# App G Direct Captures on Riverbed Accelerators

This workflow is provided in case you prefer to capture directly on the accelerators themselves using tcpdump. However, it is recommended that you capture on the accelerators using Capture Manager, as described in Capturing on Cisco and Riverbed Accelerators.

**Note—**The following information is based on the experiences of engineers working in a lab environment, and is not intended to provide comprehensive documentation about specific devices. If you need detailed information about capturing on a specific device, contact your IS organization or the device vendor.

The direct workflow consists of the following steps.

1) Log in to both accelerators using telnet, putty, or a similar utility.
   **Note—**You must be in Executive mode to capture traffic.

   Ideally, you should be able to run the application and start/stop the captures from the same host. Suppose you are capturing on two accelerators, each of which has one interface for both WAN and LAN traffic. In this case, you would have the following windows open:

   — Accelerator 1, WAN/LAN interface

   — Accelerator 2, WAN/LAN interface

   — Window for running the application to capture

   If the accelerators have in-line modules to support separate LAN and WAN interfaces, you would need to have the following windows open:

   — Accelerator 1, LAN interface

   — Accelerator 1, WAN interface

   — Accelerator 2, LAN interface

   — Accelerator 2, WAN interface

   — Window for running the application to capture

2) Identify the interfaces to capture on (see Identifying the Steelhead Interfaces for Capturing Traffic).

3) Start the capture(s) on each accelerator.

   Steelhead devices use tcpdump, a common utility for capturing traffic. For more information, see Capturing Application Traffic with tcpdump.

4) Run the user-level application transaction you want to capture.

5) When the transaction finishes, stop the capture on each accelerator: make the corresponding window active, then press Ctrl-C.

6) Transfer the packet traces from the accelerators to the AppTransaction Xpert host, as described in Transferring Packet Traces from the Steelhead Device to the AppTransaction Xpert Host.

7) Delete the original packet traces, as described in Deleting Files on the Steelhead Device.

   **Note—**For specific information about how to capture on these devices, consult the Riverbed Steelhead documentation.

8) Fill out the WAN Acceleration Worksheet.

   Although this step is not required, you might find this information useful when import the packet traces into AppTransaction Xpert.

## Identifying the Steelhead Interfaces for Capturing Traffic

Steelhead devices use separate WAN-side and LAN-side interfaces. Therefore, you must capture on two interfaces per device.

These devices can also be deployed in logical in-path mode, with one interface transferring WAN-side and LAN-side traffic (as shown in Figure 11-5 on page ATX-11-4). In this case, you can capture on one interface. The default names for these interfaces are **`wan0_0`** and **`lan0_0`**.

If you cannot identify the exact interface(s) on which to capture, contact someone in your IS organization.

## Transferring Packet Traces from the Steelhead Device to the AppTransaction Xpert Host

Steelhead devices have a web interface that you can use to download packet traces. The following steps outline the general procedure.

1) Log in to the host where you want to download the packet traces.

2) Open a web browser and log in to the web interface of the Steelhead accelerator.

3) Navigate to the Reports > Diagnostic > TCP Dumps page.

4) To download a packet trace, select the filename and save the file.

## Deleting Files on the Steelhead Device

After you download a file, it is good practice to delete the original copy on the Steelhead appliance. To do this, select the checkbox and click Remove Selected Files.