30 Capturing Packets in Riverbed Steelhead Environments

Capturing packets in a Riverbed environment requires some special knowledge and some practice. It is strongly recommend that you read this document and to practice capturing and importing before you start your first production troubleshooting effort.

This document has the following sections:

- Prerequisites
- Setup and Configuration
- Capturing, Importing, and Filtering
- Example

Prerequisites

This workflow assumes familiarity with the following topics:

- General requirements for capturing in WAN-accelerated environments, as described in:
  - Capturing Application Traffic in a WAN-Accelerated Environment
  - Importing WAN-Accelerated Capture Data
- Capturing on WAN accelerators using Capture Manager, as described in Capturing on Cisco and Riverbed Accelerators

Setup and Configuration

The following steps guide you through building traffic source models:

- Step 1: Understand the Steelhead Deployment
- Step 2: Set Up the Agent List
- Step 3: Select the Correct Interfaces
- Step 4: Set Up the Packet Filters
- Step 5: Save the Capture Agent List
- Step 6: Practice/Troubleshoot Captures

Step 1: Understand the Steelhead Deployment

Steelhead accelerators can be deployed in a few different ways. The deployment affects how you capture traffic. This section discusses two critical considerations:

- In-Path Deployment (“How many capture agents do I need?”)
- Addressing Mode (“What IP addresses do I filter on?”)

In-Path Deployment (“*How many capture agents do I need?*”)

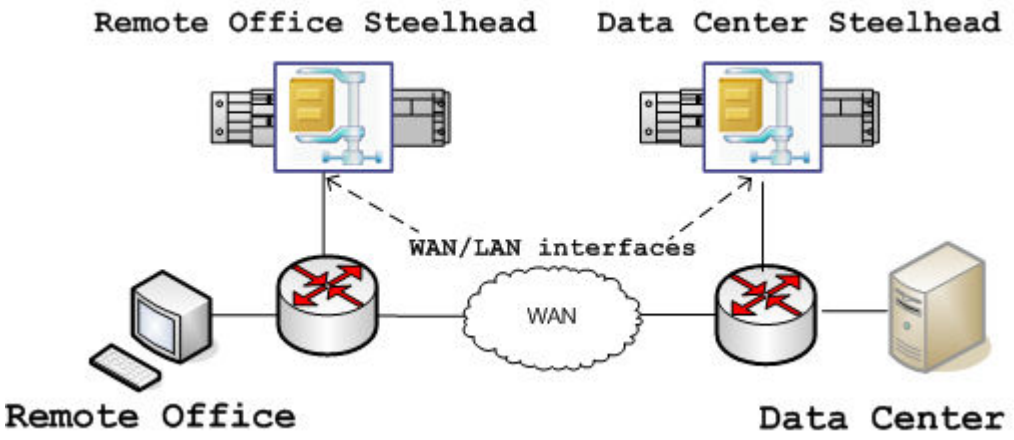
Riverbed Steelhead devices can be deployed in a few different ways. The deployment affects how you capture traffic:

- Virtual In-Path Deployment
- Physical In-Path Deployment

Note—AppTransaction Xpert does not support out-of-path deployment configurations.

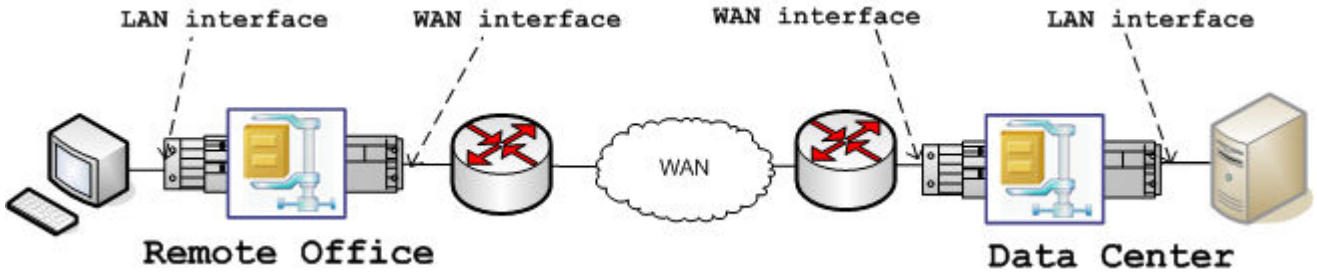
Virtual In-Path Deployment In a virtual in-path deployment, the accelerator handles both LAN and WAN traffic through the same interface. In this deployment, you create one capture agent for each Steelhead; each agent captures both LAN and WAN traffic at the same interface.

Figure 30-1 Virtual In-Path Deployment



Physical In-Path Deployment In this deployment, the accelerator handles traffic through separate LAN and WAN interfaces. In this case, you would create two agents for the device—one for each interface.

Figure 30-2 Physical In-Path Deployment

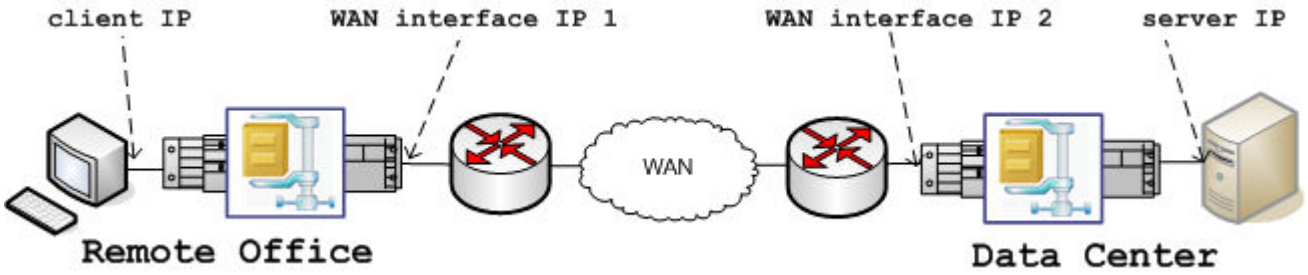


Addressing Mode (“*What IP addresses do I filter on?*”)

When you specify packet filters for your capture agents, you need to consider the addressing mode that the accelerators use when exchanging WAN traffic with each other. Steelhead devices commonly exchange WAN traffic using their own WAN-side IP addresses which are different from the LAN-side IP addresses of the end tiers. This addressing mode is referred to as “non-transparent” or “correct” addressing.

If your accelerators use this mode, your packet filters need to include the WAN (or WAN/LAN) interface IPs on the accelerators in addition to the LAN IPs of the end tiers.

Figure 30-3 Non-Transparent Addressing



Some accelerators also support *transparent addressing*, where the accelerators exchange WAN traffic by reusing the LAN-side IP addresses. In this case, you can filter on the local LAN IPs only and filter out all other IPs.

Step 2: Set Up the Agent List

Create one entry for each interface:

- Virtual in-path device—one agent per device (LAN/WAN interface)
- Physical in-path device—two agents per device (LAN interface and WAN interface)

Use the management IP address of the Steelhead as the hostname of the capture agent. The management IP is the same address that an administrator would use to configure a Steelhead through the web interface (the Steelhead administrator should know this IP address).

When you set up the agent list, it is good practice to

- Specify meaningful names in the Description field (such as `Client LAN`, `Client WAN`, or `Server LAN/WAN`)
- Use a consistent order for the agents in the list (LAN first, WAN second)

Step 3: Select the Correct Interfaces

To capture packets from a Steelhead, you must select the correct appliance interface. The Network adapter list in the Capture Manager will list many different options.

- For virtual in-path configurations, select the (`wan0_0`) interface. Virtual in-path configurations use only the WAN interfaces on the Steelhead.
- For physical in-path configurations, select the (`lanX_X`) or (`wanY_Y`) interface.

Table 30-1 Common Steelhead Monitoring Interfaces

Interface Name	Description
lan0_0	LAN-side interface for physical in-path configurations
wan0_0	WAN interface for physical in-path configurations (also handles LAN traffic in many virtual in-path configurations)

In some cases, the Steelhead will use multiple interfaces to handle the traffic of interest; thus, you might need to capture on multiple interfaces to ensure that you capture the user transaction you want. Note that each individual agent captures on one and only one interface; therefore, if you need to capture on multiple interfaces, you must add multiple agents for the device.

Key Concept—Selecting the wrong interface is a common mistake. If you do not know which interfaces handle the traffic of interest, ask the person who manages the accelerators.

Step 4: Set Up the Packet Filters

It is good practice to assign a packet filter to each capture agent. Packet filters are essential because they help to

- Minimize capture file sizes
- Minimize resource consumption on the Steelhead
- Streamline the workflow for importing your capture data into AppTransaction Xpert

Your goal is to capture unaccelerated packets on the LAN side as well as accelerated WAN packets between the two Steelhead devices. The specific IPs specified in your packet filter depends on the addressing mode used by the Steelhead devices, as described in Addressing Mode (“What IP addresses do I filter on?”).

Beyond this, the filter should exclude all other traffic that you know is irrelevant to the application(s) you want to analyze.

To determine the in-path interface IP for a device, log in to the Riverbed Steelhead management console and choose Configure > Networking > In-path Interface <*interface_name*>.

When setting up your packet filters, it is good practice to

- Include client<-->server traffic in every filter. Even with Correct Addressing, some packets on the WAN might contain the client IP and server IP address.
- Specify one filter per device; if you are capturing on multiple interfaces, use the same filter for all agents on that device.
- Save the packet filter with a meaningful name.

Step 5: Save the Capture Agent List

When you change and update the capture agent settings, save the settings to an Agent List.

Step 6: Practice/Troubleshoot Captures

After you set up the agent list, run a few test captures and import the resulting files into AppTransaction Xpert (as described in the following sections) to verify that the capture agent settings are correct. Some important questions you want to answer at this stage are:

- *Are my packet filters configured correctly?*

  In this context, “configured correctly” means that the agent is capturing packets for all IPs of interest, and only those IPs.

- *Are my agents capturing on the correct interfaces?*

  A specific accelerator might transfer traffic over several different interfaces; you want to be sure that you are capturing on the correct ones. Make sure that you capture on the interface used to handle the traffic of interest. (Do not capture on the management interface of the accelerator.)

- *The capture files are considerably larger than I expect. What can I do to make them smaller?*

  Capturing too much traffic at once can result in heavy network loads or even cause an accelerator to run out of disk space. Your goal is to capture traffic related to one user-level transaction, rather than open-ended streams of traffic, and to filter out traffic from irrelevant IPs.

  If the capture files are larger than you expect or want, consider one or more of the following options:

  — Check the packet filter to verify that you are not capturing on irrelevant IPs.

  — Capture smaller transactions (for example, capturing a 20Mb file transfer rather than a 120Mb transfer).

  — Limit the number of bytes captured per packet.

  Even with a good filter, the capture files will include unrelated traffic. You might want to limit the number of bytes captured per packet, and thereby further minimize the size of the packet trace file. To do this, set the “Maximum size of packet data to store (bytes)” field in the Remote Application Capture Agent Editor.

  WARNING—Consider this option as a “last resort.” Packet slicing might reduce the ability of AppTransaction Xpert to decode the original LAN traffic. If you do use slicing, capture at least 100 bytes of each packet to guarantee that AppTransaction Xpert can decode and merge the capture files.

Capturing, Importing, and Filtering

Capturing Packets

When you capture in a Steelhead environment, do the following:

- Always capture the initial TCP three-way handshake. This handshake enables AppTransaction Xpert to distinguish the LAN and WAN TCP connections.
- Note the capture file name. If you capture on two interfaces of the same device, the capture file names might differ only by a timestamp or by a "_0". Pay attention to where each capture file comes from (WAN side or LAN side).

Importing Capture Files

The full end-to-end import workflow is described in Merging the Capture Files. This section discusses a few key Riverbed-specific issues:

- You must set the "Geographic Location" correctly. AppTransaction Xpert cannot auto-detect these settings; you MUST set these manually. Make sure that capture files from the same Steelhead all have the same location name. It is useful to specify a meaningful name such as "client_site" or "HQ."
- Save the Transaction Analyzer model file immediately after you import the capture data. Use "_unfiltered" in the file name; you might need to return to this file.

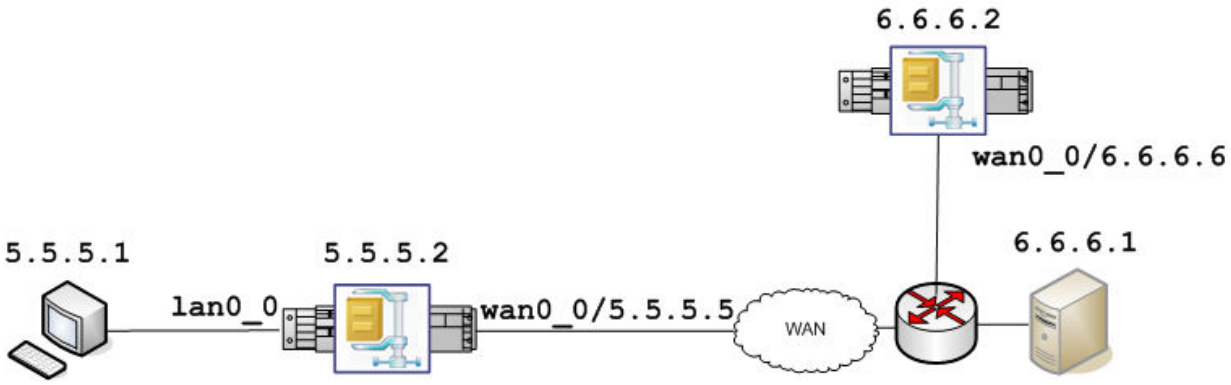
Filtering Irrelevant Traffic

Even if you captured with packet filters, the resulting Transaction Analyzer model file probably still contains irrelevant traffic. It is good practice to filter out this traffic, as described in Step 4: Set Up the Packet Filters.

Example

The the following figure shows a simple Steelhead deployment. The client (left) and server (right) communicate across the WAN through two accelerators. This section describes the various considerations for capture agents and packet filters.

Figure 30-4 Simple Steelhead Deployment



Note the following about this network:

- The client-side accelerator (`5.5.5.2`) has a physical in-line deployment, where separate interfaces handle LAN and WAN traffic.

  Implication: We need to create two separate capture agent entries for this device: one agent for the LAN interface (`lan0_0`) and another for the WAN interface (`wan0_0`).

- The server-side accelerator (`6.6.6.2`) has a virtual in-line deployment, where one interface handles both LAN and WAN traffic.

  Implication: We need to create one capture agent only for this device, which captures at the LAN/WAN interface (`wan0_0`).

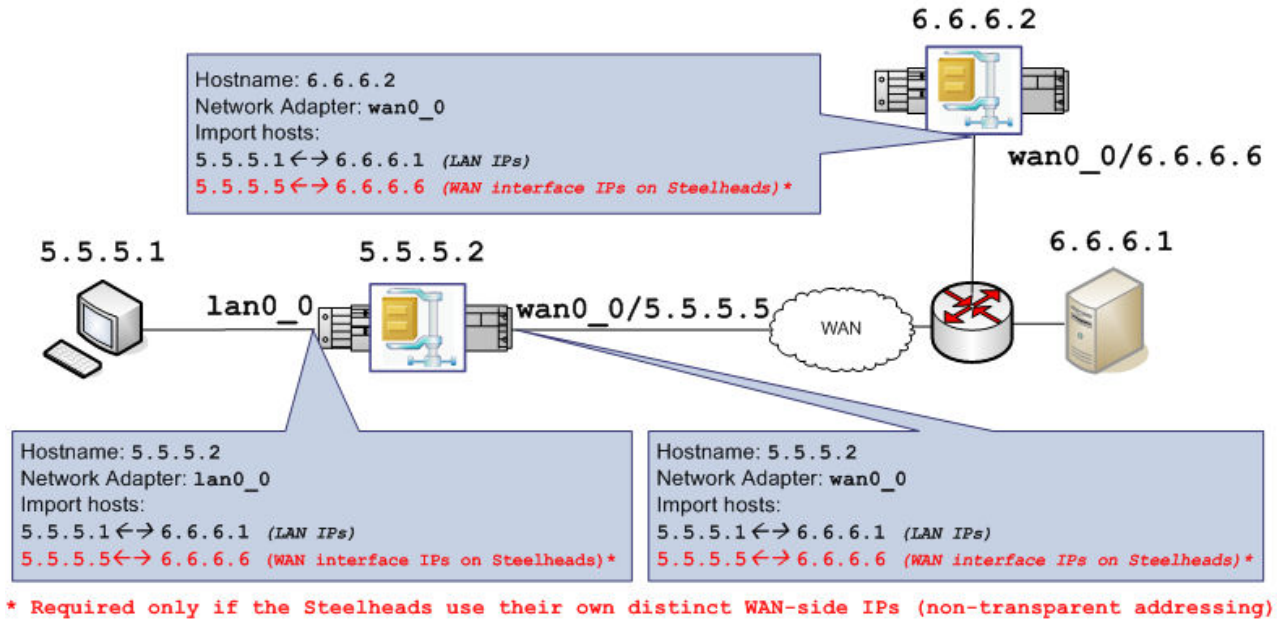
- The two accelerators use their own distinct IP addresses to exchange WAN traffic, instead of reusing the end-tier LAN IPs.

  Implication: We need to specify packet filters that include the IPs of the WAN interfaces on the accelerators (`5.5.5.5<->6.6.6.6`) in addition to the client and server IPs (`5.5.5.1<->6.6.6.1`).

  Note—Some Steelhead appliances can also support a “full transparency” addressing mode, in which the accelerators reuse the LAN IPs (rather than distinct WAN IPs) to exchange traffic with each other. In this case, your packet filters need to include the LAN IPs only.

Given how these devices are deployed, our goal is to set up three capture agents as follows:

Figure 30-5 Simple Steelhead Deployment with Capture Agents



Now we will proceed to set up each of these agents, run a simple capture, and import the packet traces into AppTransaction Xpert. The following sections walk you through the general workflow:

- Client-Side LAN Agent
- Client-Side WAN Agent
- Server-Side LAN/WAN Agent
- Merging the Capture Files

Client-Side LAN Agent

The following table lists the correct settings for this capture agent. The complete Capture Agent Editor entry appears in Figure 30-6.

Table 30-2 Settings for Client-Side LAN Capture Agent

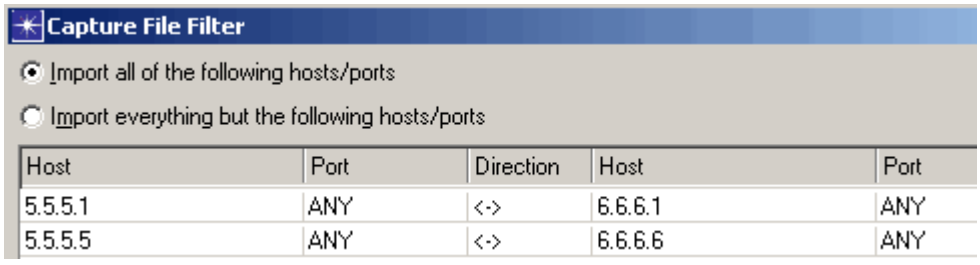
Option	Setting	Comment
Hostname	5.5.5.2	Use the IP address of the management interface on the Steelhead device. **REQUIRED**
Description	Remote Office Steelhead (LAN side, physical in-path lan0_0)	Optional, but recommended
Capture Agent Type	WAN Accelerator	**REQUIRED**
Device	Riverbed Steelhead	**REQUIRED**
Filter	• lan_wan_ips_filter (*correct addressing*) • lan_ips_filter (*fully transparent addressing*)	**REQUIRED** See Specifying the Packet Filter
Network Adapter	[lan0_0]	Interface used for sending and receiving LAN traffic at the remote site **REQUIRED**

Specifying the Packet Filter

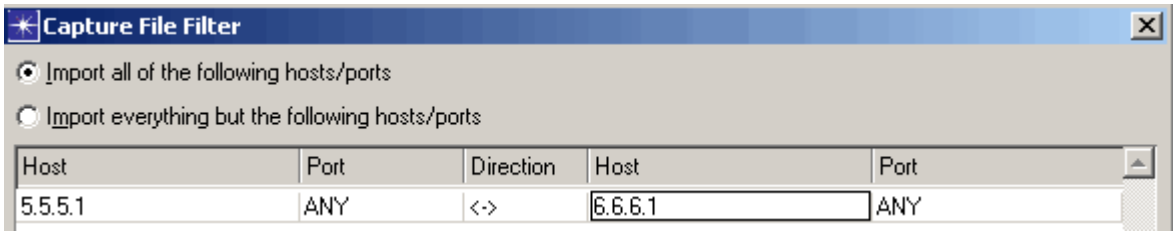
As noted previously, we configure the packet filter based on the addressing mode used by the two accelerators to exchange traffic across the WAN.

In our example the Steelheads exchange traffic using their own distinct IPs, which are different from the LAN-side client and server IPs. This means that we need to capture packets with the LAN IPs for the client and server (`5.5.5.1` and `6.6.6.1`) and also the WAN interface IPs on the accelerators (`5.5.5.5` and `6.6.6.6`).

In the Remote Application Capture Agent Editor, we choose Filter > Edit and specify the packet filter as follows. Then we save the filter with the name `lan_wan_ips_filter`.

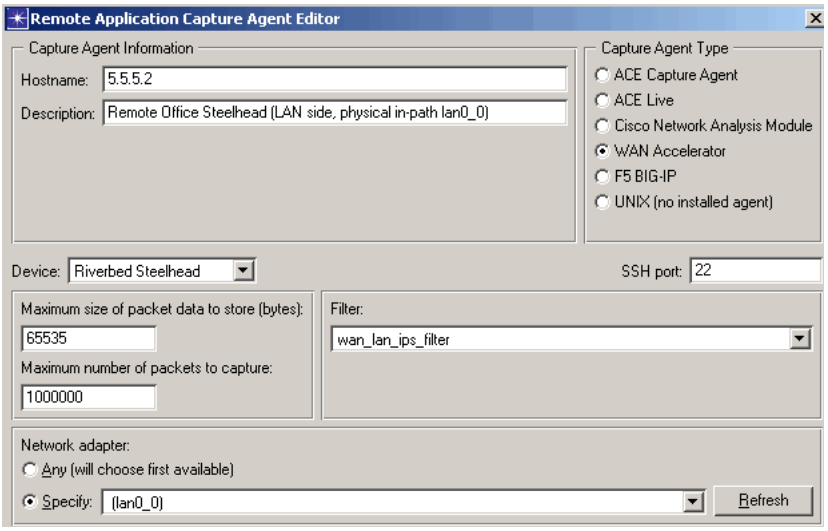


If the Steelheads exchanged traffic across the WAN by reusing the client and server IPs (*fully transparent addressing*), the filter would capture only these IPs and exclude all others. In that case, the filter would look like this:



The completed agent settings for this capture agent look like this:

Figure 30-6 Capture Agent Editor Settings for Client-Side Agent (LAN Interface)



Client-Side WAN Agent

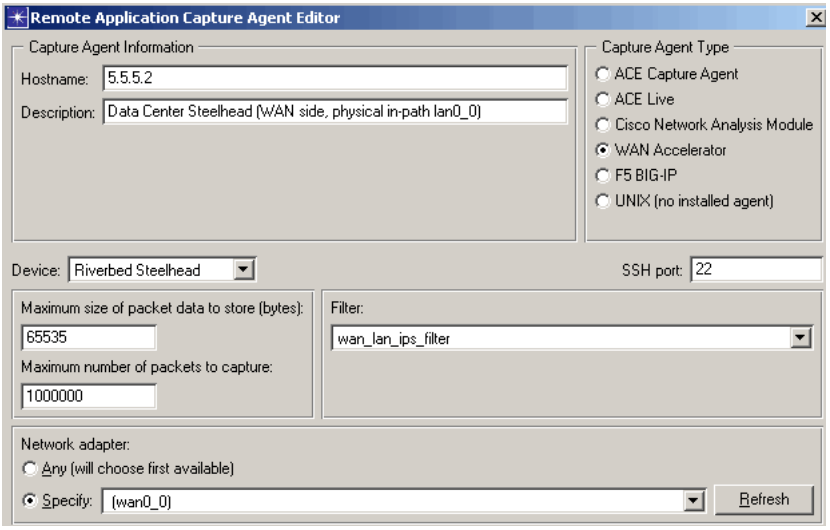
The settings for this capture agent should look like this. Note that the required settings for this agent are nearly identical to those for the Client-Side LAN Agent; the only difference is that this agent captures on the WAN-side network adapter **`wan0_0`**.

Table 30-3 Settings for Client-Side WAN Capture Agent

Option	Setting	Comment
Hostname	5.5.5.2	Use the IP address of the management interface on the Steelhead device. **REQUIRED**
Description	Remote Office Steelhead (WAN side, physical in-path wan0_0)	Optional, but recommended
Capture Agent Type	WAN Accelerator	**REQUIRED**
Device	Riverbed Steelhead	**REQUIRED**
Filter	• lan_wan_ips_filter (*correct addressing*) • lan_ips_filter (*fully transparent addressing*)	**REQUIRED** See Specifying the Packet Filter
Network Adapter	[wan0_0]	Interface used for sending and receiving WAN traffic at the remote site **REQUIRED**

The completed agent settings for this capture agent look like this:

Figure 30-7 Capture Agent Editor Settings for Client-Side Agent (WAN Interface)



Server-Side LAN/WAN Agent

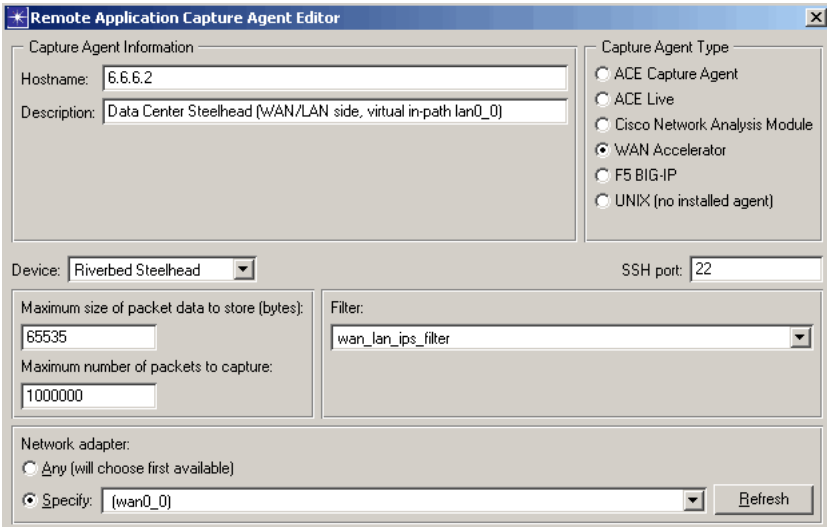
The settings for this capture agent should look like this. This agent requires a packet filter that includes both WAN and LAN IP addresses (**`lan_wan_ips_filter`**). Because this device handles both WAN and LAN traffic through one interface, we need to create only one capture agent for this device.

Table 30-4 Settings for Server-Side WAN/LAN Capture Agent

Option	Setting	Comment
Hostname	6.6.6.2	Use the IP address of the ***management interface*** on the Steelhead device. **REQUIRED**
Description	Data Center Steelhead (WAN/LAN, virtual in-path wan0_0)	Optional, but recommended
Capture Agent Type	WAN Accelerator	**REQUIRED**
Device	Riverbed Steelhead	**REQUIRED**
Filter	• lan_wan_ips_filter (*correct addressing*) • lan_ips_filter (*fully transparent addressing*)	**REQUIRED** See Specifying the Packet Filter
Network Adapter	[wan0_0]	Interface used for sending and receiving both LAN and WAN traffic at the data center **REQUIRED**

The completed agent settings for this capture agent look like this:

Figure 30-8 Capture Agent Editor Settings for Server-Side Agent (WAN/LAN Interface)



Merging the Capture Files

Now that we have set up the capture agents, we are ready to perform captures. We capture a simple client/server transaction and now have the following capture files:

1) client_accelerator_lan

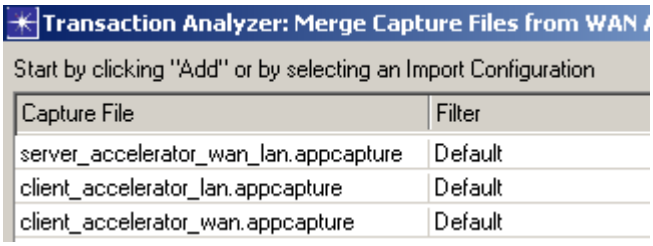
2) client_accelerator_wan

3) server_accelerator_wan_lan

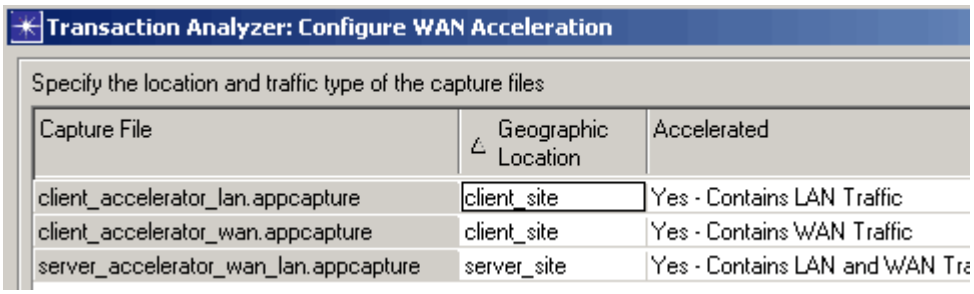
We will now go through the process of merging these files:

1) In AppTransaction Xpert, choose Merge > Capture Files from a WAN-accelerated Environment.

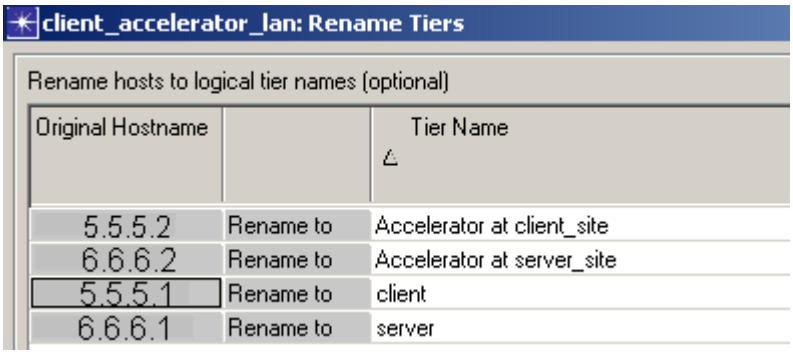
2) The first window that appears prompts us for the capture files and the packet filter to apply for each file.



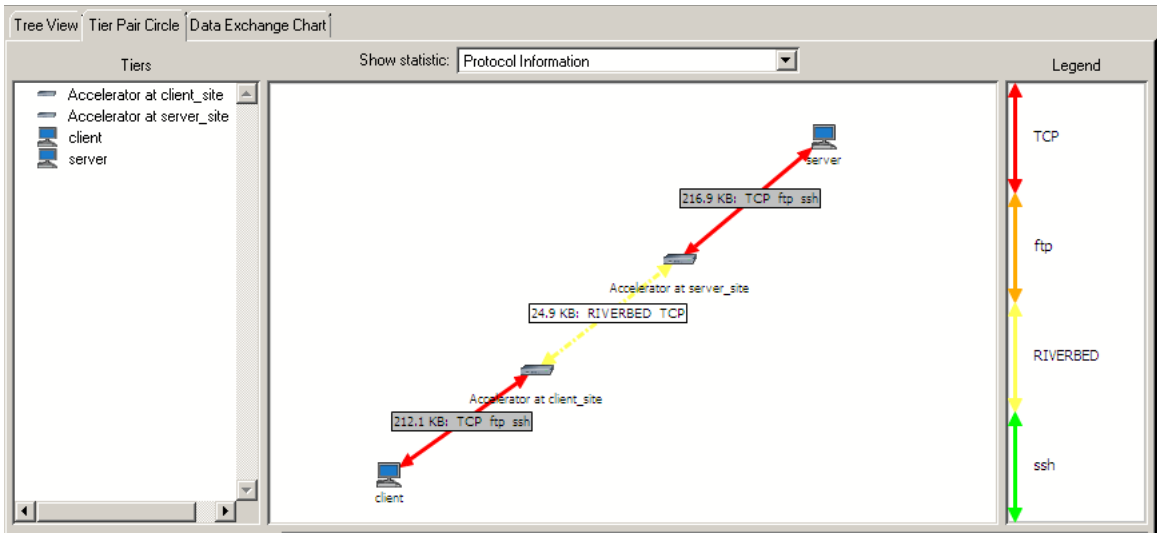
3) Next, we are prompted to specify the type of traffic in each capture file (LAN only, WAN only, WAN/LAN, or no accelerated traffic). Note that AppTransaction Xpert can often detect the type of traffic in each file and select the correct setting for this file. If AppTransaction Xpert does not detect the WAN-side traffic correctly, you might have captured the traffic incorrectly.



4) Next, we are prompted to specify the logical tier names for the IP addresses found in the capture files.



5) The end result is a four-tier application: client, client-side accelerator, server-side accelerator, and server.



Because the accelerators work to reduce the amount of data transmitted across the WAN, the resulting Transaction Analyzer file has more LAN than WAN traffic.

Note—When you merge your capture data, it is good practice to determine whether the resulting Transaction Analyzer file has the characteristics you expect. If you get unexpected results after you merge your capture files, this indicates that you captured the data incorrectly or that you specified the wrong settings during the merge process.

Remember that your “expected results” can vary depending on the network and the traffic you want to capture. For example, you might be unable to predict beforehand the WAN source/destination IPs for the traffic of interest. In this case, you might need to capture a fair amount of irrelevant traffic initially and then filter out this traffic after merging.

For specific troubleshooting advice, see Troubleshooting WAN Acceleration Imports.