29 Capturing Packets in Cisco WAAS Environments

Capturing packets in a WAAS environment requires some special knowledge and some practice. It is strongly recommend that you read this document and that you 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 WAAS 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 WAAS Deployment

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

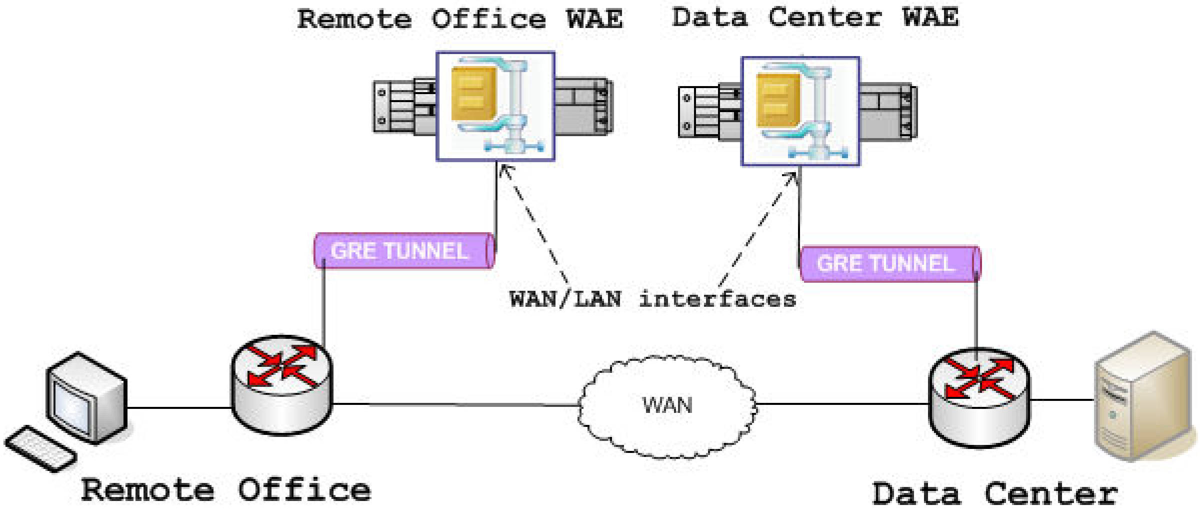
- In-Path Deployment ("How many capture agents do I need?")
- Addressing Mode ("What IP addresses do I filter on?")

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

Virtual In-Path Deployment In a virtual in-path deployment, the accelerator handles both LAN and WAN traffic through the same interface. The most common deployment uses WCCP to redirect traffic to the WAE device. The redirected traffic flows through a GRE tunnel, gets accelerated, and then travels out the same physical interface to be sent over the WAN.

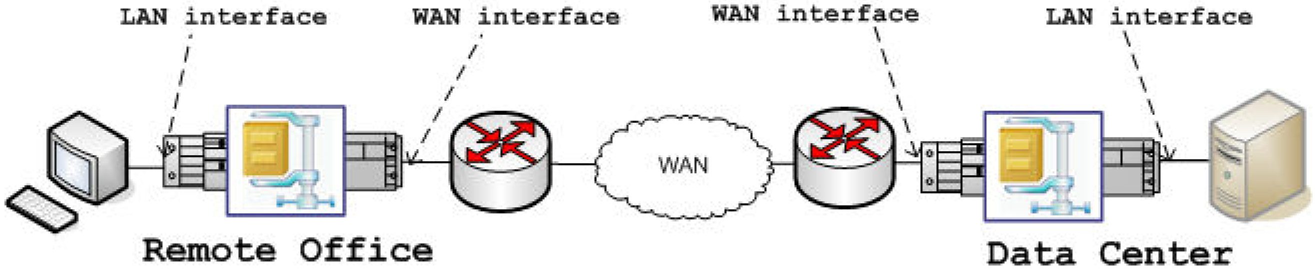
In this deployment, you create one capture agent for the accelerator, which captures both LAN and WAN traffic at the same interface.

Figure 29-1 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 29-2 Physical In-Path Deployment

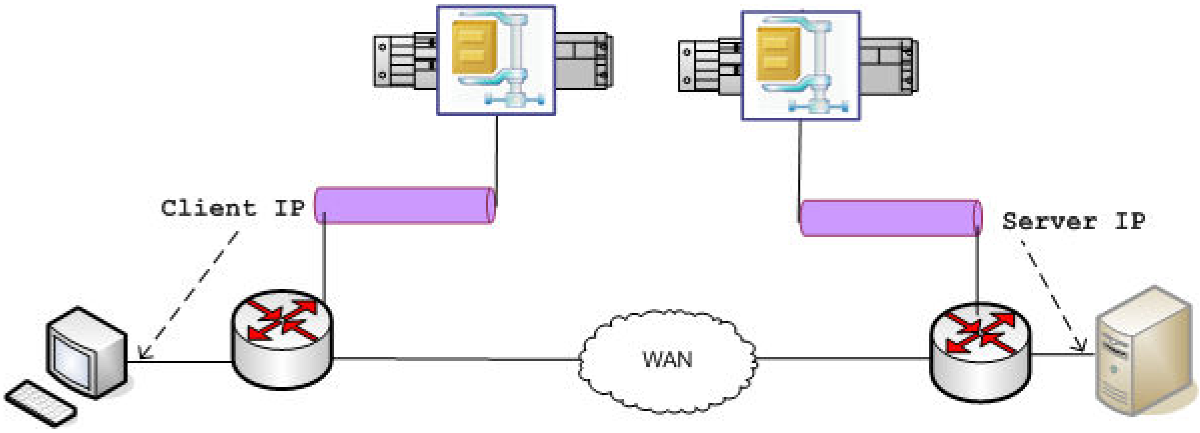


Note—AppTransaction Xpert does not support out-of-path deployment configurations.

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. The most common mode is called *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.

Table 29-1 Transparent Addressing



Some accelerators from other vendors—such as some Steelhead models—can exchange WAN traffic using their own unique WAN-side IP addresses. In this case, your packet filters would also need to include the WAN (or WAN/LAN) interface IPs on the accelerators themselves. This addressing mode is not commonly used in WAAS systems, however. For a more detailed discussion of this addressing mode, see Capturing Packets in Riverbed Steelhead Environments.

Step 2: Set Up the Agent List

Create capture agents for each accelerator:

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

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 WAE device, you must select the correct network interface. The Network Adapter list in the Capture Manager will list several different options. For typical WAAS configurations, select the Ethernet interface that carries the production traffic (eth0, eth2, …).

The following table shows some interfaces that are commonly used on WAE devices. This set of interface names is provided as an example, and will probably be different from what you would see in the Capture Agent Editor (the Network Adapter pull-down menu shows only interfaces on the appliance whose status is currently “up”).

Table 29-2 Common WAE Device Interfaces

Interface Name	Description
eth0	GigabitEthernet 1/0
eth1	GigabitEthernet 1/0
eth2	InlinePort 1/1/wan
eth3	InlinePort 1/1/lan
eth4	InlinePort 1/0/wan
eth5	InlinePort 1/0/lan

In some cases, the WAE device will use multiple interfaces to handle the traffic of interest; thus, you might need to capture on multiple interfaces to ensure that you get the specific user transaction. 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 specify a packet filter for each capture agent. Packet filters are essential because they help to

- Minimize capture file sizes
- Minimize resource consumption on the accelerator
- 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 packets between the two WAE devices. If the LAN and WAN packets use the same IP addresses—the standard addressing scheme used in Cisco WAAS—you would specify a filter so that the agent captures traffic for the LAN-side IPs alone:

- client IP
- server IP

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

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

- Make the filter as strict as possible (that is, exclude all traffic that you know is irrelevant)
- Specify one filter per device; if you are capturing on multiple interfaces, use the same filter for all agents on that device.

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).

  — Lmit 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

After you complete the setup process, you can start capturing packets. When you capture in a WAAS environment, it is good practice to

- Always capture the initial TCP three-way handshake for all connections of interest. This handshake enables AppTransaction Xpert to distinguish the LAN and WAN TCP connections.
- If your accelerators use GRE tunnels, use AppTransaction Xpert release 16.0 (and higher). GRE packets have two IP layers, an "outer" (tunnel endpoint IPs) and an "inner" (original source/destination IPs). Starting with release 16.0, the capture engine automatically drills into GRE packets and filters these packets based on the original source/destination IPs.
- 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 which capture file comes from the WAN side and from the 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 Cisco WAAS-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 WAAS device all have the same location name. It is useful to specify a meaningful name such as “Headquarters” 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.

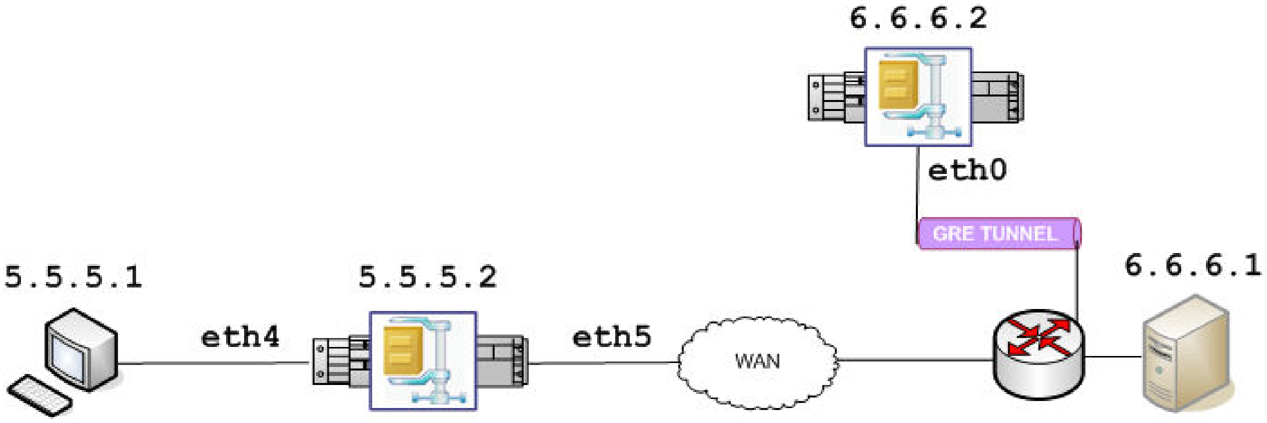
Filtering Irrelevant Traffic

Even if you captured with packet filters, the resulting Transaction Analyzer model file might still contain 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 Cisco 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 29-3   Simple WAE 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 (`eth4)` and another for the WAN interface (`eth5)`.

- 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 (`eth0`).

- The two accelerators reuse LAN-side IP addresses to exchange WAN traffic, rather than using distinct WAN-side IPs; this mode is often referred to as "transparent addressing."

  Implication: We can specify a packet filter that captures only the LAN-side addresses of the client and server (`5.5.5.1` and `6.6.6.2`) and filters out all other packets. This filter will capture both WAN and LAN packets between the client and server.

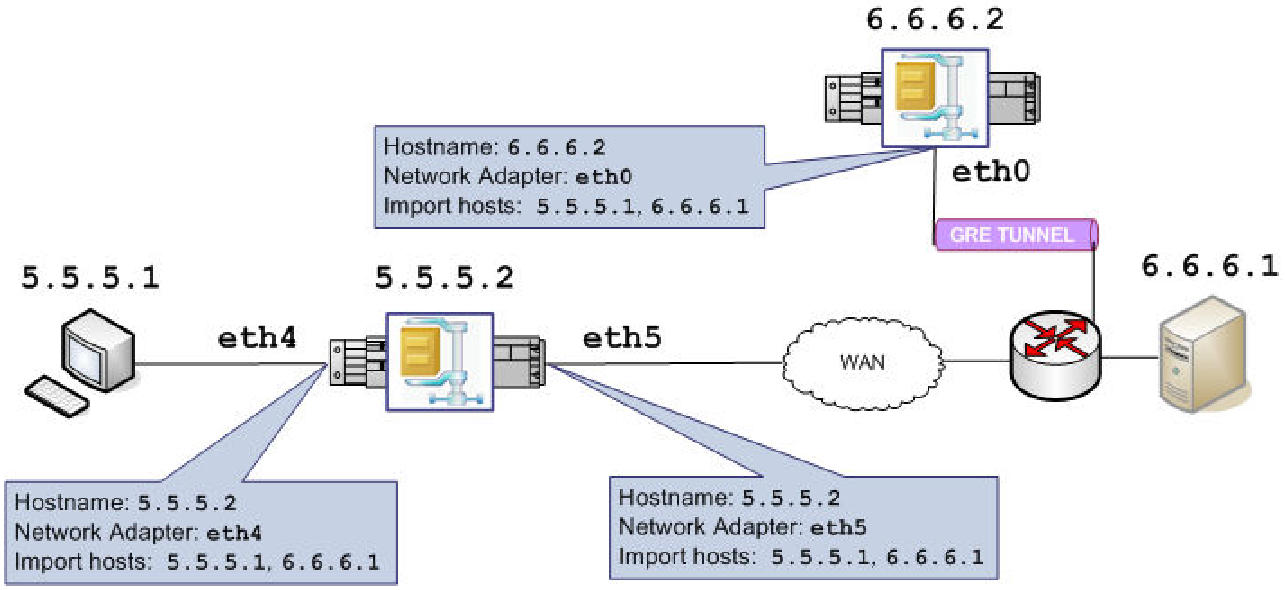
  If the accelerators used their own distinct WAN-side IP addresses to exchange traffic, we would need to capture these addresses as well.

- Traffic is redirected to the server-side accelerator through a GRE tunnel.

Implication: If your accelerators use GRE tunnels, you should use AppTransaction Xpert release 16.0 (or higher) when capturing. Starting with this release, the capture engine can drill into GRE packets and filter these packets based on the original source/destination IPs (not the GRE tunnel endpoint IPs).

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

Figure 29-4 Simple WAE Deployment with Capture Agents



Now we will proceed to set up each of these agents and configure to capture and filter GRE packets. 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 29-5 on page AW-29-11.

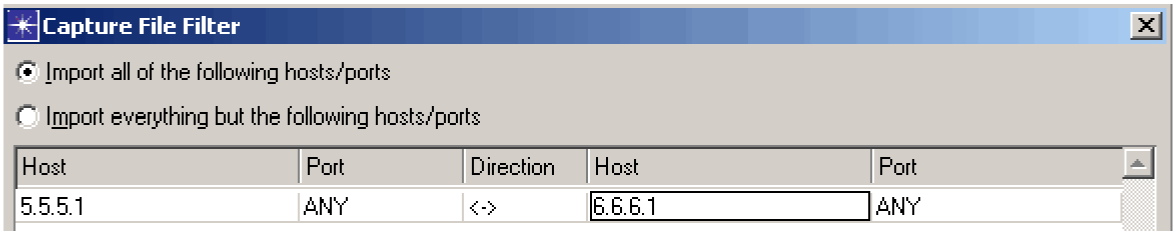
Table 29-3 Settings for Client-Side LAN Capture Agent

Option	Setting	Comment
Hostname	5.5.5.2	Use the IP address of the management interface on the WAE device. **REQUIRED**
Description	client-side WAE (LAN side, physical in-path eth5)	Optional, but recommended
Capture Agent Type	WAN Accelerator	**REQUIRED**
Device	Cisco WAAS	**REQUIRED**
Filter	wae_example_filter	**REQUIRED** See Specifying the Packet Filter
Network Adapter	[eth4]	Interface used for sending and receiving LAN traffic at the remote site **REQUIRED**

Specifying the Packet Filter

As noted previously, the accelerators in this network reuse the client and server IP addresses to exchange WAN-side packets. This means that we define a packet filter to include the client and server IPs only, and exclude all other packets.

In the Remote Application Capture Agent Editor, we choose Filter > Edit and specify the packet filter as follows:



Capture File Filter

● Import all of the following hosts/ports

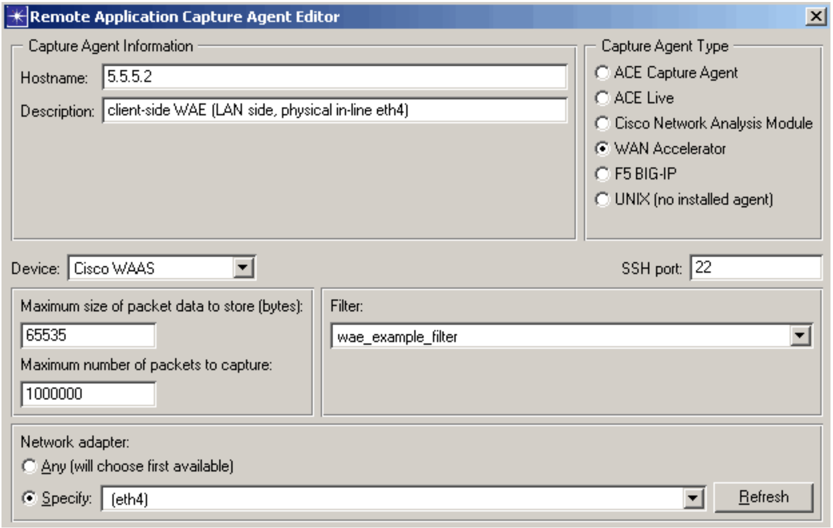
○ Import everything but the following hosts/ports

Host	Port	Direction	Host	Port
5.5.5.1	ANY	<->	6.6.6.1	ANY

Then we save the filter with the name `wae_example_filter`. We will use this packet filter for all three capture agents.

The completed agent settings look like this:

Figure 29-5 Capture Agent Editor Settings for Client-Side Agent (LAN Interface)



Remote Application Capture Agent Editor

Capture Agent Information

Hostname: 5.5.5.2

Description: client-side WAE (LAN side, physical in-line eth4)

Capture Agent Type

- ○ ACE Capture Agent
- ○ ACE Live
- ○ Cisco Network Analysis Module
- ● WAN Accelerator
- ○ F5 BIG-IP
- ○ UNIX (no installed agent)

Device: Cisco WAAS

SSH port: 22

Maximum size of packet data to store (bytes): 65535

Maximum number of packets to capture: 1000000

Filter: wae_example_filter

Network adapter:

- ○ Any (will choose first available)
- ● Specify: (eth4)

Client-Side WAN Agent

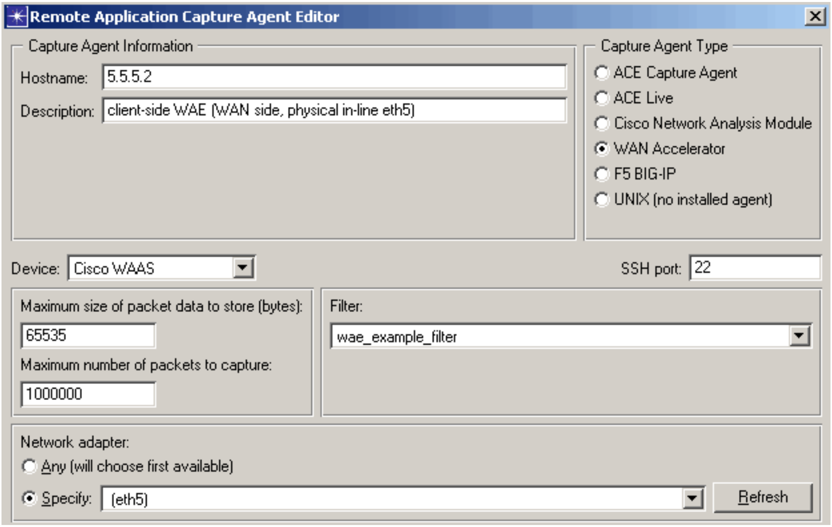
The settings for this capture agent should look like this. Note that the required settings for this agent are nearly identical to those for the Client-Side LAN Agent; the only difference is that this agent captures on the WAN-side network adapter `eth5`.

Table 29-4 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 WAE device. **REQUIRED**
Description	client-side WAE (WAN side, physical in-path eth5)	Optional, but recommended
Capture Agent Type	WAN Accelerator	**REQUIRED**
Device	Cisco WAAS	**REQUIRED**
Filter	wae_example_filter	**REQUIRED** See Specifying the Packet Filter
Network Adapter	[eth5]	Interface used for sending and receiving WAN traffic at the remote site **REQUIRED**

The completed agent settings look like this:

Figure 29-6 Capture Agent Editor Settings for Client-Side Agent (WAN Interface)



Remote Application Capture Agent Editor

Capture Agent Information

Hostname: 5.5.5.2

Description: client-side WAE (WAN side, physical in-line eth5)

Capture Agent Type

○ ACE Capture Agent
○ ACE Live
○ Cisco Network Analysis Module
● WAN Accelerator
○ F5 BIG-IP
○ UNIX (no installed agent)

Device: Cisco WAAS

SSH port: 22

Maximum size of packet data to store (bytes): 65535

Maximum number of packets to capture: 1000000

Filter: wae_example_filter

Network adapter:
○ Any (will choose first available)
● Specify: (eth5)

Server-Side LAN/WAN Agent

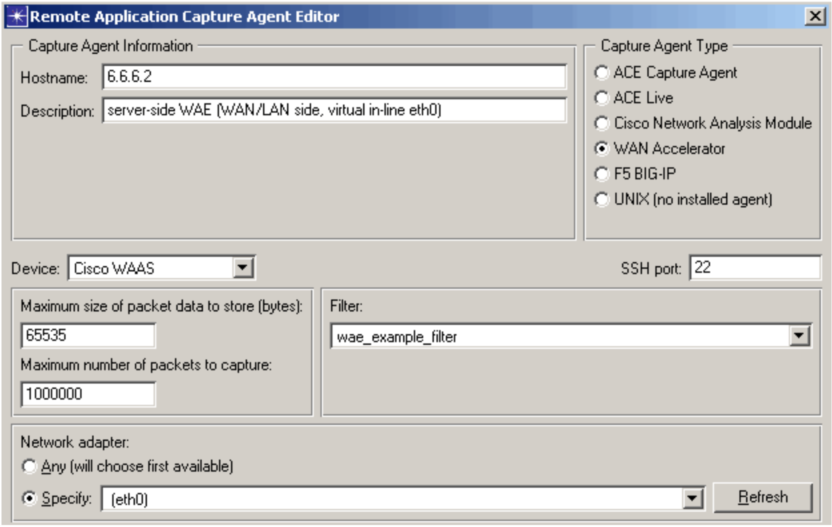
The settings for this capture agent should look like this. The required settings for this agent are nearly identical to the other two agents, except that this agent captures on a different host (`6.6.6.2`) and network adapter (`eth0`). Because this device handles both WAN and LAN traffic through one interface, we need to create only one capture agent for this device.

Table 29-5 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 WAE device. **REQUIRED**
Description	server-side WAE (WAN/LAN, virtual in-path eth2)	Optional, but recommended
Capture Agent Type	WAN Accelerator	**REQUIRED**
Device	Cisco WAAS	**REQUIRED**
Filter	wae_example_filter	**REQUIRED** See Specifying the Packet Filter
Network Adapter	[eth0]	Interface used for sending and receiving both LAN and WAN traffic at the data center **REQUIRED**

The completed agent settings look like this:

Figure 29-7 Capture Agent Editor Settings for Server-Side Agent (WAN/LAN Interface)



Remote Application Capture Agent Editor

Capture Agent Information

Hostname: 6.6.6.2

Description: server-side WAE (WAN/LAN side, virtual in-line eth0)

Capture Agent Type

○ ACE Capture Agent
○ ACE Live
○ Cisco Network Analysis Module
● WAN Accelerator
○ F5 BIG-IP
○ UNIX (no installed agent)

Device: Cisco WAAS

SSH port: 22

Maximum size of packet data to store (bytes): 65535

Maximum number of packets to capture: 1000000

Filter: wae_example_filter

Network adapter:
○ Any (will choose first available)
● Specify: (eth0)

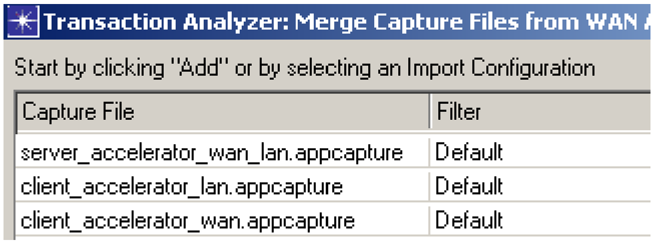
Merging the Capture Files

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 locations where they were captured.

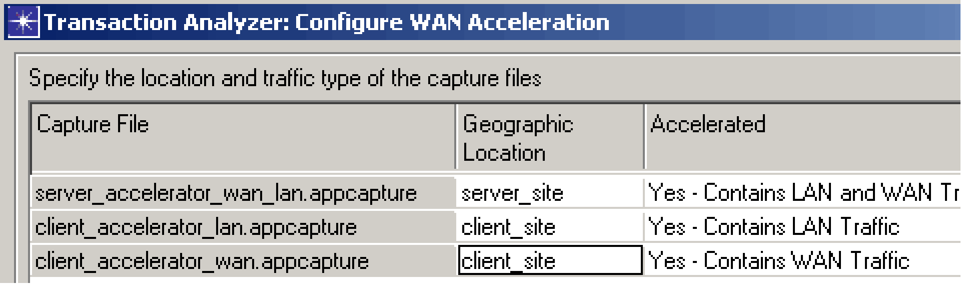


Transaction Analyzer: Merge Capture Files from WAN A

Start by clicking "Add" or by selecting an Import Configuration

Capture File	Filter
server_accelerator_wan_lan.appcapture	Default
client_accelerator_lan.appcapture	Default
client_accelerator_wan.appcapture	Default

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) and the geographic location where each capture file was generated. Note that AppTransaction Xpert can often detect the type of traffic in each file and select the correct setting for this file.



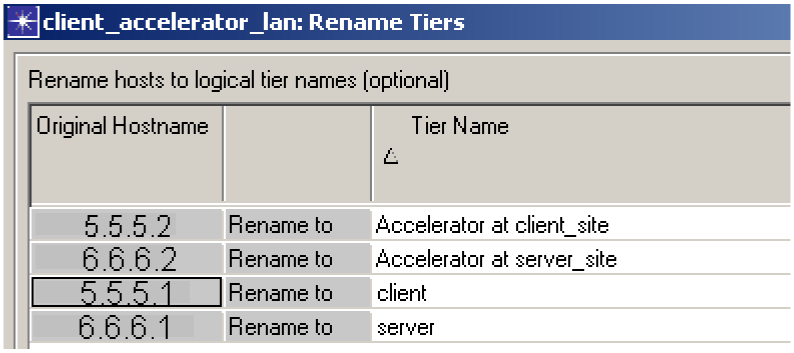
Transaction Analyzer: Configure WAN Acceleration

Specify the location and traffic type of the capture files

Capture File	Geographic Location	Accelerated
server_accelerator_wan_lan.appcapture	server_site	Yes - Contains LAN and WAN Tr
client_accelerator_lan.appcapture	client_site	Yes - Contains LAN Traffic
client_accelerator_wan.appcapture	client_site	Yes - Contains WAN Traffic

Note—You must set the “Geographic Location” correctly; AppTransaction Xpert cannot auto-detect these settings. Make sure that capture files from the same WAAS device all have the same location name. It is useful to specify a meaningful name such as “Headquarters” or “HQ.”

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

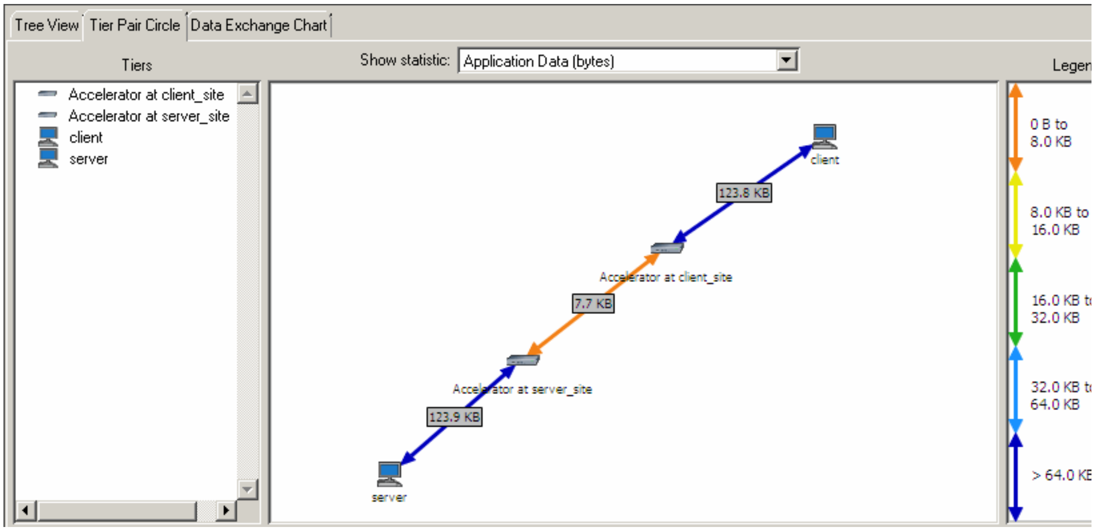


client_accelerator_lan: Rename Tiers

Rename hosts to logical tier names (optional)

Original Hostname		Tier Name
5.5.5.2	Rename to	Accelerator at client_site
6.6.6.2	Rename to	Accelerator at server_site
5.5.5.1	Rename to	client
6.6.6.1	Rename to	server

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



Tiers

- Accelerator at client_site
- Accelerator at server_site
- client
- server

Show statistic: Application Data (bytes)

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.