11 Capturing Application Traffic in a WAN-Accelerated Environment

A pair of synchronous accelerators adds two tiers and one intermediate segment to any application transaction. This means that, to analyze an application in a WAN-optimized environment, you must capture traffic at four different locations:

1) LAN traffic at the client

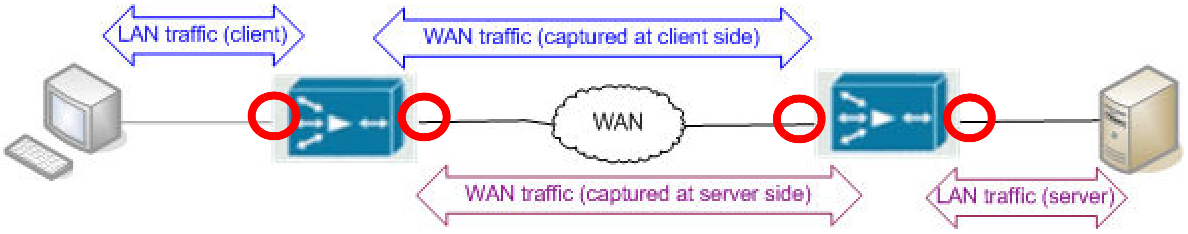
2) WAN traffic between the accelerators (captured at client side)

3) WAN traffic between the accelerators (captured at server side)

4) LAN traffic at the server

To capture an application in the environment shown in the following figure, you might need to capture at four different locations. You might be able to capture at fewer locations, however, depending on the network configuration and the specific type of accelerator. Some devices enable you to capture both LAN and WAN traffic in one packet trace; in this case you can capture at two locations only (that is, on the devices themselves).

Figure 11-1 Required Traffic for Two-Tier Application in a WAN-Optimized Environment


LAN traffic (client)
WAN traffic (captured at client side)
WAN
WAN traffic (captured at server side)
LAN traffic (server)

This section includes the following topics:

- Direct Captures (On the Accelerators)
  - — Capturing on WAN Accelerators (Direct Captures): Workflow Descriptions
  - — Selecting the Interfaces on the Accelerator (Single- vs. Dual-Interface Captures)
- Capturing on Cisco and Riverbed Accelerators
- Capturing on Other Accelerators
- Indirect Captures (Near the Accelerators)
  - — Capturing near WAN Accelerators (Indirect Captures): Workflow Descriptions

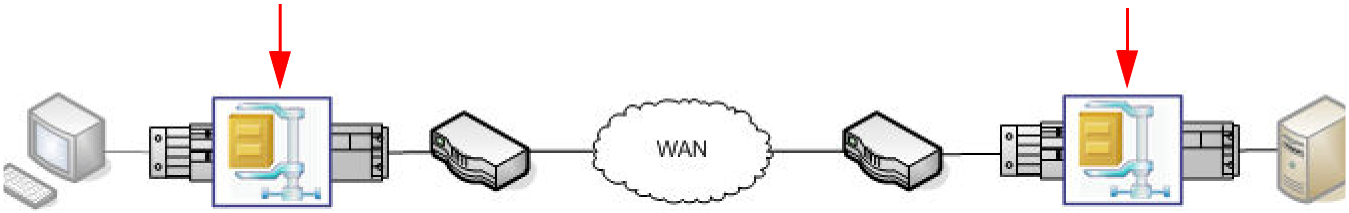
Related Topics

- *WAN Accelerators and AppTransaction Xpert*

Direct Captures (On the Accelerators)

You can capture directly on an accelerator if you have privileges to capture traffic on that device.

Figure 11-2 Direct Capture (On the Accelerators)



The advantages of this approach are:

- Because the accelerator sees both the LAN-side and the WAN-side traffic, you can capture at the two accelerators only. You do not need to capture at the end tiers.
- The initial set-up process can be simpler than capturing near the device. Because the accelerator already has capture functionality, you do not need to set up any external hosts so that they can capture the relevant traffic.

The disadvantages of this approach are:

- This approach might be impossible in your specific organization. If your IS department does not allow you to capture on the accelerators, you will have no choice but to capture near the devices.
- It might be more difficult to perform simultaneous captures if you are capturing on accelerators that do not have an interface that specifically supports simultaneous captures (such as the Capture Manager interface for Cisco and Riverbed devices, or the web interface for Juniper devices).

Capturing at LAN-Side Tiers

You must also capture at the end tier within a LAN if both the following conditions are true:

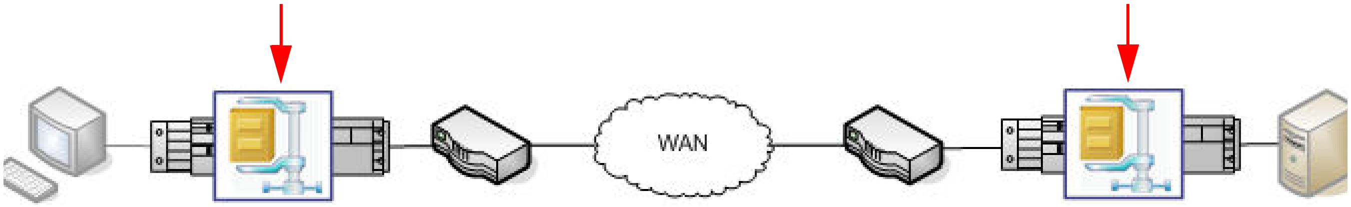
- The application of interest includes traffic that does not go through the accelerator (that is, the router sends this traffic directly into the LAN without going through the accelerator).
- You want to study this traffic in AppTransaction Xpert.

If you cannot capture directly on the accelerators, see Indirect Captures (Near the Accelerators).

Capturing on WAN Accelerators (Direct Captures): Workflow Descriptions

The following sections describe how to select the correct interfaces and how to capture on specific types of devices.

Figure 11-3 Capturing Directly on the Accelerators



Key Concept—Remember that you need to capture both *LAN and WAN traffic at the client side* and *LAN and WAN traffic at the server side*.

The following topics are described in detail:

- Selecting the Interfaces on the Accelerator (Single- vs. Dual-Interface Captures)
- Capturing on Cisco and Riverbed Accelerators
- Capturing on Other Accelerators

Note—The following sections are 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.

Selecting the Interfaces on the Accelerator (Single- vs. Dual-Interface Captures)

Before you can start capturing on the accelerator, you must to determine the interfaces on which to capture. Remember that you need to capture both the LAN-side and the WAN-side traffic.

One factor to consider is how a specific accelerator is deployed. This is highly vendor- and model-specific. There are two general types of deployments:

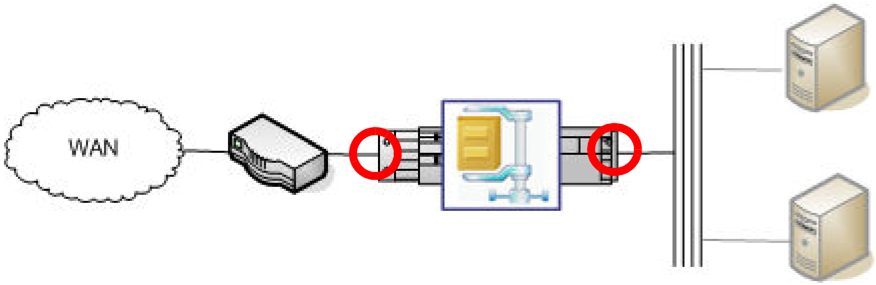
- Physical in-path deployment—The accelerator is in the direct physical path between the WAN gateway and the end tier.
- Virtual in-path deployment—The accelerator is in a virtual/logical path, but not in a direct physical path, between the WAN gateway and the end tier.

Physical in-path deployment

The accelerator is in the direct physical path between the WAN gateway and the end tiers. It receives traffic through one interface, processes the traffic, and transmits it through a different interface.

In this type of deployment, you must capture from two interfaces (LAN-side and WAN-side), as shown in the following figure. Some devices allow you to capture on both interfaces, and thereby generate a single packet trace that contains traffic from both interfaces.

Figure 11-4 Physical In-Path Configuration

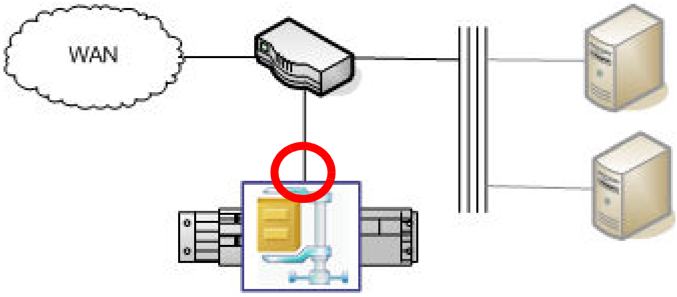


Virtual in-path deployment

In this type of deployment—also called a *logical in-path deployment*—the accelerator is in a virtual path, but not the physical path, between the end tiers. Routers intercept packets as they are received; based on preconfigured policies, the routers then redirect some of these packets to accelerators. Typically, these routers use PBR (Policy Based Routing) and WCCP (Web Cache Communications Protocol) to reroute traffic to the accelerators.

Because the accelerator has one interface that sees both LAN and WAN traffic, you can capture both types of traffic from this one interface. (See the following figure.)

Figure 11-5 Virtual In-Path Configuration



Capturing on Cisco and Riverbed Accelerators

You can capture directly on Cisco and Riverbed WAN accelerators using Capture Manager. Capture Manager uses the built-in tcpdump functionality on the accelerator—not an installed agent—to capture traffic and communicate with the accelerator over a secure SSH connection. This functionality makes no changes to the accelerator and stores no data on the device (except the tcpdump data file, which is immediately downloaded to Capture Manager when you finish the capture).

This section has the following subsections:

- Important Notes
- Workflow Description
- Configuring Capture Options on the Cisco/Riverbed Device

Important Notes

When capturing on an accelerator, note the following:

- You can run on-demand captures only; continuous captures are not supported on WAN accelerators.
- This functionality supports captures on the following devices:
  - — Cisco WAAS
  - — Riverbed Steelhead

  For a complete list of the supported versions, see the system requirements on the Riverbed Support Website.
- You must have a valid username/password for each accelerator on which you want to capture.

  Note—For Riverbed Steelhead accelerators, you must have administrator privileges.
- SSH (Secure Shell) must be enabled on the device.
- The first time you connect to an accelerator in the current AppTransaction Xpert session, you must enter a valid username/password for that device. (You can choose to retain the usernames/passwords for the current session, but AppTransaction Xpert does not save the login information.)

- You cannot store packet traces on the accelerator. When you finish a capture, Capture Manager downloads all capture data from all accelerators.
- Because tcpdump creates a separate copy of each captured packet, you must take care not to consume all available disk space on the accelerator while the capture is in progress. You must configure the agent to limit the size of the resulting packet traces. For more information, see Configuring Capture Options on the Cisco/Riverbed Device.

Workflow Description

The following procedure describes the workflow for capturing on a Cisco or Riverbed accelerator.

Procedure 11-1 Capturing Traffic on Cisco WAE or Riverbed Steelhead Accelerators

1 Verify that you have a valid username and password for each accelerator on which you want to capture.

Note—For Riverbed Steelhead accelerators, you must have administrator privileges.

2 Open Capture Manager and click the On-Demand tab.

3 Create an agent list on the accelerators if you have not already done so.

For each accelerator interface on which you want to capture, do the following:

3.1 Click Add agent to open the Remote Application Capture Agent Editor (Figure 11-6).

3.2 Make sure that Capture Agent Type is set to WAN Accelerator.

3.3 Specify settings for the agent. (You might get prompted to specify a username and password before you can access the device.)

WARNING—You must configure the agent to ensure that the accelerator does not run out of disk space. Because tcpdump creates a separate copy of each captured packet, you must ensure that the capture process does not consume more disk space than is necessary on the accelerator. The Filter, Maximum size of packet data to capture (bytes), and Maximum number of packets to capture options are especially relevant for limiting packet trace sizes.

For descriptions of these and other settings, see Table 11-1.

3.4 Repeat step 3.1 and step 3.3 for every interface on which you want to capture.

Note—When capturing across a WAN-accelerated connection, you must capture both the LAN-side and the WAN-side traffic. If an accelerator uses separate interfaces for LAN and WAN traffic, specify a separate agent for each interface.

3.5 Optionally, save the complete agent list by clicking “Save Agent List”.

4 Verify that all agents are enabled (checked) in the Capture Manager treeview, then click “Start Capture”. If prompted, enter your login username and password for that device.

AppTransaction Xpert retains your username and password for the current session but does not save this information anywhere on the local host or the accelerator. Therefore, you must supply your username/password before the first capture in the current session of AppTransaction Xpert.

Note—For AppTransaction Xpert to determine the components of delay, the Transaction Analyzer model file must include all packets for the user-level transaction being analyzed. For this reason, it is good practice to start the capture process *immediately before* you start the transaction of interest, and then to stop the capture *immediately after* the transaction ends.

5 Run the application transaction that you want to capture.

6 When the transaction finishes, click “Stop Capture”.

➥ AppTransaction Xpert automatically downloads the packet traces from all accelerator interfaces. (You cannot store capture data on an accelerator.)

End of Procedure 11-1

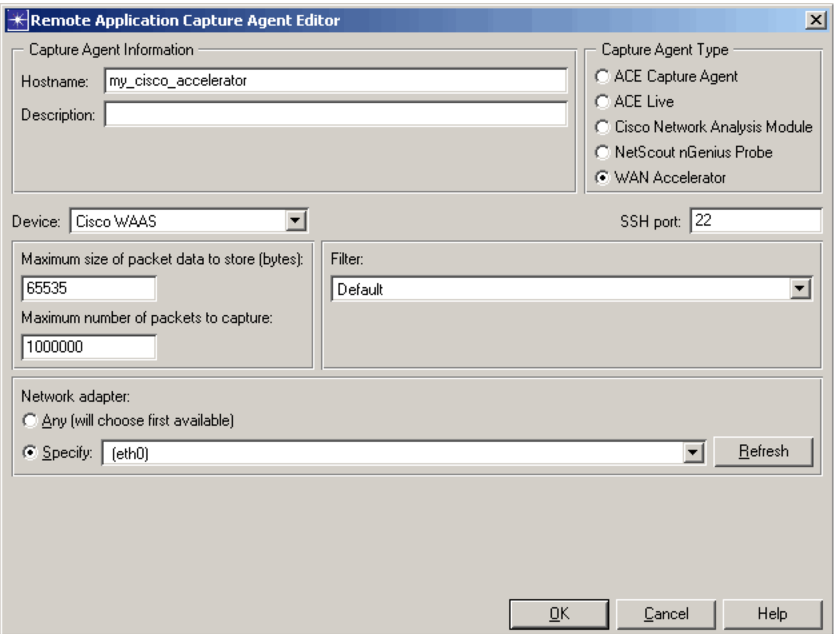
Configuring Capture Options on the Cisco/Riverbed Device

The Remote Application Capture Agent Editor has some options that are unique to WAN accelerators. These options are listed in Table 11-1.

WARNING—You must limit packet trace sizes or the accelerator might run out of disk space.

Because tcpdump creates a separate copy of each captured packet, you must take care not to consume more disk space than is necessary on the accelerator. The Filter, Maximum size of packet data to capture (bytes), and Maximum number of packets to capture options are especially relevant for limiting packet trace sizes.

Figure 11-6 WAN Accelerator Options in Remote Application Capture Agent Editor



Remote Application Capture Agent Editor

Capture Agent Information

Hostname: my_cisco_accelerator

Description:

Capture Agent Type

○ ACE Capture Agent
○ ACE Live
○ Cisco Network Analysis Module
○ NetScout nGenius Probe
● WAN Accelerator

Device: Cisco WAAS

SSH port: 22

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

Maximum number of packets to capture: 1000000

Filter: Default

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

The following table lists the configuration options available for WAN accelerators in the Remote Application Capture Agent Editor.

Table 11-1 WAN Accelerator Options in Remote Application Capture Agent Editor

Options	Description
Hostname	Hostname or IP address of the appliance.
Description	Description that appears in the Capture Manager treeview.
Capture Agent Type	Make sure that WAN Accelerator is selected.
Device	Accelerator type (Riverbed Steelhead or Cisco WAAS).
SSH port	The default SSH port is 22. Change this setting only if the accelerator uses a different port for SSH connections.

Table 11-1 WAN Accelerator Options in Remote Application Capture Agent Editor (Continued)

Options	Description
Maximum size of packet data to capture (bytes)	You might want to limit the amount of data in each packet. However, note the following: • Do not specify a value that is less than 130 bytes per packet. This is necessary to ensure that all protocol header data is captured. • If you limit the number of bytes captured per packet, and application payload data is not captured, you might be unable to perform detailed application-layer analyses when you import the traffic into AppTransaction Xpert.
Maximum number of packets to capture	You might want to specify a lower value than the default when capturing on a LAN-side interface, or on a WAN-side interface that uses transparent addressing.
Filter	How you filter traffic depends on whether you are specifying an agent on a WAN-side or a LAN-side interface. **LAN-side interfaces:** Capture only relevant traffic between the LAN-side tiers (on both sides of the WAN) by filtering out irrelevant hosts and ports. For more information, see Filtering Traffic. **WAN-side interfaces:** Your capture strategy depends on the addressing mode used by the accelerators. • *Accelerators exchange traffic using the same addresses as the LAN-side tiers:* Capture only relevant traffic between the two accelerators by filtering out irrelevant hosts and ports. • *Accelerators exchange traffic using their own distinct WAN-side addresses:* You must capture all traffic between the two accelerators. This is necessary because you cannot predict in advance the ports that the two accelerators will use to exchange the traffic of interest. For more information, see Accelerator Addressing Modes.
Network Adapter	Always select a specific adapter (do not select Any). Remember that you need to capture both WAN-side and LAN-side traffic. Therefore, if the accelerator has separate LAN and WAN interfaces, you must specify a separate capture for each interface.

Related Topics

- *Capturing Packets in Cisco WAAS Environments*
- *Capturing Packets in Riverbed Steelhead Environments*

Capturing on Other Accelerators

You can capture traffic on other types of accelerators. Remember that they must be able to generate compatible packet traces, and that you must have the necessary permissions to capture traffic on the accelerators.

The following steps outline the general workflow for capturing applications directly on the accelerators.

1) Verify that you have one or more user accounts that have permissions to capture traffic on the accelerators.

   If you cannot capture directly on the accelerator, use the indirect-capture method described in Indirect Captures (Near the Accelerators).

2) For each accelerator, determine the names of the interfaces on which you will capture the traffic. (*vendor-specific*)

   For more information, see Selecting the Interfaces on the Accelerator (Single- vs. Dual-Interface Captures).

3) Configure packet filters on both accelerators to filter out as much irrelevant traffic as possible. (*vendor-specific*)

4) Start the capture processes on both accelerators. (*vendor-specific*)

   Note—To determine the components of delay, the Transaction Analyzer model file must include all packets for the user-level transaction being analyzed. For this reason, it is good practice to start the capture process *immediately before* starting the transaction of interest, and then to stop the capture *immediately after* the transaction ends.

5) Run the application you want to capture.

6) Stop the capture process on both accelerators. (*vendor-specific*)

7) Transfer the files to a computer that has AppTransaction Xpert (14.5 PL2 or higher) installed. (*vendor-specific*)

8) Delete the original files on the accelerators. (*vendor-specific*)

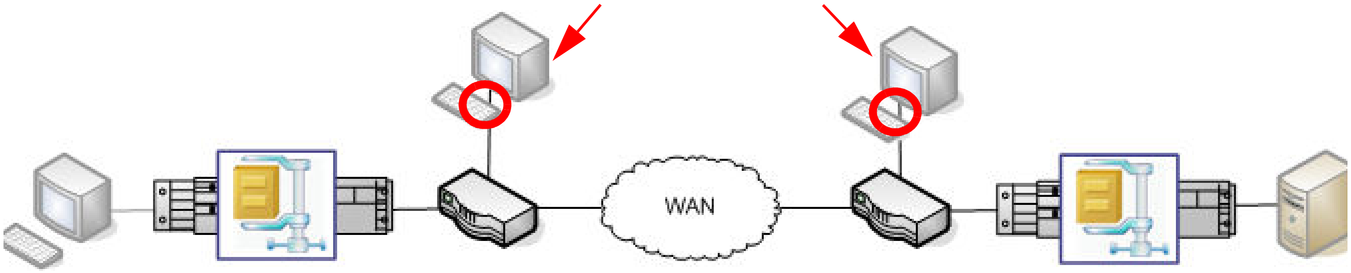
9) Import the packet traces into AppTransaction Xpert.

   For more information, see Creating a Transaction Analyzer Model.

Indirect Captures (Near the Accelerators)

Indirect captures are necessary if you cannot obtain permission to capture directly on the accelerators, as described in Direct Captures (On the Accelerators). To perform indirect captures, you need to install an AppTransaction Xpert capture agent or other type of agent/sniffer/analyzer on a nearby host, then connect that host to the mirror port of the device. (See the following figure.)

Figure 11-7 Indirect Capture (near the Accelerators)



If you use the indirect-capture approach, note the following:

- The initial set-up process can be longer than capturing directly on an accelerator. You might need to install a capture agent on a nearby host, and then to connect that host to the mirror port on the router/switch.
- The mirror port must be available on the router or switch.
- You might need additional equipment (cables, hubs) to provide connectivity between the capture agent and the acceleration device.

Capturing at LAN-Side Tiers

You must capture at the end tier within a LAN if both the following conditions are true:

- The application of interest includes traffic that does not go through the accelerator. (That is, the router sends this traffic directly into the LAN without going through the accelerator.)
- You want to study this traffic in AppTransaction Xpert.

Capturing near WAN Accelerators (Indirect Captures): Workflow Descriptions

The following steps outline the workflow for performing indirect captures.

1) For each accelerator, set up a capture process at a network location between the accelerator and the gateway to the WAN.

   If the LAN has a switch that can capture traffic, you can capture directly on that device (Figure 11-8).

Another option is to install from a nearby host using an AppTransaction Xpert capture agent. To do this, perform the following steps:

a) Install a capture agent on a host that is accessible to a switch between the accelerator and the WAN (as shown in Figure 11-9).

b) Connect this host to a mirror port on that switch.

2) Install AppTransaction Xpert capture agents on the end tiers. This step is required only if the capture processes you have set up cannot capture LAN-side traffic.

3) In Capture Manager, create an agent list that specifies the agents on all end tiers and on the hosts that are set up to capture on the switches.

4) Configure the traffic filter on each capture agent so that it captures only relevant traffic.

Note—Filtering irrelevant traffic is especially important for the intermediate hosts; otherwise the agents will capture all traffic (both relevant and irrelevant) that goes through the router/switch.

Figure 11-8 Capturing on the Switches

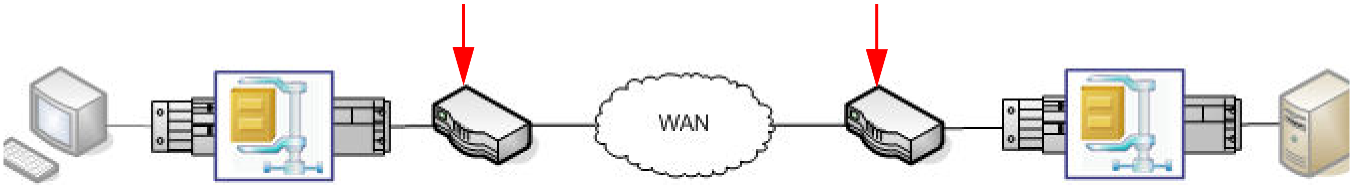
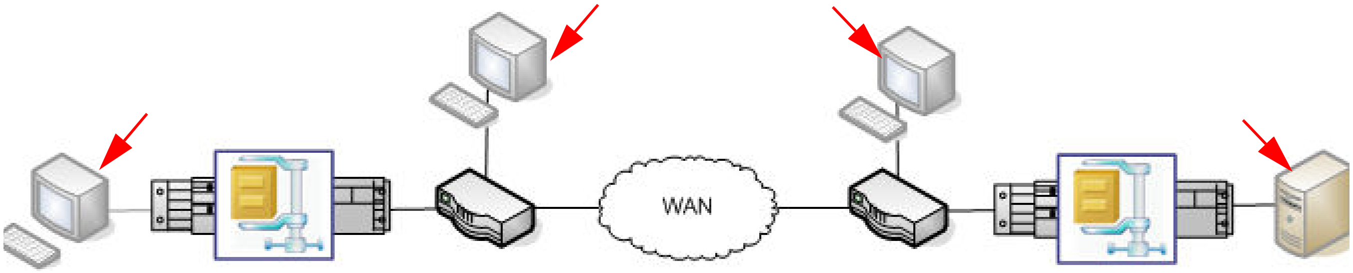


Figure 11-9 Capturing near the Switches and on the End Tiers



*Key Concept—*You always need to capture both *LAN and WAN traffic at the client side* and *LAN and WAN traffic at the server side*.

After you complete these steps, you can capture applications, and import the resulting packet traces, directly from Capture Manager. For more information, see Capturing Traffic with AppTransaction Xpert.