminated by the capture name specified by the user. If the user does not specify a capture name,

SOLUTION BRIEF: Cascade Pilot for Steelhead and Whitewater

the timestamp of the file in YYYY-MM-DD-HH-MM-SS format is appended to the hostname and interface to uniquely complete the filename.

Capture Traffic Between: Allows the user to specify pairs of IP addresses and ports for the traffic that will be included in the capture file. Multiple IP addresses and ports should be separated by commas. CIDR ranges are not allowed. The default setting for these fields is all traffic (i.e., All IP addresses and all ports).

Capture Interfaces: Allows the user to specify which Steelhead interfaces to use when capturing traffic. This supports selecting a physical, MIP, or RSP interface.

The screenshot displays a configuration window with three main sections:

- Capture Interfaces:** A list of checkboxes for selecting interfaces. The 'All Interfaces' checkbox is highlighted in yellow. Other options include primary, aux, lan0_0, wan0_0, lan0_1, rios_lan0_0, rios_wan0_0, rios_lan0_1, and rios_wan0_1.
- Capture Parameters:** A set of input fields for configuring the capture process. The values shown are: Capture Duration (Seconds): 30; Maximum Capture Size (MB): 100; Buffer Size: (empty); Snap Length: (empty); Number of Files to Rotate: 5; Only Capture VLAN-Tagged Traffic: (unchecked); Custom Flags: (empty text box).
- Schedule:** A section with a 'Schedule Dump' checkbox (unchecked) and two input fields: Start Date: 2010/11/18 and Start Time: 09:51:27.

An 'Add' button is located at the bottom left of the configuration area.

Selecting “All” results in dumping traffic from all of the interfaces. Selecting more than one interface or “All” generates individual traffic capture files corresponding to each interface.

There is no default selection and a capture interface must be selected or the capture job will return an error when it is started (see the highlighted area in the screen shot below).

No valid interface provided

Reports > Diagnostics > TCP Dumps ?

Stored TCP Dumps:

- Remove Selected		
Download Link	Timestamp	Size
No stored TCP dumps.		

Capture Parameters: Allows the user to specify characteristics of the capture job such as file size, capture duration, and packet size. The table below describes these in more detail.

Control	Description
Capture Duration	Specify how long the capture runs, in seconds. The default value is 30. Leave this value blank to initiate a continuous trace. When a continuous trace reaches the maximum space allocation specified, the oldest file is overwritten.
Maximum Capture Size	Specify the maximum capture file size in megabytes. The default value is 100. The recommended maximum capture file size is one gigabyte.
Buffer Size	Optionally, specify the maximum number of packets allowed to queue up before processing. The default value is 154.
Snap Length	Optionally, specify the snap length value for the trace dump. Specify 0 for a full packet capture. The default value is 1518.
Number of Files to Rotate	Specify how many TCP trace dump files to rotate in case the results cannot be contained in a single file. The default value is 5.
Only Capture VLAN Tagged Traffic	Captures only VLAN-tagged packets within a trace dump for a trunk port (802.1Q). This setting applies to physical interfaces only.
Custom Flags	Specify custom flags to capture uni-directional traces. See the online help for more detail.

Schedule Dump: Allows the user to specify when the dump should be started. By default, the capture job starts immediately. If a schedule is desired, specify the start date as YYYY/MM/DD and the time as HH:MM:SS in 24 hour format.

When all of the desired options are set, click **Add** to either start or schedule the capture job. Running capture jobs appear in the TCP Dumps Currently Running list at the bottom of the screen. The screen shot below shows a running job named “Example”:

Reports > Diagnostics > TCP Dumps ?

Stored TCP Dumps:

	Download Link	Timestamp	Size
<i>No stored TCP dumps.</i>			

TCP Dumps Currently Running:

<input type="checkbox"/>	Running Capture Name	Start Time
<input type="checkbox"/>	Example	10:03:34

Running jobs can be stopped by clicking the checkbox to the left of the job and clicking the button labeled **Stop Selected Captures**. This is particularly useful for continuous captures that are no longer needed.

Once the capture job is complete, the resulting TCP dump file appears in the Stored TCP Dumps display at the top of the page. These capture jobs can be selected individually and a copy can be saved on a system where Cascade Pilot is installed, as shown below:

Reports > Diagnostics > TCP Dumps ?

Stored TCP Dumps:

<input checked="" type="checkbox"/>	Download Link	Timestamp	Size
<input checked="" type="checkbox"/>	cam-sh14_primary_Example.cap0	2010/11/18 10:04	144.0 kB

click to download the file

TCP Dumps Currently Running:

	Running Capture Name	Start Time
<i>No TCP dumps currently running.</i>		

This brings up a dialog that allows the file to be saved and optionally renamed. Browse to the location where you want to save the file.

Enabling Packet Capture on Steelhead Mobile Controller (SMC)

A Steelhead Mobile deployment relies on the Mobile Controller, which acts as a gateway for remote users and is installed at a data center or at the server-side of the WAN. The Mobile Controller features a Web-based GUI that is use for centrally managing endpoint clients and can be used monitoring endpoint clients.

On Steelhead Mobile Controller (SMC), packet capture for endpoint clients is configured using the Reports → Endpoints → Endpoint Report. Select the check box next to one or more endpoint client and Click on the Request TCP Dump to upload the files.

SOLUTION BRIEF: Cascade Pilot for Steelhead and Whitewater

The screenshot shows the Steelhead Mobile Controller interface. The top navigation bar includes 'Home', 'Setup', 'Manage Endpoints', 'Reports', 'Logging', and 'Help'. The 'Reports' tab is active. The main content area is titled 'Endpoints - Endpoint Report' and shows a table of endpoint data. A red box highlights the 'Request TCP Dump' button, and a red arrow points to the checkbox next to the 'DEMO\\$demo' user name. A text box explains: 'Click the check box next to one or more endpoint user names and click Request TCP Dump to upload the files.'

User	Status	Version	IP Address	Group	Accel Policy	Endpt Policy	Total Reduction	LAN Data	Warmed Data	WAN Data	Connected At
DEMO\\$demo	Warning	3.1.0	172.30.0.50	Default	Initial	Initial	(64%)	26.5 MB	0 Bytes	9.3 MB	2010/12/19 23:46:10

To view endpoint TCP dump files, Click on Reports → Endpoint Diagnostic → TCP Dumps. Click the TCP dump name to open a file save dialog box and download the file.

The screenshot shows the 'Endpoint Diagnostics - TCP Dumps' page. It displays a list of diagnostic endpoint TCP dumps stored on the controller. The table below shows the details of these files.

Name	User	Size
trace-272425377-mgmttrace_jan.cap-20080606-014806.gz	DEMO\\$demo	1353 bytes
trace-272425377-mgmttrace_jan_0.cap-20101220-124055.gz	DEMO\\$demo	194491 bytes
trace-272425377-mgmttrace_jan_0.cap-20101220-124132.gz	DEMO\\$demo	197552 bytes
trace-272425377-mgmttrace_wan.cap-20080606-014806.gz	DEMO\\$demo	1054 bytes
trace-272425377-mgmttrace_wan_0.cap-20101220-124055.gz	DEMO\\$demo	97231 bytes
trace-272425377-mgmttrace_wan_0.cap-20101220-124132.gz	DEMO\\$demo	99494 bytes

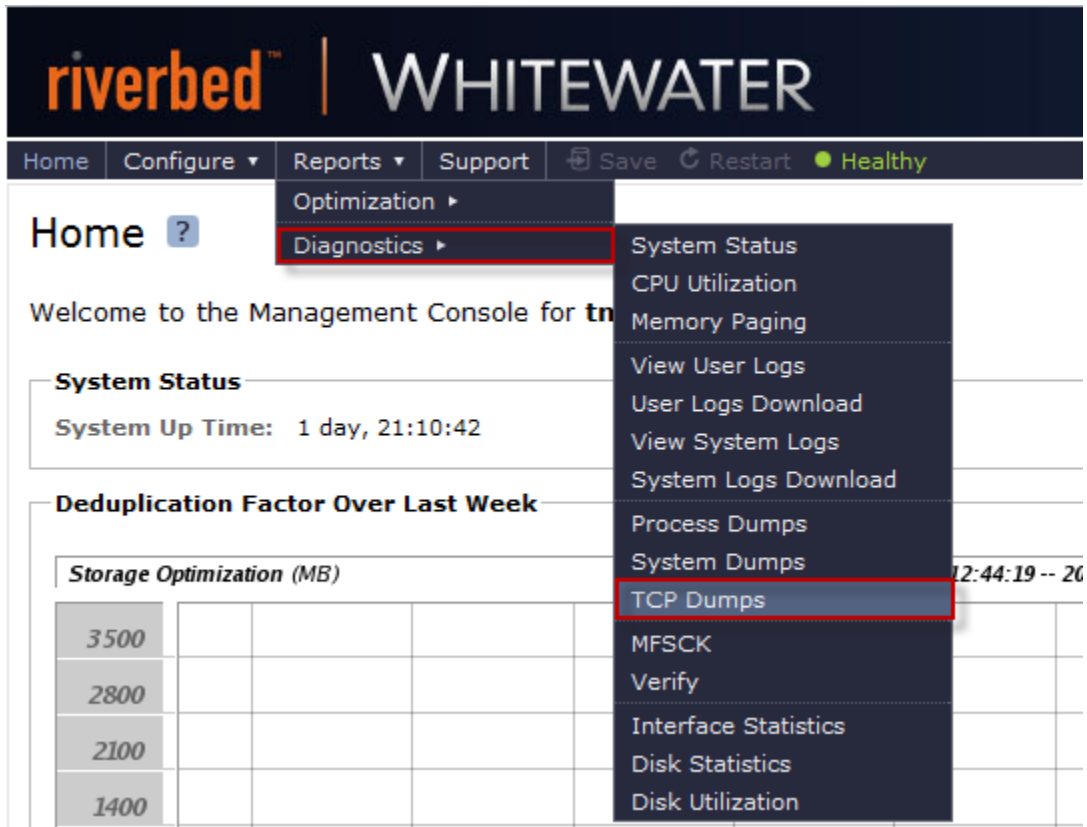
6 file(s)

Remove Selected Files

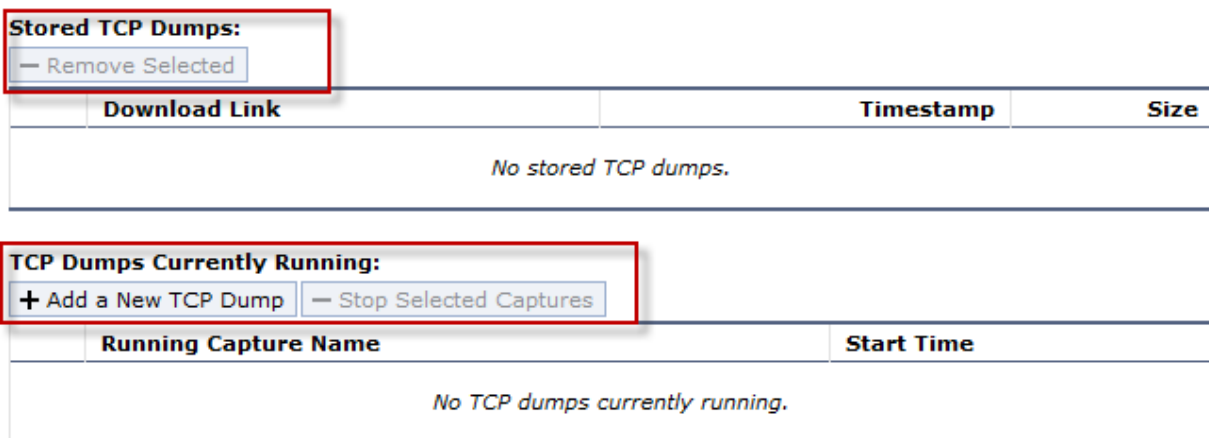
Note: In some cases the extension used for the file is a variation of .cap such as .cap0 or .gz. Files with this extension are not seen in Cascade Pilot by default. Therefore, when saving the file, it might be a good idea to change the extension to .cap to make things more straightforward in Cascade Pilot.

Enabling Packet Capture on Whitewater

Riverbed Whitewater appliance is a disk-to-disk data storage optimization system with unique cloud storage integration. The process of capturing packets on the Whitewater appliance is analogous to the Steelhead, click on Reports → Diagnostics → TCP Dumps menu item.



The top of the TCP Dumps page displays a list of existing TCP trace dumps and the bottom of page displays controls to create a new trace dump. It also includes the trace dumps that are currently running.



Capture Interfaces: Allows the user to specify which Whitewater interfaces to use when capturing traffic. You can select all interfaces, primary, eth0_0, eth0_1, eth0_2, eth0_3, or auxiliary. Click only one interface per trace dump. The default setting is none. You must specify a capture interface.

The screenshot displays the configuration interface for Cascade Pilot, divided into three main sections:

- Capture Interfaces:** A list of checkboxes for selecting interfaces. A red box highlights the following options:
 - All Interfaces
 - primary aux
 - eth0_0
 - eth0_1
 - eth0_2
 - eth0_3
- Capture Parameters:** A series of input fields and checkboxes:
 - Capture Duration (Seconds):
 - Maximum Capture Size (MB):
 - Buffer Size:
 - Snap Length:
 - Number of Files to Rotate:
 - Only Capture VLAN-Tagged Traffic:
 - Custom Flags:
- Schedule:** A section for scheduling the capture:
 - Schedule Dump
 - Start Date: Start Time:

An **Add** button is located at the bottom left of the interface.

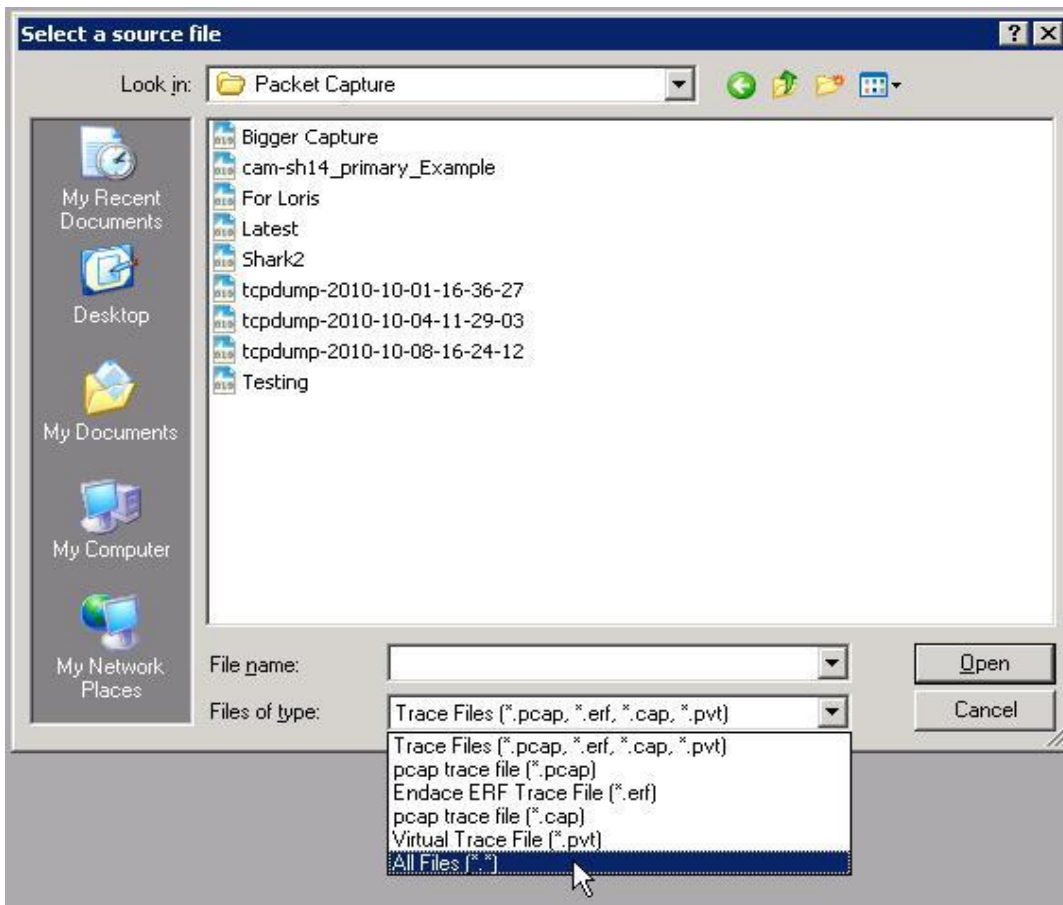
Loading Capture Files in Cascade Pilot

Once the file is saved, you can load it into Cascade Pilot. After launching Cascade Pilot, click the **Add Trace File** icon on the Home ribbon as shown below:

SOLUTION BRIEF: Cascade Pilot for Steelhead and Whitewater



This brings up a standard Explorer window for browsing and selecting files.

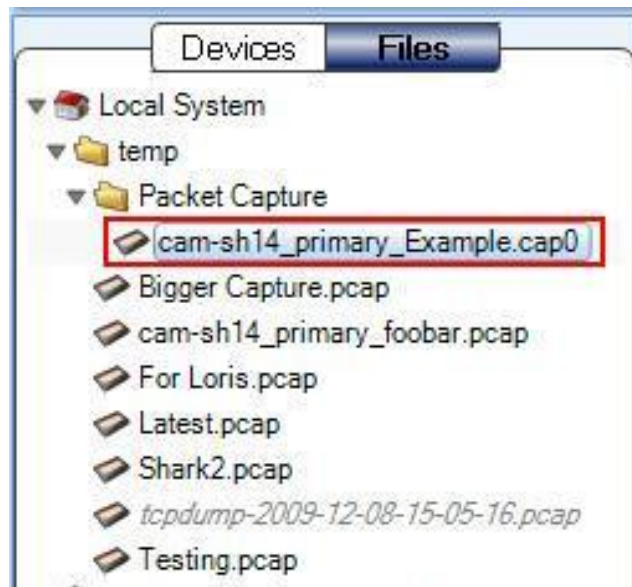


Note: If the file extension was not changed (from .cap0 or .gz to .cap) when saving the capture file on the local system, it will not be visible in this list unless “All Files” is selected in the file type drop down list (shown above).

Once the file is loaded in Cascade Pilot, it appears in under the Files tab at the top left of the screen. If the Devices

SOLUTION BRIEF: Cascade Pilot for Steelhead and Whitewater

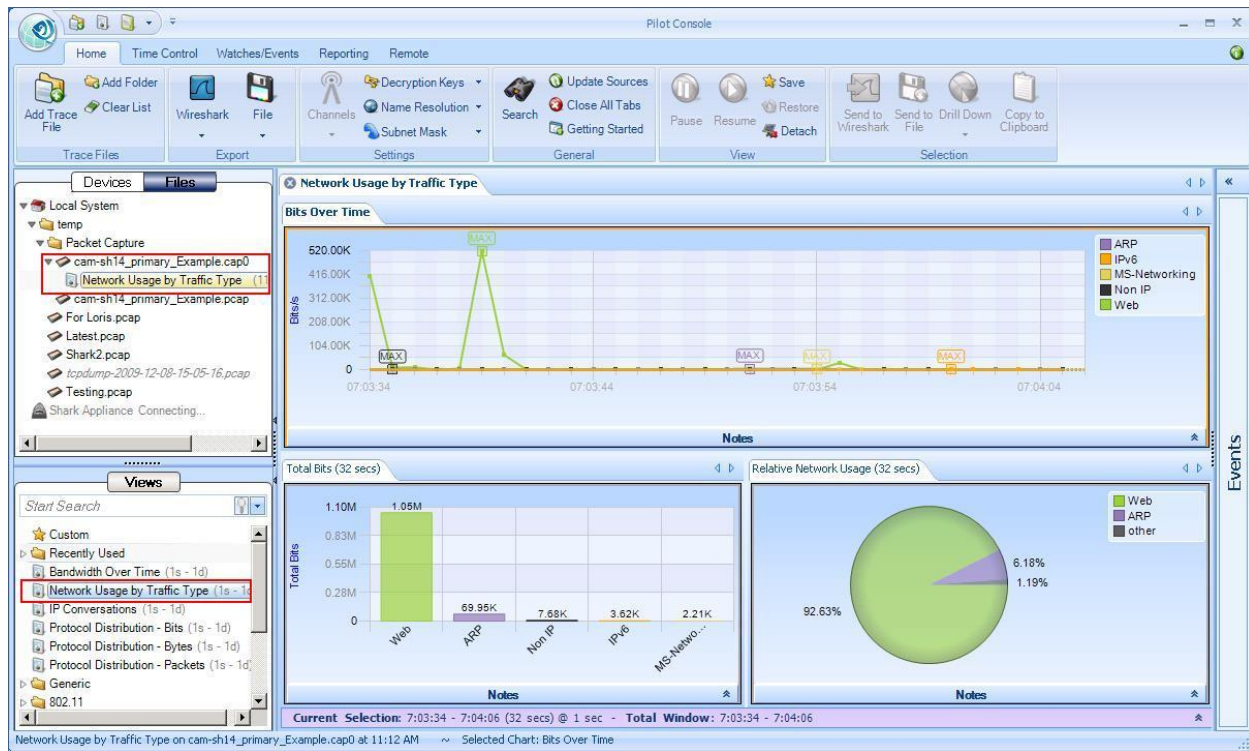
tab is currently selected, the file will be loaded but won't be visible. Clicking **Files** causes the list of locally stored files to appear. The screen shot below shows the packet capture file "Example" loaded in Cascade Pilot:



The folder hierarchy from the local system is shown here (i.e. path to this file) as well as other trace files that were loaded previously. Now that the file is available in Cascade Pilot, the user can drag views from the list at the bottom left of the screen onto the capture files. This causes the view to be applied to the trace file and the results to appear in the area to the right.

The screen shot below shows how the Network Usage by Traffic Type view (highlighted in the Views panel on the bottom left) was dragged over the trace file (highlighted in the files panel on the top right) with the result that the analysis was performed and displayed on the right. Notice that each view being applied to a trace file is shown in an indented list below the relevant trace file.

SOLUTION BRIEF: Cascade Pilot for Steelhead and Whitewater



About Riverbed

Riverbed is the IT performance company. WAN optimization solutions from Riverbed liberate businesses from common IT constraints by increasing application performance, enabling consolidation, and providing enterprise-wide network and application visibility – all while eliminating the need to increase bandwidth, storage or servers.



Riverbed Technology, Inc.
 199 Fremont Street
 San Francisco, CA 94105
 Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
 Farley Hall, London Rd., Level 2
 Binfield
 Bracknell, Berks RG42 4EU
 Tel: +44 1344 354910

Riverbed Technology Pte. Ltd.
 391A Orchard Road #22-06/10
 Ngee Ann City Tower A
 Singapore 238873
 Tel: +65 6508-7400

Riverbed Technology K.K.
 Shiba-Koen Plaza, Bldg. 9F
 3-6-9, Shiba, Minato-ku
 Tokyo, Japan 105-0014
 Tel: +81 3 5419 1990

Copyright © 2010 Riverbed Technology. All Rights Reserved. Riverbed Technology, Riverbed, Steelhead, RiOS, Interceptor, Cascade, Riverbed Cascade, Think Fast, the Riverbed logo, Mazu, and Profiler are trademarks or registered trademarks of Riverbed. All other trademarks mentioned in this website are the property of their respective owners. The trademarks and logos displayed on this website may not be used without the prior written consent of Riverbed or their respective owners.