

4 Capturing Traffic with AppTransaction Xpert

Use AppTransaction Xpert's Capture Manager utility to capture traffic and import the data into AppTransaction Xpert. This utility uses capture processes (called *capture agents*) that enable you to capture traffic from multiple locations simultaneously. You can use Capture Manager to manage all capture agents and operations from one computer.

This section includes the following topics:

- Capturing Overview
- Prerequisites for Capturing
- Installing Capture Agents
- Troubleshooting Captures and Capture Agents
- Capture Encryption
- Capture Security: Restricting Access to Capture Operations
- Excluding Sensitive Information from Captures
- Capture Manager
- On-Demand Capture Tabbed Page
- AppResponse Xpert Tabbed Page
- Creating a Capture Agent/Appliance List
- Editing a Capture Agent
 - Configuring a Capture Agent
 - Configuring an AppResponse Xpert Capture
 - Editing a Cisco NAM Probe
- Running a Capture
- Managing Packet Traces
- Measuring Network Connections with PathProbe
- Collecting Performance Data from AppInternals Xpert
- Running Scheduled Captures and Downloads
- Downloading Packets from High Speed Captures on AppResponse Xpert Appliances

Related Topics

- *Capturing Application Traffic: Overview*
- *Continuous Captures*
- *On-Demand Agentless Captures (Experimental)*

Capturing Overview

AppTransaction Xpert supports the following types of capture operations:

- **On-Demand Capture**—If the problem can be reproduced, you can do an *on-demand capture* that consists of the following steps: start capture, run transaction, stop capture.

On-demand capture is the most common type of capture, and is described in detail in the following sections.

- **Scheduled Capture**—If a problem occurs intermittently, but you know that it occurs within a specific time window, you can perform a *scheduled capture* in which the capture agent runs according to a specified schedule (for example, daily from 2:00 to 2:05 am). You can also use this type of utility to schedule and run automatic downloads.

For more information, see [Running Scheduled Captures and Downloads](#).

- **Continuous Capture**—If the transaction or problem of interest occurs intermittently but you cannot predict when it will occur, you can do a *continuous capture* in which you start the capture and keep it running until the transaction occurs. Then you can stop the capture, extract the transaction of interest, and import it.

For more information, see [Continuous Captures](#).

Note—The ability to run scheduled and continuous captures requires a license for AppTransaction Xpert Plus or AppTransaction Xpert Advanced Capabilities.

Related Topics

- [Capturing Traffic with AppTransaction Xpert](#)

Prerequisites for Capturing

Before you can capture traffic with Capture Manager, AppTransaction Xpert's packet trace capture utility, you must do the following steps:

- 1) Install a capture agent on every computer where you want to capture traffic.

For more information, see *Installing Capture Agents*.

- 2) Create an agent list, which specifies the capture agents you want to use for a capture operation and the configuration settings for each capture agent.

For more information, see *Creating a Capture Agent/Appliance List*.

After performing these steps, you can run on-demand captures and continuous captures. If you have a Distributed Agent Controller (DAC) license, you can also capture traffic from a command prompt as described in *Distributed Agent Controller*.

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Installing Capture Agents

Before you can capture traffic, you must install capture agents on the computers where you want to capture traffic. A capture agent resides on a local or remote computer. It records packet traffic in response to commands from the Capture Manager utility.

To download capture agent installers and instructions, go to <https://support.riverbed.com>.

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Troubleshooting Captures and Capture Agents

To obtain the latest list of troubleshooting information about capture agents, go to <https://support.riverbed.com> and search the Knowledge Base. Search for a relevant string such as “capture agents,” “agent uninstall,” or a keyword based on your specific question.

The following table lists a partial list of capture-related FAQs. There are many more entries available in the Knowledge Base. In addition, some of these FAQs might have been updated since the publication of this help system.

Table 4-1 AppTransaction Xpert Capture-Related FAQ's (Partial List)

| Category | Question |
|------------------------|--|
| Troubleshooting | How do I troubleshoot the capture agent? [FAQ 907] |
| | What information can I provide to OPNET for troubleshooting the capture agents? Is there a way to turn on logging for the capture agents? [FAQ 1188] |
| | The Windows version of the capture agent appears to be losing packets when I capture traffic over a heavily-utilized high-speed link. Is there anything I can do to reduce the chance of this happening? [FAQ 2057] |
| Capture Agent Features | What resources does the capture agent use on a computer? [FAQ 1368] |
| | On what network types can capture agents capture traffic? [FAQ 949] |
| Installation and Setup | Why does the capture agent still use the default port even though a different port is specified during installation? [FAQ 809] |
| | How do I use a capture agent remotely through a firewall? [FAQ 696] |
| Managing Packet Traces | Where are the packets that are captured with capture agents stored during the capture period? That is, prior to stopping the capture and moving the packet trace to the computer running Capture Manager, where are the packets stored locally on the capturing device? [FAQ 1268] |
| | How can I convert a packet trace created by the capture agent (*.appcapture) into .enc format? [FAQ 1205] |

**How do I
troubleshoot the
capture agent?
[FAQ 907]**

This FAQ describes troubleshooting version 2.x of the capture agent, but this FAQ may still provide insights for other versions of the capture agent. Therefore, OPNET recommends that all clients use this FAQ as a starting point for troubleshooting capture agents.

This FAQ discusses the following problems:

- Problem #1. Capture Manager reports the "Capture service is not running" on a host, which has a capture agent installed.
- Problem #2. The Capture Agent is running, but Capture Manager reports the "Capture service is not running" on the host.
- Problem #3. The Capture Agent is reporting "0 packets accepted", but there is traffic on the network.
- Problem #4. When specifying the NIC to use for capture traffic, Capture Manager reports the error, "Unable to query agent interfaces for the following reason: Capture service is not running."
- Problem #5. When importing a packet trace from Capture Manager, the system reports that there are no packets to import. However, the manager reports capturing packets.

Problem #1. Capture Manager reports the "Capture service is not running" on a host, which has a capture agent installed.

Make sure that the capture agent is running on the specified host:

For Windows NT/2000/XP, check that the capture agent is "Started" using the "Services" applet under the Windows "Control Panel". (NOTE: For Windows XP, the "Services" applet is located in "Control Panel-->Administrative Tools".) If the capture agent is not started, select the "OPNET Application Capture Agent" in the "Services" applet window, and then click the "Start" button.

For Windows 95/98/ME, press Ctrl-Alt-Delete to display the task list. If the entry "op_capture_server.exe" does not appear in the task list, the capture agent is not running. To start the capture agent, open Windows Explorer, and navigate to the directory that contains the capture agent's executable files. Then double-click on "op_capture_server.exe", and press Ctrl-Alt-Delete to confirm the capture agent is running.

For UNIX, use the "ps" command to determine if the capture agent is running. The "ps" command varies depending on the UNIX platform, so consult your system's man pages for usage details. If the capture agent is not running, navigate to the directory that contains the capture agent's executable files. Then type "./op_capture_server" to start the capture agent. Verify the capture agent is running by using the "ps" command.

On Windows, if you previously had an older version of WinPcap (pre-3.0) and/or an older version of the capture agent (pre-2.2), it may be necessary to reboot the machine.

Problem #2. The Capture Agent is running, but Capture Manager reports the "Capture service is not running" on the host.

Make sure both Capture Manager and the capture agent are set to the same TCP port number. By default, both will use TCP port 27401. However, the capture agent's port is configurable during capture agent installation. If the port is no longer the default number, the manager will need to communicate with the capture agent using the new port number. To change the manager's port number for the capture agent, double-click on the capture agent's entry in the manager, and change the "Capture Service TCP Port:" to match the capture agent's port number.

Make sure a firewall is not blocking network traffic between Capture Manager and the capture agent. See FAQ 696 for more details about using the capture agent with a firewall.

Problem #3. The Capture Agent is reporting "0 packets accepted", but there is traffic on the network.

In the Capture Agent Editor:

- Make sure the agent's filter is set to "None".
- Make sure the agent's Promiscuous Mode check box is checked.
- Make sure the proper Agent Network Adapter has been specified. (If you are not sure which Adapter is the proper Adapter, then you can experiment by doing test captures on each Adapter until you find the proper Adapter.)
- Set "Maximum Size of Packet Data to Store" to default of 2000.
- Set "Agent Buffer Size" to default of 1024.
- Set "Maximum Number of Packets to Capture" to default of 100,000.

Note—Try the above recommendation first. If you still see "0 packets accepted", try disabling Promiscuous mode.

Additional details: the "Default" filter will only allow the capturing of packets that use either the TCP or the UDP protocols. To change the filter, stop the capture agent (if running) using Capture Manager. Double-click on the capture agent, and then select "None" in the "Filter" drop down menu.

Make sure the capture agent is capturing traffic from the correct NIC. To specify a NIC, first, use the manager to make sure the capture agent is not currently capturing. Then double-click on the capture agent's entry in Capture Manager, and click on the "Specify" radio button in the "Agent Network Adaptor" panel. Finally, from the "Specify" drop-down menu, select the NIC on which the capture agent will capture traffic. This method is the only way to specify which NIC the capture agent will use to capture traffic. Otherwise, the capture agent will choose the first available NIC (adaptor driver for Windows clients).

Setting the maximum packet size, agent buffer size, and maximum number of packets to large values can sometimes cause the agent to not capture any packets. For almost all captures, the default settings for max packet size and agent buffer size can (and should) be left at the default values. Increasing the maximum number of packets is generally safe, but if none of the above suggestions resolve the issue, try setting this back to the default as well.

Problem #4. When specifying the NIC to use for capture traffic, Capture Manager reports the error, "Unable to query agent interfaces for the following reason: Capture service is not running."

Make sure the capture agent is running and set to the expected TCP port number. Check the previous advice given in this FAQ.

Problem #5. When importing a packet trace from Capture Manager, the system reports that there are no packets to import. However, the manager reports capturing packets.

Make sure the import filter (not the capture agent filter) is set to "None". The "Default" filter will only allow the importation of packets that use either the TCP or the UDP protocols. The import filter is assigned in the Import window, which appears right after clicking the "Import Trace(s)" button in Capture Manager. Each row has a column called "Filter", which allows the user to modify the import filter.

***What information
can I provide to
OPNET for
troubleshooting the
capture agents? Is
there a way to turn
on logging for the
capture agents?
[FAQ 1188]***

- 1) What type of machine is the capture agent running on? Is it running on a multi-processor machine?
- 2) What is the machine hardware configuration (e.g., number of CPUs, brand/model/settings of NIC, hyperthreading, etc.)? You can obtain your NIC brand, model, and settings by right-clicking on "My Computer", selecting "Properties", selecting the "Hardware" tab, clicking on the "Device Manager" tab, and looking at the "Network Adapters" branch of the treeview. Right-click on an adapter and select "Properties" to obtain more information.
- 3) What is the exact OS (including service packs if appropriate)?
- 4) Does the machine have any special networking software installed (e.g., teaming, VPN, load balancing, etc.)?

- 5) Did you receive any error messages when installing the capture agent? If so, what were those error messages?
- 6) What is the exact error message that you receive when attempting to start a capture?
- 7) What is the exact error message (if any) that you receive when you attempt to select an ethernet adapter?
- 8) What version of the capture agent are you using? If you are not sure, provide us with the exact name of the installer executable.

If the above information is not sufficient to diagnose the issue, Technical Support might ask you to configure the capture agent to generate a diagnostic log.

The following procedures provide instructions for versions 2.x and 3.x of the capture agents. See Procedure 4-1 and Procedure 4-2 for the Windows and UNIX instructions, respectively.

Procedure 4-1 Generating a Capture Agent Log (Windows)

- 1 Start regedit.
- 2 Navigate to the key HKEY_LOCAL_MACHINE\Software\OPNET Technologies\AppCapture<version> (replace <version> with capture agent's version number).
- 3 Add two new "String Value[s]":
 - Name="AgentLog"; Data="2"
 - Name="ServerLog"; Data="2"
- 4 Close regedit.
- 5 Open the Windows "Control Panel".
- 6 Open the Windows "Services" applet.
- 7 Stop the "OPNET Application Capture Agent" service.
- 8 Start the "OPNET Application Capture Agent" service.
- 9 Close the Windows "Services" applet.
- 10 Close the Windows "Control Panel".
- 11 Reproduce the error you are observing.

This will create one or two logs on the capture agent's machine. The log names are `opnet_capture_agent_log` and `opnet_capture_server_log`. These logs are found in the same directory, which contains the capture agent's executable files (typically, `c:\program files\OPNET\AppCapture<version>`).

End of Procedure 4-1

The following procedure describes how to generate a log on UNIX.

Procedure 4-2 Generating a Capture Agent Log (UNIX)

- 1 Terminate the capture agent (if running) using the UNIX kill command.
- 2 Start the capture agent using the following command (replace `<port>` with the port number on which the capture agent will listen):

```
op_capture_server -tcp_port <port> -verbose_log
```

- 3 Reproduce the error you are observing.

This will create one or two log(s) on the capture agent's machine. The log names are `opnet_capture_agent_log` and `opnet_capture_server_log`. These logs are found in the same directory, which contains the capture agent's executable files.

End of Procedure 4-2

Capture Manager Logging

AppTransaction Xpert has an additional logging feature on the Capture Manager machine. To enable this log, you need to start the software from the OPNET Console as follows:

```
>> atx -ace_capture_manager_debug_enable TRUE
```

After the product launches, go to Capture Manager and add the problematic capture agent; then:

- 1) Click Update Status.
- 2) Click Start Capture.
- 3) After the error is reproduced, close Capture Manager.

This creates a "capture_manager_log" file in the `...\op_admin\tmp` folder.

**What resources
does the capture
agent use on a
computer?
[FAQ 1368]**

When not capturing, the capture agent is completely idle. The capture agent consumes negligible CPU cycles and minimal memory.

When capturing in typical situations, the agents have a very light foot print in terms of memory and CPU usage.

However, if the agents are used to record data for an extended period of time at a sustained data transfer rate approaching full high-speed LAN data rates, CPU usage can become more significant. This applies to both On-Demand and Continuous Capture. In this case, note that configuring the agent to capture only the first 90 bytes of each packet will improve performance.

Both On-Demand and Continuous Capture require a certain amount of free disk space to operate. The default value for both capture types is 25 MB, but may be changed by configuring file storage from the Remote Capture Agent Editor. If free disk space drops below the configured value, new captures cannot be started, and captures in-progress will terminate.

In addition to the minimum free disk space requirement, Continuous Capture stores data in a "rolling buffer" file which has a default maximum size of 100 MB. This value may be modified using the Remote Capture Agent Editor.

**On what network
types can capture
agents capture
traffic?
[FAQ 949]**

Capture agents only officially work with Ethernet (10BaseT, 100BaseT, and GigE). On Windows and AIX there is also support for token ring.

Note that for Gigabit Ethernet, the capture agents can capture data under typical workloads, but cannot handle sustained data transfers at high utilizations (because, for example, a disk drive cannot keep up with the amount of data that would be required to be written to disk by the capture agent). Note that reducing the "Maximum size of packet data" field in the capture agent will help in this situation (for example, reduce it from the default size of 2000 to 80).

The capture agents do not support PPP, PPTP, or other NDisWAN adapters.

For Wireless LANs (802.11b / WLAN) on Windows, the following notes apply:

- 1) You must upgrade to OPNET 9.1 or later and be using the latest version of the capture agents.
- 2) You must be using a Wireless Network Interface Card (NIC) that is running in Ethernet Emulation mode, which currently is how almost all WLAN network adapter drivers are implemented.
- 3) You should set the capture agent's promiscuous mode to DISABLED (note that this means that you will only see traffic that is actually destined for your card; most WLAN NICs do not currently even support a promiscuous mode that also allows for traffic to be sent from that NIC at the same time).

Why does the capture agent still use the default port even though a different port is specified during installation?
[FAQ 809]

The installer uses a deprecated entry name in the registry when installing the capture agent. To update the entry name, use the Windows registry editor to navigate to the key `HKEY_LOCAL_MACHINE\SOFTWARE\OPNET Technologies\AppCapture2.0`; then rename the entry "ServicePort" to "ServerPort".

For this to take effect, you must then use the "Services" panel to stop then start the "OPNET Application Capture Agent" service.

How do I use a capture agent remotely through a firewall?
[FAQ 696]

To use a remote capture agent through a firewall, there must be a TCP port open in the firewall for the duration of the capture—that is, from the time you click "Start Collection" to the time you click "Finish Collection". When the remote capture agent receives the signal to stop capturing, it creates a packet trace and forwards it to your local machine, at which point you can close the hole in your firewall. The TCP port that a capture agent uses is specified when installing the capture agent. By default, the port number is TCP port 27401. See FAQ 691 to restrict access to a capture agent.

Where are the packets that are captured with capture agents stored during the capture period? That is, prior to stopping the capture and moving the packet trace to the computer running Capture Manager, where are the packets stored locally on the capturing device?
[FAQ 1268]

By default, they are stored in the same folder where the capture agent is installed. The default location for this on Windows is:

`C:\Program Files\OPNET\AppCapture<version>`

You can also specify a location of your choice:

On UNIX:

When starting the capture server:

`op_capture_server -capture_temp_path <path>`

On Windows:

Modify the following registry key with the new path, and then restart the capture agent:

`HKEY_LOCAL_MACHINE\SOFTWARE\OPNET Technologies\AppCapture<version>\CapturePath`

How can I convert a packet trace created by the capture agent (*.appcapture) into .enc format?
[FAQ 1205]

The capture agent outputs a packet trace file (filename suffix *.appcapture) in the libpcap format (also known as the tcpdump format).

If you have the AppTransaction Xpert Decode Module, you can open the packet trace in Trace Explorer and perform a "Save-As .ENC File..." operation to save the file into a ENC format.

Here is a utility that can automatically convert the format:

- **Ethereal** (<http://www.ethereal.com/>) is an open source solution that can convert this trace file to an enc file.

***The Windows version of the capture agent appears to be losing packets when I capture traffic over a heavily-utilized high-speed link. Is there anything I can do to reduce the chance of this happening?
[FAQ 2057]***

Yes. Using Capture Manager, you can tune the Windows capture agent (version 3.5 and later) to use more kernel memory when performing a capture. This will decrease the likelihood of having the capture agent lose packets when capturing traffic over a heavily-utilized high-speed link.

To modify this setting, increase the value of the “Agent buffer size (Kbytes)” field when editing a capture agent entry in Capture Manager.

Note that increasing this value will cause the capture agent to use more non-paged kernel memory, which is a shared system-wide resource. The theoretical upper limit on Windows is 256MB, although the actual size available may be less. If you specify a value that is too high, you'll receive the error message “Capture failed: Setting kernel buffer failed.” when attempting to start the capture agent.

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Capture Encryption

AppTransaction Xpert supports SSL encryption of communications between Capture Managers and capture agents.

A Capture Manager and capture agent can transfer data using one of the following types of encryption:

- Anonymous (Level 1) encryption—Using this level, Capture Manager and the capture agent communicate over an encrypted connection but do not attempt any type of authentication. This type of encryption ensures that passive listeners cannot decipher data transferred between Capture Manager and the capture agent.
- Certificate (Level 2) encryption—This level provides both encryption and authentication, and requires that Capture Manager and the capture agent have SSL certificates that were validated by a trusted CA (Certificate Authority). Level 2 encryption has the following advantages over Level 1 encryption:
 - Because the capture agent immediately checks for a valid certificate on Capture Manager, Level 2 encryption protects against “man in the middle” attacks.
 - Because Capture Manager requires a password before it starts a capture operation, Level 2 encryption also prevents unauthorized users from running capture operations.

AppTransaction Xpert implements encryption using OpenSSL. The details of working with OpenSSL and creating certificates are outside the scope of this documentation. Fortunately, there are numerous reference books and websites with information about implementing encryption with OpenSSL; a good place to start is the OpenSSL website (<http://www.openssl.org>).

Note—SSL encryption is useful for securing data while it is being transmitted from the capture agent to Capture Manager. However, it does not secure sensitive data in the resulting packet traces. To prevent highly sensitive information from being captured, you must configure the capture agent to capture traffic using headers-only mode. For more information, see Capture Security: Restricting Access to Capture Operations.

Requirements for Encryption (Level 1 and Level 2)

To capture traffic using encryption, the following conditions must be true:

- The Capture Manager computer must be running AppTransaction Xpert version 11.0 or higher.
- The AppTransaction Xpert capture agent must be version 3.0 or higher.

Generating Random Data

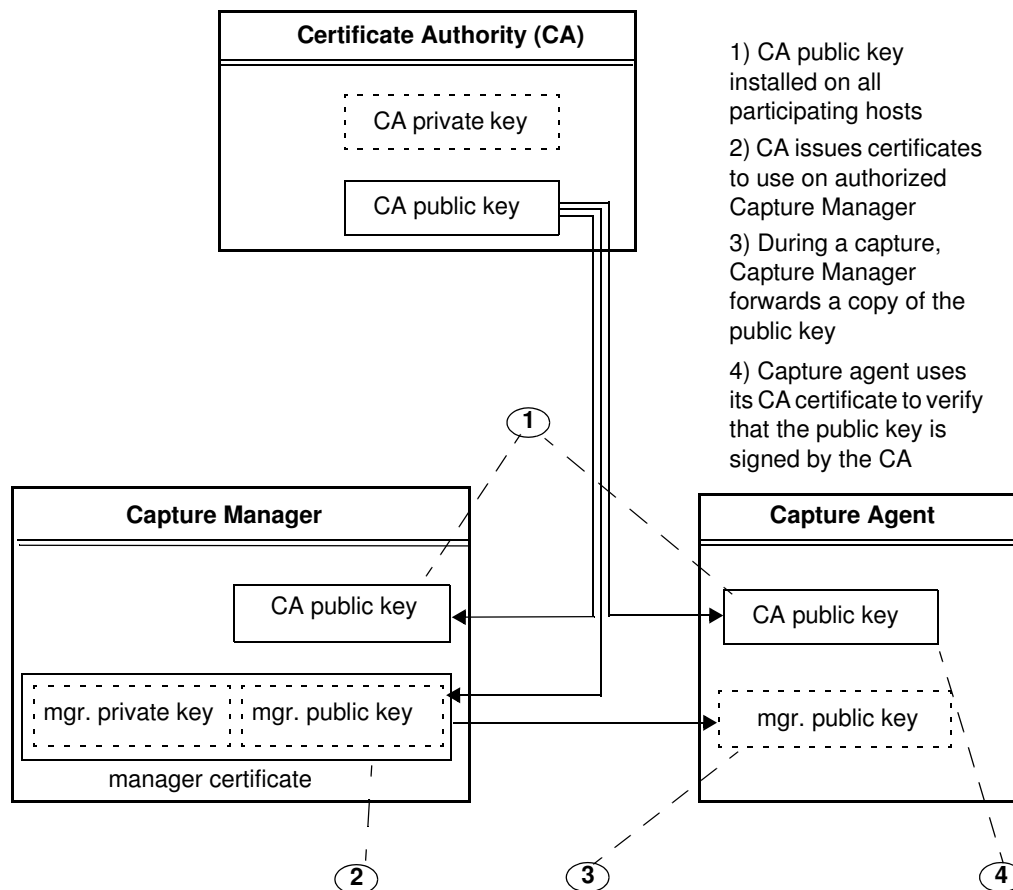
To generate cryptographically secure traffic, the OpenSSL library needs access to random numbers. AppTransaction Xpert and capture agents can generate random numbers using the standard methods for the operating system of the host computer. Alternately, you can create your own `rand` files (for Windows or UNIX) and `rand_cmd` files (UNIX only) and place them in the following directories:

- On the AppTransaction Xpert computer:
`<user_home>/op_admin/ace_import_configs`
- On the capture agent computer, place the file(s) in the same directory as the capture agent executables.

Requirements for Certificate Encryption (Level 2)

In addition to the requirements listed in the previous section, Certificate (Level 2) encryption also requires the following:

- Both Capture Manager and the capture agent computers must have the same CA public certificate; this certificate must be signed by a Certificate Authority (CA). The capture agent uses this certificate to ensure that the Capture Manager's certificate is signed by the same trusted CA. The capture agent certificate must be installed in the same directory as the capture agent executables.
- The Capture Manager computer—that is, the computer running AppTransaction Xpert—must have a certificate that was signed by a CA. This certificate includes both a private and a public key, and must be installed in the directory `<user_home>/op_admin/ace_import_configs`.
- To ensure the maximum level of security for Certificate encryption, set the `ace_application_capture_min_allowable_encrypt_level` preference to 2 on the Capture Manager computer. If this preference is set to 1, a Capture Manager or capture agent could drop to Anonymous (Level 1) encryption and establish a connection without a valid certificate.

Figure 4-1 Certificate (Level 2) Encryption in AppTransaction Xpert

For more information about SSL and AppTransaction Xpert, see Using SSL Encryption with AppTransaction Xpert.

Setting the Encryption Level

Every Capture Manager and capture agent has a range of allowable encryption levels:

- The *minimum* allowable level for a connection is specified by the setting of the AppTransaction Xpert preference `ace_application_capture_min_allowable_encrypt_level` on Capture Manager.
- The *maximum* allowable level for a connection is determined by the following:
 - On Capture Manager, level-2 encryption requires signed certificates and a valid username and password entered by the user. Otherwise the maximum allowable encryption is 1.
 - On the capture agent, level-2 encryption requires a signed certificate. Otherwise the maximum allowable level is 1.

A Capture Manager and a capture agent can establish a connection at either level 1 or level 2. If Capture Manager and a capture agent cannot agree on an encryption level, the connection is terminated and the capture operation fails for that Capture Manager-capture agent pair.

The following tables list how Capture Manager and capture agents determine the encryption level for a connection. Table 4-2 lists the outcome if certificate authentication succeeds; Table 4-3 lists the outcome if certificate authentication fails. A 'D' means that the connection is disconnected.

Table 4-2 Encryption Level (Certification Authentication Succeeds)

| | | Minimum/Maximum Encryption Levels (Capture Agent) | |
|---|-----|--|---|
| | | 1 | 2 |
| Minimum / Maximum Encryption Levels (Capture Manager) | 1/1 | 1 | D |
| | 1/2 | 1 | 2 |
| | 2/2 | D | 2 |

Table 4-3 Encryption Level (Certification Authentication Fails)

| | | Minimum/Maximum Encryption Levels (Capture Agent) | |
|---|-----|--|---|
| | | 1 | 2 |
| Minimum / Maximum Encryption Levels (Capture Manager) | 1/1 | 1 | D |
| | 1/2 | 1 | D |
| | 2/2 | D | D |

Viewing the Encryption Level

The Capture Manager's title bar shows the minimum and maximum encryption level specified for that manager. During a capture operation, the Capture Manager treeview shows the encryption level used for each connection.

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Capture Security: Restricting Access to Capture Operations

To restrict access to capture operations, you can create a capture authorization file and store it on a capture agent computer. This file lists specific computers and users; only the users listed, when logged onto the computers listed, can capture traffic on that host.

Note—If you do not create a capture authorization file, and are using Anonymous (Level 1) encryption, anyone with access to AppTransaction Xpert can use it to capture traffic.

Procedure 4-3 Creating a Capture Authorization File

- 1 In a text editor, create a file called `capture_auth`.
- 2 Type a list of hosts and users that have access to capture operations, in the form:

```
<ip_address_of_capturing_host> <user_name>
```

```
<ip_address_of_capturing_host> <user_name>
```

Note—The capture agent software does not perform DNS lookups. Therefore, this file must use IP addresses to specify computers that can capture traffic on that host. If Capture Manager and the capture agent are installed on the same host, use the address 127.0.0.1 (the “local-host” IP address) to authorize captures on that host. If you cannot capture using this address, replace it with the network IP address.

Use the plus sign (+) to match any user or any host, as shown in the following example.

```
+ sjones
127.16.10.150 +
127.0.0.1 root
127.16.2.134 pcook
```

This example shows that:

- sjones can capture when logged into any computer
- any user can capture when logged onto the computer with IP address 127.16.10.150
- any user logged onto the local computer as “root” can capture on that computer
- pcook can capture when logged into the computer with IP address 127.16.2.134

- 3 Copy the `capture_auth` file to the same directory on the capture agent computer where the application-capture software is installed.

End of Procedure 4-3

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Excluding Sensitive Information from Captures

In some cases, you might want to capture and study application traffic that contains sensitive or personal information. The capture agents support a special “headers-only” capture mode. When this mode is turned on, the capture agent captures only IP, TCP, and UDP header information; no other protocol or application data is captured.

To turn headers-only mode on or off, you must run the capture agent installer. The installer program asks if you want to turn on this capture mode.

To determine whether a capture agent is in headers-only mode, open Capture Manager and click “Update Status”. The Status field for the capture agent indicates whether the capture agent is in headers-only capture mode, as shown in the following figure.

Figure 4-2 Status Field of a Capture Agent in “Headers-Only” Mode

| Filter | Status |
|--------|---|
| None | Agent is idle [*HeadersOnly* Version 2.5 (Build 193), Windows |

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Capture Manager

Use Capture Manager to capture traffic and manage AppTransaction Xpert capture agents.

To open Capture Manager, perform one of the following:

- From the AppTransaction Xpert System window, choose File > Capture Manager...
- From the Transaction Analyzer window, choose Capture > Capture Manager

Depending on your available licenses, Capture Manager includes the following tabbed pages:

- **On-Demand Capture**
Manages on-demand captures.
For more information, see On-Demand Capture Tabbed Page.
- **Continuous Capture**
Manages continuous captures.
For more information, see Continuous Capture Tabbed Page.
- **AppResponse Xpert**
Manages captures on AppResponse Xpert appliances.
For more information, see AppResponse Xpert Tabbed Page.
- **PathProbe**
Measures network characteristics, such as bandwidth and latency.
For more information, see Measuring Network Connections with PathProbe

Related Topics

- *Packet Captures on AppResponse Xpert Appliances*
- *Packaging of Product Licenses and AppTransaction Xpert Licenses*

On-Demand Capture Tabbed Page

You can configure, run, and view on-demand captures using the On-Demand Capture page in Capture Manager.

Figure 4-3 Capture Manager: On-Demand Capture Page

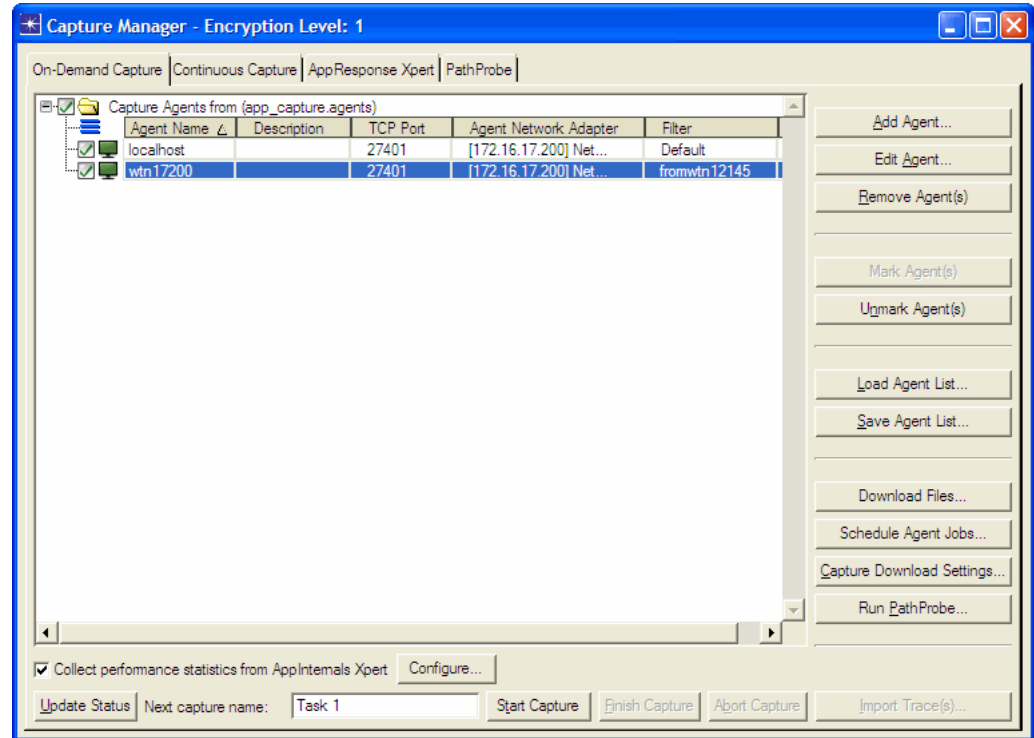


Table 4-4 Capture Manager: On-Demand Capture Page

| Item | Description |
|--|--|
| Abort Capture | Abort an on-demand capture that is currently running For more information, see Running a Capture. |
| Add Agent... | Add a capture agent to the list For more information, see Creating a Capture Agent/Appliance List. |
| Capture Download Settings... | Specify the directory, on the local computer, where packet trace files are stored. Additionally, you can specify the maximum size of downloaded packet trace files. Packet trace files that are larger than the specified size are broken into multiple files when downloaded. The default value is defined using the “Maximum trace file size in MB” preference. |
| Collect performance statistics from AppInternals Xpert | Capture performance data from AppInternals Xpert. For more information, see Collecting Performance Data from AppInternals Xpert. |

Table 4-4 Capture Manager: On-Demand Capture Page (Continued)

| Item | Description |
|--------------------|---|
| Download Files... | Download one or more packet traces from the selected capture agent. For more information, see Managing Packet Traces. |
| Edit Agent | Configure the capture agent selected in the Capture Agents treeview. For more information, see Configuring a Capture Agent. |
| Finish Capture | Finish the capture operation. This button appears only when a capture operation is in progress. For more information, see Running a Capture. |
| Import Trace(s) | Import the selected packet traces. For more information, see Creating a Transaction Analyzer Model. |
| Load Agent List... | Load a saved capture agent list from a file. The name of the capture agent list displays at the top. |
| Mark Agent(s) | Enable selected capture agents so that they capture during the next capture task |
| PathProbe tab | Select the PathProbe tabbed page <i>(Not available in all solutions)</i> For more information, see Measuring Network Connections with PathProbe. |
| Remove Agent(s) | Remove the selected capture agent(s) from the Capture Agents treeview |
| Run PathProbe... | Run a PathProbe experiment <i>(Not available in all solutions)</i> For more information, see Run PathProbe Dialog Box. |
| Save Agent List | Save the current capture agent list and configuration settings to an agent list (*.agents) file For more information, see Creating a Capture Agent/Appliance List. |

Table 4-4 Capture Manager: On-Demand Capture Page (Continued)

| Item | Description |
|------------------------|---|
| Start Capture | Start a capture operation. For more information, see <i>Running a Capture</i> . |
| Schedule Agent Jobs... | Schedule a capture. Capture jobs can be scheduled to run once, daily, weekly, or monthly. |
| Unmark Agent(s) | Disable the selected capture agents so they do not capture during the next capture task |
| Update Status | Shows information about each enabled capture agent: <ul style="list-style-type: none">• If the capture agent is idle—Shows agent build and OS of host computer• During a capture operation—Shows information about traffic captured by the agent (number of packets captured, number of packets filtered, etc.) For more information, see <i>Running a Capture</i> . |

Related Topics

- *Capture Manager*
- *Packet Captures on AppResponse Xpert Appliances*
- *On-Demand Agentless Captures (Experimental)*

AppResponse Xpert Tabbed Page

You can configure, run, and view AppResponse Xpert captures using the AppResponse Xpert page in Capture Manager.

Figure 4-4 Capture Manager: AppResponse Xpert Page

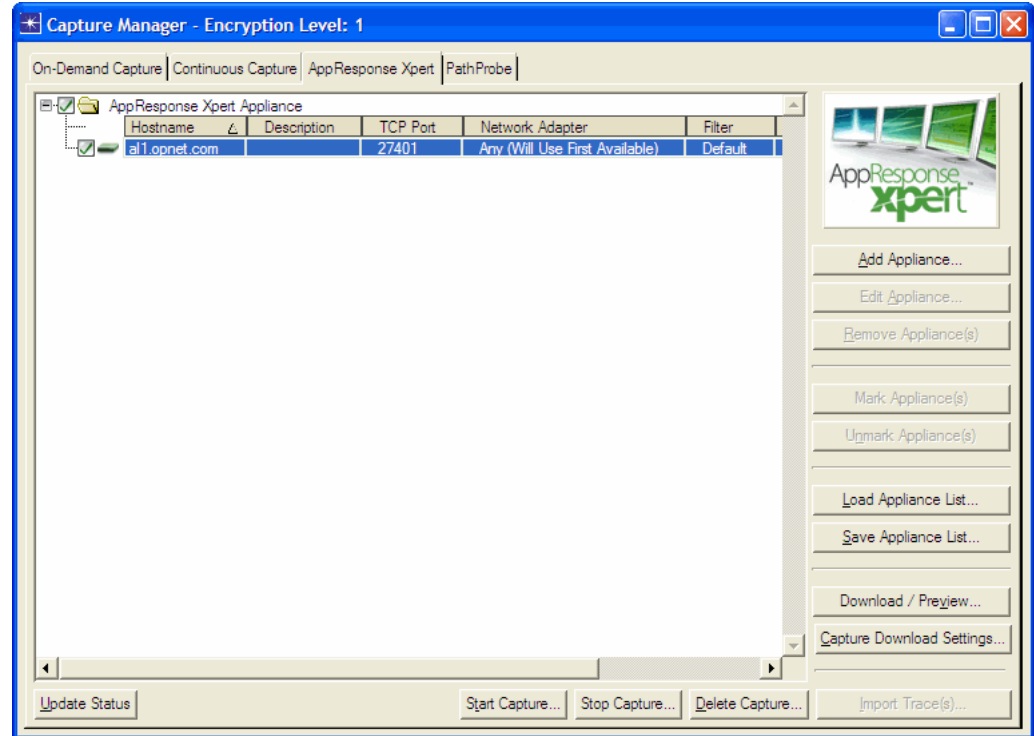


Table 4-5 Capture Manager: AppResponse Xpert Page

| Item | Description |
|------------------------------|--|
| Add Appliance... | Add an AppResponse Xpert appliance to the list of appliances. For more information, see <i>Creating a Capture Agent/Appliance List</i> . |
| Capture Download Settings... | Specify the directory, on the local computer, where packet trace files are stored. Additionally, you can specify the maximum size of downloaded packet trace files. Packet trace files that are larger than the specified size are broken into multiple files when downloaded. The default value is defined using the "Maximum trace file size in MB" preference. |
| Delete Capture... | Delete the selected appliance(s) from the AppResponse Xpert Appliance treewiew. |
| Download / Preview... | Download and previews the packet trace from the AppResponse Xpert appliance. For more information, see <i>Downloading Packets from High Speed Captures on AppResponse Xpert Appliances</i> . |

Table 4-5 Capture Manager: AppResponse Xpert Page (Continued)

| Item | Description |
|------------------------|--|
| Edit Appliance... | Configure the capture settings for the appliance selected in the Capture Agents treeview. For more information, see <i>Configuring an AppResponse Xpert Capture</i> . |
| Load Appliance List... | Load a saved appliance list from a file. The name of the appliance list displays at the top. |
| Mark Appliance(s) | Enable the selected appliances. |
| Remove Appliance(s) | Remove the selected appliance(s) from the AppResponse Xpert Appliance treeview. |
| Save Appliance List... | Save the current appliance list and configuration settings to an agent list (*.agents) file. For more information, see <i>Creating a Capture Agent/Appliance List</i> . |
| Start Capture... | Start a capture operation. For more information, see <i>Running a Capture</i> . |
| Stop Capture... | Stop an AppResponse Xpert capture. For more information, see <i>Running a Capture</i> . |
| Unmark Appliance(s) | Disable the selected appliances. |
| Update Status | Display status information about each enabled appliance. |

Packet Captures on AppResponse Xpert Appliances

Capture Manager includes the ability to capture on AppResponse Xpert appliances from the following tabbed pages:

- On-Demand tabbed page—For captures on 2000, 2100, 3000, 3100, and 3150 appliances.
- AppResponse Xpert tabbed page—For captures on 2000, 2100, 3000, 3100, 3150, 3170, 3200, 3700, 4100, 4200, and 5000 appliances.

AppTransaction Xpert does not support packet captures on AppResponse Xpert VMon, AppResponse Xpert on RSP, and AppResponse Xpert Rover.

Note—The information in this section was correct at the time of publication. For the latest information, see FAQ #2282 on the Support website.

Related Topics

- *Capture Manager*

Creating a Capture Agent/Appliance List

After capture agents are installed, the next step is to create a capture agent/appliance list. An agent/appliance list specifies the agents/appliances and settings to use during a capture.

Procedure 4-4 Creating a Capture Agent/Appliance List

- 1 Do one of the following:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager.

➔ The Capture Manager window appears. (See Figure 4-3.)
- 2 Select the tab that corresponds to the type of capture: On-Demand Capture, Continuous Capture, AppResponse Xpert.

For more information, see Capture Manager.
- 3 For each agent/appliance that you want to add to the list, do the following:
 - 3.1 Click Add Agent/Appliance.

➔ The Remote Capture Agent Editor window (shown in Figure 4-5) displays.
 - 3.2 In the Hostname field, specify the computer where the agent resides. Enter a computer name or an IP address.
 - 3.3 An agent can capture traffic on one network interface only. If the host computer has multiple network adapter cards, set the Agent Network Adapter radio buttons and specify an interface.
 - 3.4 If a host computer has multiple interfaces, you can create separate agents (one per interface) for that computer. This is essentially equivalent to creating agents on separate computers. When you create multiple agents for the same computer, you must specify the interface for each agent under “Agent network adapter”; do not use the default setting of Any.
 - 3.5 Verify the other default settings for your agent and change other settings as needed.
 - 3.6 Click OK to return to Capture Manager.

➔ A new agent entry appears in the Capture Agents treeview.
- 4 Optionally, to save the list for future use, after all agents are added click “Save Agent List...” and then specify a file name and directory.

➔ The agent list file is saved with a “.agents” extension.

End of Procedure 4-4

Related Topics

- *Installing Capture Agents*

Editing a Capture Agent

You can capture traffic using AppTransaction Xpert capture agents, AppResponse Xpert appliances, and Cisco Network Analysis Module (NAM) blades. The available options differ depending on the type of capture agent, and are described in the following sections:

- [Configuring a Capture Agent](#)
- [Configuring an AppResponse Xpert Capture](#)
- [Editing a Cisco NAM Probe](#)

Related Topics

- [Direct Captures on Cisco WAE Accelerators](#)
- [Direct Captures on Riverbed Accelerators](#)
- [Capturing Application Traffic with tcpdump](#)
- [On-Demand Agentless Captures \(Experimental\)](#)

Configuring a Capture Agent

Table 4-6 lists the options available in the Remote Capture Agent Editor (On-Demand Captures), which you can open from Capture Manager (On-Demand Page). Additionally, the table lists the options available in the Remote Capture Agent Editor (Continuous Captures), which you can open from Capture Manager (Continuous Capture Page).

Note—The Rolling Buffer Size (MB) setting is especially important when configuring a continuous capture. The setting specifies the maximum amount of data that can be stored in the buffer before the data is overwritten with new data.

Figure 4-5 Remote Capture Agent Editor (On-Demand Captures)

Remote Capture Agent Editor

Capture Agent Information

Hostname:

Description:

Capture Agent Type

☒ Capture Agent

☐ AppResponse Xpert

☐ Cisco Network Analysis Module

☐ WAN Accelerator

☐ F5 BIG-IP

☐ UNIX (no installed agent)

Capture Agent TCP port:

☒ Promiscuous mode

Maximum size of packet data to store (bytes):

Kernel buffer size (KB), Windows-only:

Maximum number of packets to capture:

Filter:

☐ Leave file on remote host

Download data rate (Kbits/sec):

Agent network adapter:

☒ Any (will choose first available)

☐ Specify:

☐ Include Server Data

Figure 4-6 Remote Capture Agent Editor (Continuous Captures)
Table 4-6 Remote Capture Agent Editor

| Item | Description |
|---------------------------|--|
| Agent Network Adapter | <p>Specifies the network interface for capturing traffic. An agent can capture on one network interface only.</p> <p>If a host computer has multiple interfaces, you can create separate agents (one per interface) for that computer. This is essentially equivalent to creating agents on separate computers. When you create multiple agents for the same computer, you must specify the interface for each agent under “Agent network adapter”—do not use the default setting of Any.</p> <p>For more information, see <i>Creating a Capture Agent/Appliance List</i>.</p> |
| Capture Agent TCP Port | Specifies the port that the op_capture_server service or daemon uses to communicate with the capture agent. The default value is 27401. (You can specify a different TCP port when installing the capture agent.) |
| Capture Agent Type | <p>Specifies the capture agent.</p> <p>Select “Capture Agent”.</p> |
| Configure File Storage... | <p>Configures the file-storage options on the remote agent.</p> <p>For more information, see <i>Managing Packet Traces</i>.</p> |
| Description | Specifies a brief description for identifying the capture agent. This description is for informational purposes only. |

Table 4-6 Remote Capture Agent Editor (Continued)

| Item | Description |
|--|--|
| Download Data Rate (Kbits/sec) | Specifies the maximum data rate to use when downloading packet traces from a remote agent. Use this option to reduce the risk of overloading the network when downloading many files and/or very large files. For more information, see Procedure 4-8 Downloading Packet Traces from a Remote Agent on page ATX-4-44. |
| Filter pull-down menu | Specifies/defines a filter to capture specific packets. For more information, see Packet Filters. |
| Hostname | Specifies the host computer running the agent. Enter either the computer name (DNS name) or the IP address. |
| Include Server Data | Specifies to capture Windows performance data. This option allows you to capture Windows performance data and application traffic data simultaneously. (<i>Windows only</i>) For more information, see Creating Windows Performance Data Files with Application Capture Agents. |
| Kernel Buffer Size (KB), Windows-only | Specifies the kernel buffer size, in kilobytes. (<i>Windows only</i>) |
| Leave File on Remote Host | If selected, specifies that the agent should store the generated packet traces on the agent computer. For more information, see Procedure 4-7. If not selected, specifies that the agent should transfer the packet traces to the computer that started the capture operation. |
| Maximum Number of Packets to Capture | Specifies the default setting. The default is 100,000. (<i>On-Demand captures only</i>) Enter "-1" to specify an unlimited number of packets. |
| Maximum Size of Packet Data To Store (Bytes) | Specifies the maximum number of bytes from each packet to include in a packet trace. You might want to fine-tune this setting to capture packet headers (such as IP and TCP information) only, and to minimize the amount of application data captured. |
| Promiscuous Mode | If enabled, specifies that the agent captures all packets that traverse its LAN segment. |
| Rolling Buffer Size (MB) | Specifies the maximum amount of disk space that can be used for a rolling buffer. If a continuous capture reaches this threshold, the oldest capture data in the buffer is discarded to make space for new data. (<i>Continuous captures only</i>) |

Related Topics

- *Editing a Capture Agent*

Configuring an AppResponse Xpert Capture

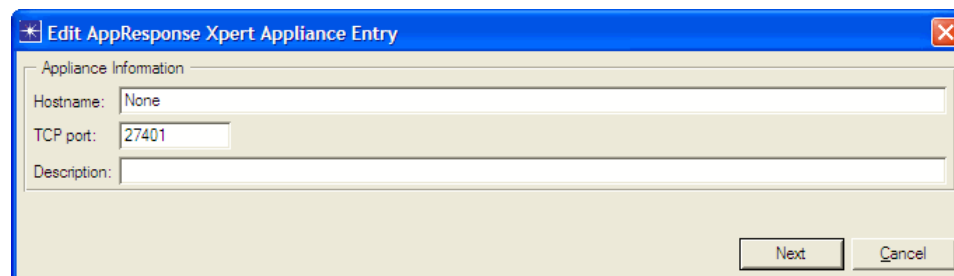
AppResponse Xpert captures can be performed from the On-Demand tabbed page and the AppResponse Xpert tabbed page. Use the On-Demand tabbed page to define on-demand captures on specific AppResponse Xpert appliances. Use the AppResponse Xpert tabbed page to define captures on all AppResponse Xpert appliances.

The workflow for configuring/performing captures on AppResponse Xpert appliances is similar to the workflow on hosts that have AppTransaction Xpert capture agents.

Note—There is no need to install a capture agent on the appliance. AppResponse Xpert console software includes capture functionality that supports both on-demand (on specific appliances) and continuous captures.

When defining a capture from the AppResponse Xpert tabbed page (shown in the following figure), you must specify the hostname and the login/password. The type of AppResponse Xpert appliance and its abilities are determined automatically.

Figure 4-7 Configuring Continuous Captures on an AppResponse Xpert Appliance (AppResponse Xpert Tabbed Page)



The screenshot shows a Windows-style dialog box titled "Edit AppResponse Xpert Appliance Entry". Inside the dialog, there is a section labeled "Appliance Information". This section contains three text input fields: "Hostname" with the value "None", "TCP port" with the value "27401", and "Description" which is currently empty. At the bottom right of the dialog, there are two buttons: "Next" and "Cancel".

When defining an on-demand capture from the On-Demand tabbed page (shown in the following figure), you must specify the capture settings, as listed in the following table.

Figure 4-8 Configuring On-Demand Captures on an AppResponse Xpert Appliance (On-Demand Tabbed Page)

The following table lists the configuration options for captures on an AppResponse Xpert appliance.

Table 4-7 Capture Settings for AppResponse Xpert Appliances

| Item | Description |
|--|--|
| Download data rate (Kbits/sec) | Specifies the maximum data rate to use when downloading packet traces from the appliance. (For on-demand captures only.) For more information, see Procedure 4-8. |
| Filter | Specifies a packet trace filter so the appliance captures only certain packets. (For on-demand captures only.) For more information, see Packet Filters. |
| Hostname | Hostname of the AppResponse Xpert appliance. You can specify either the computer name or the IP address. |
| Maximum Number of Packets to Capture | The default setting is 100,000. Enter -1 to specify an unlimited number of packets. (For on-demand captures only.) |
| Maximum Size of Packet Data To Store (Bytes) | Specifies the maximum number of bytes from each packet to include in a packet trace. You might want to fine-tune this setting to capture packet headers (such as IP and TCP information) only, and to minimize the amount of application data captured. (For on-demand captures only.) |

Table 4-7 Capture Settings for AppResponse Xpert Appliances

| Item | Description |
|----------|--|
| TCP Port | Specifies the port that the op_capture_server service or daemon uses to communicate with the appliance. The default value for this is 27401. |

Related Topics

- *Editing a Capture Agent*

Editing a Cisco NAM Probe

The following recommended procedure describes how to create and edit a Cisco NAM (Network Analysis Module) probe.

Procedure 4-5 Editing a Cisco NAM Probe

- 1 Open the Remote Capture Agent Editor (Figure 4-9) from the Capture Manager: On-Demand Capture Page:
 - To edit a new NAM probe, click Add Agent.
 - To edit an existing NAM probe, double-click on the probe or select it in the treeview and click Edit Agent.
- 2 In the Hostname field, enter the hostname or IP address of the NAM host.
- 3 Select the “Cisco Network Analysis Module” radio button.
 - ➔AppTransaction Xpert attempts to contact the NAM probe. An error message appears if the hostname is incorrect or not specified.
- 4 Set the “Maximum capture size (Kbytes)” field to 16,000 or less.

Note—The NAM probe has limited buffer space. If all buffer space is in use when you start a capture operation, the capture on that probe will fail. If this happens, the NAM administrator will need to free up buffer space on the probe.
- 5 Click the Refresh button.
- 6 In the “NAM probe network interface” menu, select the interface that you want to use to capture data.
- 7 Set the other options as needed. (For option descriptions, see Table 4-8.)
- 8 Click OK to close this window and return to the Capture Manager: On-Demand Capture Page.

After configuring the probe, you can capture traffic as described in Running a Capture.

End of Procedure 4-5

Table 4-8 lists the options available in the Cisco NAM Probe Editor dialog box.

Figure 4-9 Cisco NAM Probe Editor

Table 4-8 Cisco NAM Probe Editor Options

| Item | Description |
|-----------------------------|---|
| Hostname | Specifies the host computer running the Cisco NAM. Enter a DNS name or the IP address. |
| Read/Write Community | Specifies the read/write community to use with the NAM. You must specify a write-capable community. |
| Timeout | <p>Specifies the amount of time that Capture Manager waits to receive a response from the NAM. If the request times out, Capture Manager re-sends the request a number of times; if it still gets no response, a time-out message appears in the Capture Manager window.</p> <p>Note—Change the default setting only if you are experiencing problems with capturing:</p> <ul style="list-style-type: none"> - If you cannot capture, a possible cause is that the Timeout setting is too low. - If capture and download operations are starting too slowly, a possible cause is that the Timeout setting is too high. |
| Filter | Specifies the packet filter to use with the NAM. |
| NAM probe network interface | <p>Specifies the NAM interface to use when capturing traffic.</p> <p>Click Refresh to ensure that the pull-down list shows the interfaces that are currently available on the NAM.</p> |

Related Topics

- *Editing a Capture Agent*

Packet Filters

A packet filter ensures that the agent captures only packets that meet certain criteria. The Remote Capture Agent Editor (On-Demand Captures) and Cisco NAM Probe Editor include a Filter pull-down menu that defines a packet filter for the agent/probe. (Capturing on Cisco NAM probes is not available in all solutions.)

Packets can be filtered based on hosts, ports, and protocols. You can edit a filter in one of two ways:

- To edit a filter in the user interface, select the filter in the Filter pull-down menu; then select Edit... in the menu. This opens the filter in the Capture File Filter dialog box. You can use these filters both when capturing traffic (“capture only packets of type...”) and when importing capture data (“import only packets of type...”). For more information, see Packet Trace Filters.
- To edit a filter using the Berkeley Packet Filter (BPF) notation, select the filter in the Filter pull-down menu; then click Manually Edit Filter. This opens the filter in the Manually Edit the Filter Specification dialog box. You can use manually edited filters when you capture traffic, but not when you import packet traces into AppTransaction Xpert.

Packet filter files are saved in the default models directory with the “.ace.f” extension. For more information, see Packet Filtering.

Related Topics

- *Editing a Capture Agent*

Running a Capture

The following procedure describes how to capture traffic using Capture Manager.

Procedure 4-6 Capturing Traffic with Capture Manager

- 1 Open Capture Manager:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager
- 2 If necessary, click the “Load Agent List...” button to select the agent list that you want to use.

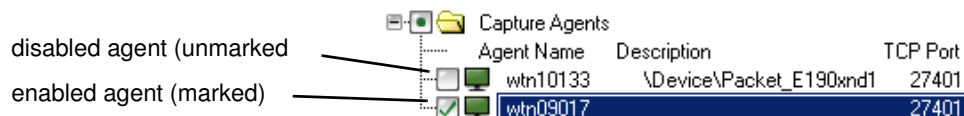
For more information, see Creating a Capture Agent/Appliance List.

- 3 Enable the agents that you want to capture data.

To enable an agent, do one of the following:

 - Select the agent in the Capture Agents tree, then click the Mark Agent(s) button.
 - Right-click on an agent and choose “Mark Agent”.
 - Select the agent’s checkbox.

Figure 4-10 Enabling and Disabling Capture Agents in Capture Manager



- 4 Click Capture Save Directory... and specify the directory where you want to store the packet traces.
- 5 Click Start Capture to start the capture operation.

➡ Each enabled agent begins to capture data.

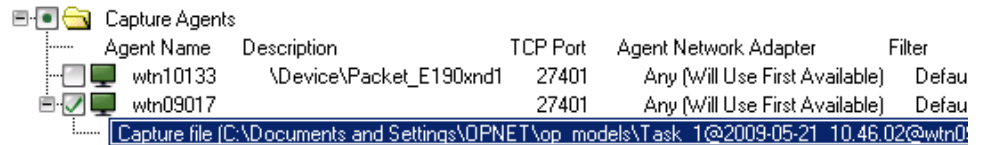
Note—To determine the components of delay, the Transaction Analyzer model must include all packets for the user-level transaction being analyzed. For this reason, it is good practice to start the capture process *immediately before* you start the transaction of interest, and then to stop the capture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

- 6 Optionally, note the following:
 - To abort the capture, click Abort Capture.
 - To view the statistics about the capture, click the Update Status button. Current status appears in both the Status field and the tooltip for each agent.

7 When the transaction ends, click “Finish Capture”.

- The message “Capture completed” appears in the Status field next to each enabled agent. Information about the packet trace appears in a line beneath each enabled agent.

Figure 4-11 Packet Trace Location



| Agent Name | Description | TCP Port | Agent Network Adapter | Filter |
|------------|-------------------------|----------|--------------------------------|--------|
| wtn10133 | \Device\Packet_E190xnd1 | 27401 | Any (Will Use First Available) | Defau |
| wtn09017 | | 27401 | Any (Will Use First Available) | Defau |

Capture file (C:\Documents and Settings\DPNET\op_models\Task_1@2009-05-21_10.46.02@wtn0

8 Open the packet trace.

To open the packet trace directly from the Capture Manager window, select the file in the agent tree and click the “Import Trace(s)...” button.

End of Procedure 4-6

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Managing Packet Traces

This section describes how packet traces are organized. The specific capture method and configuration of remote agents determine the location where a packet trace is saved, as listed in the following table.

Table 4-9 Packet Trace Storage Locations

| Capture Method | Download File Immediately? ¹ | Host | Directory |
|------------------------------|---|-------|---|
| Capture Manager | yes | local | <capture_save_dir>/ |
| Capture Manager | no ² | agent | <capture_agent_dir>/ capture_files/ <task_name>/ <console_location> ³ |
| Distributed Agent Controller | yes | local | <DAC_save_dir>/ capture_files/ <task_name>/ <console_location> |
| Distributed Agent Controller | no ⁴ | agent | <DAC_save_dir>/ capture_files/ <task_name>/ <console_location> |

1. Whether a remote agent stores its packet traces locally, or downloads them after the capture, depends on the configuration of each individual agent. For more information, see Procedure 4-7 Configuring Packet Trace Settings for an Agent on page ATX-4-43.

2. If you leave a packet trace on a remote agent, then download it using Capture Manager, AppTransaction Xpert stores the file in the following directory on the AppTransaction Xpert computer: <capture_save_dir>/capture_files/<task_name>/<capture_launch_host>

3. <console_location> refers to the host that initiated the capture operation. Thus, if a file resides in subdirectory <task_name>/<console_location>, this means that the files were captured as part of <task_name> and that <console_location> initiated the capture operation.

4. If you leave a packet trace on a remote agent, and then download it using the Distributed Agent Controller, AppTransaction Xpert stores the file in the following directory on the Distributed Agent Controller computer: <DAC_save_dir>/capture_files/<task_name>/<console_location>

Packet Trace Storage Settings

By default, a remote agent is configured to download packet traces to the local computer immediately after a capture finishes. However, you might prefer to leave the packet traces on the remote computer and download the files at a later time.

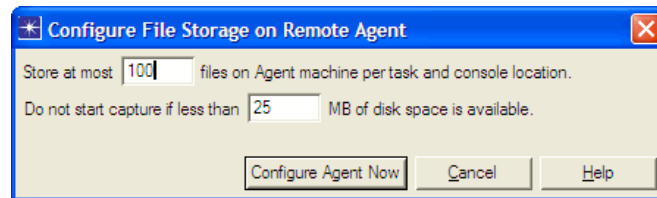
Note—This option is not available with capture agent versions 2.3 and earlier. To update the capture agent, visit the Support Center.

To use this option, you must do the following:

- Configure the agent to store the packet traces locally (see Procedure 4-7)
- When you want to import a packet trace, download the file from the remote agent (see Procedure 4-8)

Procedure 4-7 Configuring Packet Trace Settings for an Agent

- 1 Open Capture Manager:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager.
 - ➔ The Capture Manager window appears. This window includes an On-Demand Capture tab. If you have a license for AppTransaction Xpert Advanced Capabilities, this window includes a Continuous Capture tab.
- 2 Select the On-Demand Capture or the Continuous Capture tab, depending on the type of capture that you want to configure.
- 3 In the Capture Agents treeview of Capture Manager, right-click on the agent and choose Edit Agent.
 - ➔ The “Remote Capture Agent Editor” dialog box appears.
- 4 Select the “Leave file on remote host” checkbox.
- 5 Click the “Configure File Storage...” button.
 - ➔ The “Configure File Storage on Remote Agent” dialog box appears.



- 6 Set the following options:
 - Store at most *n* files on Agent machine per task and console location—When you start a capture called *<capture_task_name>*, the remote agent checks the number of packet traces in its *<capture_file_dir>/<capture_task_name>/<console_location>* directory. If the current number of packet traces is equal to or greater than this threshold, the agent deletes the oldest files to ensure that it can save the new packet trace without exceeding this threshold.
 - Minimum disk space (MB)—The minimum amount of free disk space required on the remote agent for the capture task to proceed. If this amount of free space is not available, the agent does not capture any traffic during the capture operation.
- 7 Click “Configure Agent Now” to close the “Configure File Storage on Remote Agent” dialog box.
- 8 Click OK to close the “Remote Capture Agent Editor” dialog box.

End of Procedure 4-7

Procedure 4-8 Downloading Packet Traces from a Remote Agent

- 1 Open Capture Manager:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager
- 2 Optionally, to reduce the risk of overloading the network, you can specify a maximum data rate for the file download. This is useful if you are downloading many files or the files are very large.

To specify a maximum data rate:

 - 2.1 In the Capture Agents tree, right-click on the remote agent where the files are installed and choose Edit Agent.
 - ➡ The Remote Capture Agent Editor (On-Demand Captures) appears.
 - 2.2 Set the Download Data Rate (Kbits/sec) option.

The default is "Maximum Available".
 - 2.3 Click OK to return to the Capture Manager window.
- 3 In the Capture Agents treeview, right-click on the remote agent and choose "Download Files". Alternately, select the agent and click the "Download Files..." button.
 - ➡ The Manage Remote Files dialog box appears.
- 4 Expand the treeview (if necessary) and select the files to download.
- 5 Optionally, to delete the files on the remote agent after downloading, select the "Delete selected files after download" checkbox. To delete the files on the remote agent without downloading them, click the Delete button.
- 6 Click Download.
 - ➡ The selected files are downloaded to the download directory.
- 7 Click Cancel to close the Manage Remote Files dialog box.
 - ➡ Note that the downloaded files are listed under the remote agent on the Capture Manager dialog box. To quickly open the packet trace(s) in AppTransaction Xpert, select the packet trace(s), right-click on a selected packet trace, and choose an open/merge option.

End of Procedure 4-8

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Measuring Network Connections with PathProbe

Use PathProbe to obtain approximate measurements of your network's connections, such as bandwidth and latency. Then view the PathProbe results within AppTransaction Xpert.

Use PathProbe to:

- Determine the correct bandwidth and latency values to enter for packet traces. This is especially useful when you create a transaction analyzer model from one packet trace instead of multiple packet traces.
- Diagnose and evaluate the network, especially when AppDoctor reports that a bottleneck is due to the network and not the application. For example, AppDoctor might blame congestion or transmission delay on a specific network path. In this case, use PathProbe to examine the actual conditions on that path.
- Characterize the network when performing predictive analyses with QuickPredict.

Procedure Description

Procedure 4-9 Creating a PathProbe Run

- 1 Open PathProbe from one of the following locations:
 - Capture Manager (PathProbe tabbed page)—Click Run
 - Capture Manager (Capture Manager tabbed page)—Click Run PathProbe
 - Capture Manager (Capture Manager tabbed page)—Right-click on the agent you want to use as the Source Agent; then choose Run PathProbe.

➡ The Run PathProbe dialog box appears.
- 2 To specify the type of data to collect, choose Configure.

For more information, see Configure PathProbe Run Dialog Box.
- 3 In the Run PathProbe dialog box, specify the source agent, network destination, and run name. You should express the network destination by its IP address or by a DNS-resolvable name, such as "www.<domain_name>.com." For more information, Run PathProbe Dialog Box.
- 4 Click Start to start the PathProbe run.

➡ The capture agent uses ICMP to measure bandwidth, latency, and other characteristics along the specified path. When PathProbe completes, the message "PathProbe Experiment Completed" appears at the bottom of the Run PathProbe dialog box.
- 5 Click View Results to examine the results.

For more information, see PathProbe Results.

End of Procedure 4-9

PathProbe Tabbed Page (Capture Manager)

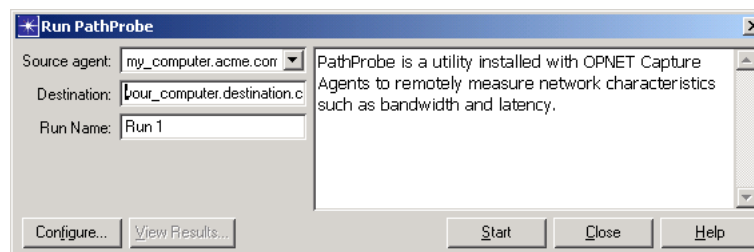
The PathProbe tabbed page in Capture Manager supports the following operations:

- Create a PathProbe run. (See Run PathProbe Dialog Box.)
- View the results for a previous PathProbe run. (See PathProbe Results.)

Run PathProbe Dialog Box

In the Run PathProbe dialog box you can start a new run, view results for a completed run, and specify the network path to study (Source Agent/Destination) and the type of experiments to run (Configure).

Figure 4-12 Run PathProbe Dialog Box



Configure PathProbe Run Dialog Box

The Configure PathProbe Run dialog box includes fields to specify the results that PathProbe generates.

Figure 4-13 Configure PathProbe Dialog Box

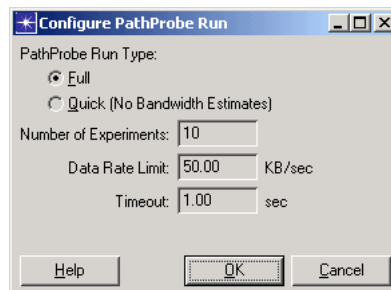


Table 4-10 Configure PathProbe Run Dialog Box

| Item | Description |
|-----------------------|---|
| PathProbe Run Type | If set to Quick, PathProbe does not measure bandwidth. |
| Number of Experiments | This value affects the number of packets that PathProbe generates during a run (a higher value results in more packets). This value is most relevant when PathProbe measures bandwidth. A higher value can produce better estimates of per-hop bandwidth, but also results in longer runs. |
| Data Rate Limit | <p>To measure the network, PathProbe needs to generate traffic in the form of ICMP packets. This field should equal the maximum rate at which the source agent can introduce packets onto the network.</p> <p>PathProbe measurements do not depend on the amount of outstanding PathProbe traffic in the network (network flooding). A lower data-rate limit affects the experiment completion time, but does not affect the accuracy of PathProbe results.</p> |
| Timeout | The response time window for a sent packet. You might need to increase this value when you measure a high-latency path that results in longer response times (for example, a path over a dial-up modem). |

PathProbe Results

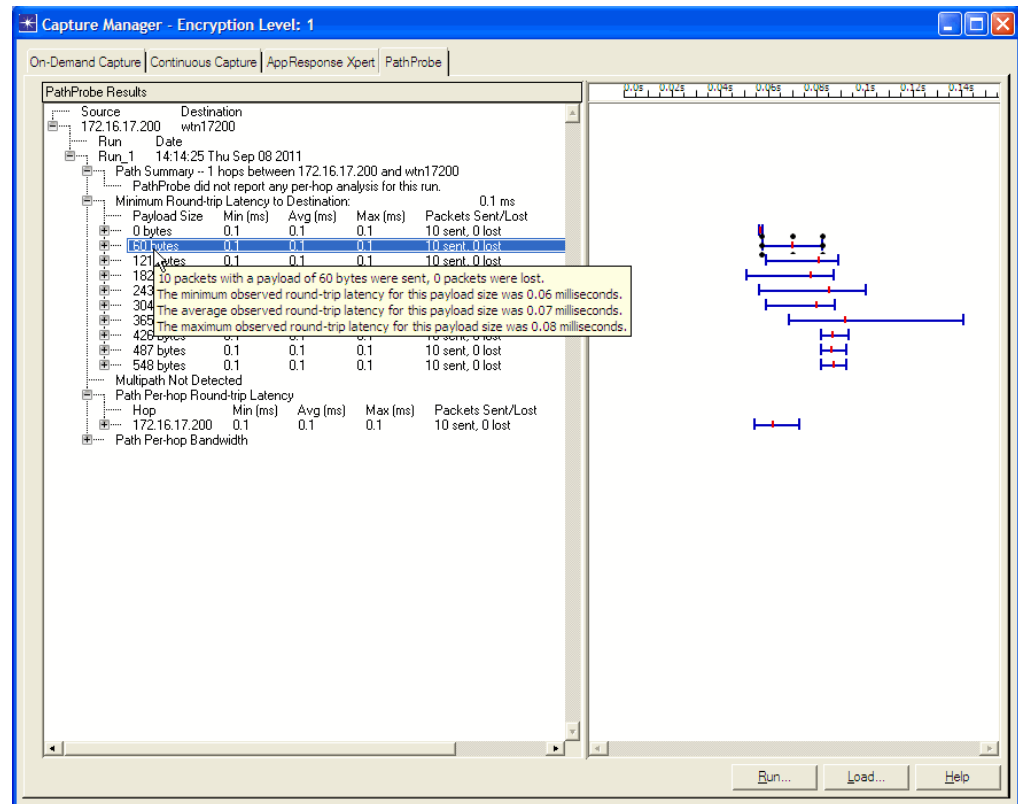
When a PathProbe run completes, the results are stored in the Capture Download directory. (The Capture Download directory is specified on the Capture Manager: On-Demand Capture Page.) The file name uses the following format:

```
<run_name>@<capture_agent>@<date>_<time>.pp
```

To view the results, open Capture Manager, click the PathProbe tab, and then click Load.

For information about the individual results in this report, click Help. You can also place the cursor over a specific line to view tooltip information, as shown in the following figure.

Figure 4-14 PathProbe Results Dialog Box



Related Topics

- *Capture Manager*

Collecting Performance Data from AppInternals Xpert

You can collect statistics directly from AppInternals Xpert as part of the traffic-capture process.

In AppInternals Xpert, a *correlation view* specifies a customized set of statistics for which you want to display data. When a capture operation finishes, Capture Manager can retrieve data from AppInternals Xpert based on the capture time window and a correlation view.

Procedure 4-10 Collecting AppInternals Xpert Data During a Capture Operation

- 1 Open Capture Manager using one of the following methods:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager
- 2 Click the On-Demand Capture tab.
- 3 Select the “Collect performance statistics from AppInternals Xpert” checkbox and click the Configure... button.
 - ➡ The Configure AppInternals Xpert Collection dialog box appears.
- 4 Specify the following information:
 - AppInternals Xpert hostname—Specifies the hostname where AppInternals Xpert is installed.
 - Username—Specifies the username to log on to AppInternals Xpert.
 - Password—Specifies the password associated with the username.
 - Connect using SSL—When checked, communication with AppInternals Xpert SMP will be encrypted using SSL.
 - Store password as clear text in Agent List file—When checked, the password is stored as clear text (e.g., unencrypted) in the Agent List file. Otherwise, the password is saved in memory and must be retyped every time AppTransaction Xpert is restarted.
 - Correlation view—Specifies the correlation view for the data that you want to collect.
- 5 Click OK.

- 6 Run the capture operation as described in Procedure 4-6 Capturing Traffic with Capture Manager.
 - When the capture operation finishes, AppTransaction Xpert does the following:
 - Downloads performance data from the AppInternals Xpert server, based on the time window of the capture and the selected correlation view
 - Stores the AppInternals Xpert data as a .pan file in the download directory of the AppTransaction Xpert computer
- 7 To view the AppInternals Xpert data in AppTransaction Xpert, do the following:
 - Import the packet traces, as described in Creating a Transaction Analyzer Model.
 - Import the AppInternals Xpert data into an existing Transaction Analyzer model, as described in Transaction Trace Analysis.

End of Procedure 4-10

For more information about correlation views, see the AppInternals Xpert documentation.

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Running Scheduled Captures and Downloads

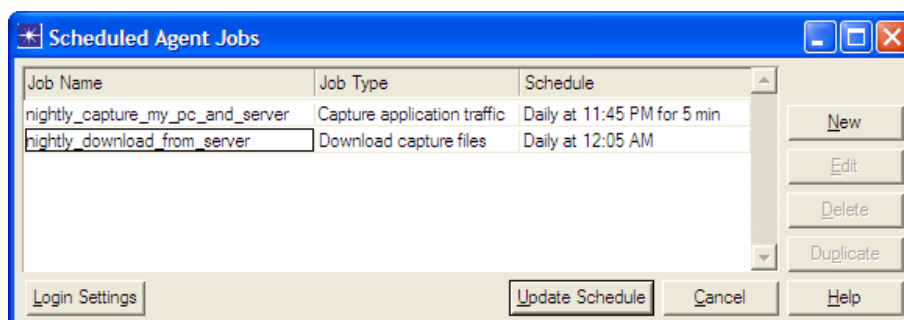
You can capture traffic and download packet traces at regular, pre-scheduled intervals. For example, you can capture traffic at regular intervals during the week (for troubleshooting intermittent network problems). You might also find it convenient to download all remote packet traces using a nightly scheduled download, when network traffic is lightest.

Note—This feature requires a license for AppTransaction Xpert Advanced Capabilities.

Procedure 4-11 Creating and Editing a Scheduled Capture/Download

- 1 A scheduled capture/download requires a capture agent list that specifies the agents and agent settings to use for that job. You have three options:
 - Specify the agent settings currently selected in Capture Manager
 - Use an existing agent (*.agents) list
 - Create a new agent list (as described in Creating a Capture Agent/Appliance List)
- 2 Open Capture Manager using one of the following methods:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager.
- 3 Create a job:
 - 3.1 In Capture Manager, click “Schedule Agent Jobs...”.
 - ➔ The Scheduled Agent Jobs dialog box appears.

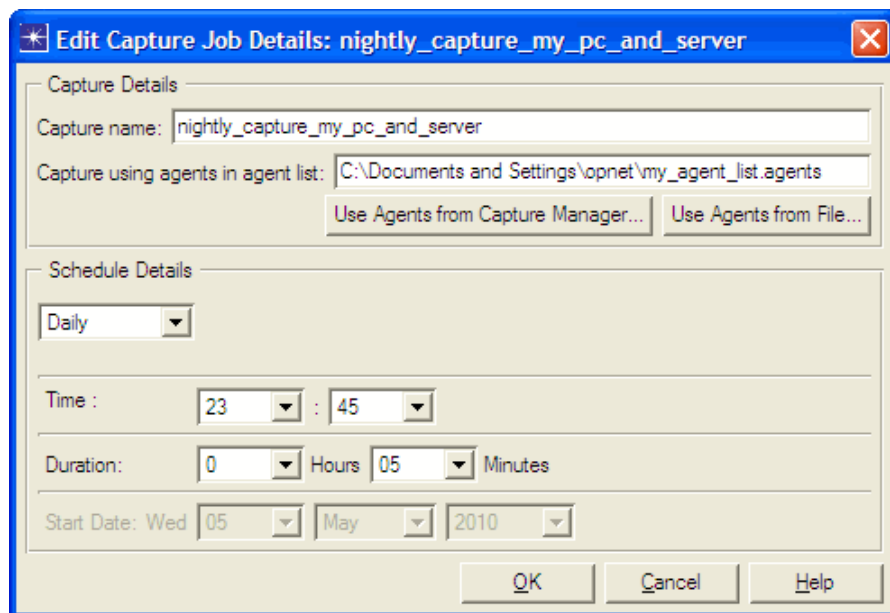
Figure 4-15 “Scheduled Agent Jobs” Dialog Box



The dialog box lists all scheduled jobs that are currently defined.

- 3.2 Click New to add a row to the table.

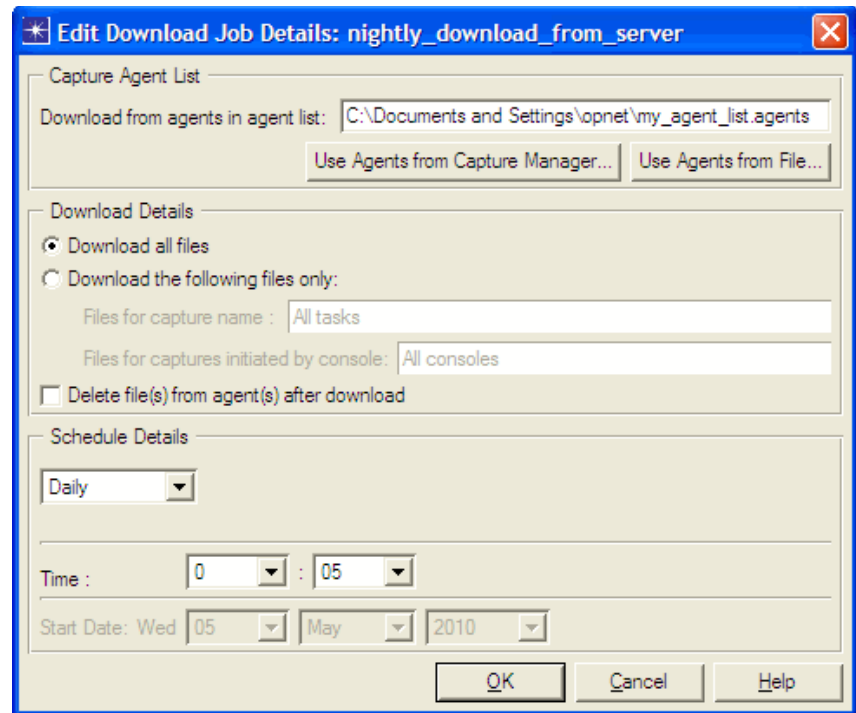
- 3.3 Verify that the Job Type field is set correctly (either “Capture application traffic” or “Download capture files”).
- 3.4 In the Job Name field, enter a descriptive name for the job (for example, “nightly_download_from_remote_office” or “daily_3pm_capture_from_web_server”).
- 4 Edit the job: perform step 5 for a capture job or step 6 for a download job.
- 5 To edit a capture job, do the following:
 - 5.1 In the “Scheduled Agent Jobs” Dialog Box, click in the Schedule column for the capture job (or select the job in the Job Name column and click Edit).
 - ➔ The “Edit Capture Job Details” dialog box appears.



- 5.2 Enter a descriptive name in the “Capture name” field.
 - Set the “Capture using agents in agent list” option to specify the file with the agents and options to use for the scheduled capture.
 - To select an existing file, click Use Agents from File.
 - To use the capture agents and options currently specified in Capture Manager, click Use Agents from Capture Manager. This gives you the option to save the current agent list—that is, the capture agents and settings currently specified in Capture Manager—to a file that the scheduled capture can use. (This option is available only if there is at least one agent enabled in the Capture Manager.)
- 5.3 Under Schedule Details, specify the frequency (One time/Daily/Weekly/Monthly), start time, duration, and start date of the scheduled capture.
- 5.4 After specifying the job options, click OK and proceed to step 7.
- 6 To edit a download job, do the following:

- 6.1** In the Scheduled Agent Jobs dialog box, click in the Schedule column for the download job (or select the job in the Job Name column and click Edit).

➡ The Edit Download Job Details dialog box appears.



- 6.2** Set the “Download from agents in agent list” option to specify the file with the remote agents from which the packet traces will be downloaded.

- To select an existing file, click Use Agents from File.
- To use the agents and options currently specified in Capture Manager, click Use Agents from Capture Manager. This provides the option to save the current agent list—that is, the capture agents and settings currently specified in Capture Manager—to a file that the scheduled capture can use. (This option is available only if there is at least one agent enabled in the Capture Manager.)

- 6.3** Under Download Details, specify the capture name and the console that initiated the capture to download. The download job uses these fields to locate the packet traces to download from the remote agent. An agent stores files locally in the following directory:

```
<capture_save_dir>/
  capture_files/
    <capture_name>/
      <console_location>
```

Because these fields are set to “All tasks” and “All consoles” by default, perform this step only if you want the job to download some (not all) files from the remote agent.

- 6.4** Set the “Delete file(s) from agent(s) after download” checkbox as needed. This option is turned off by default so that remote packet traces are not unintentionally deleted.

6.5 Under Schedule Details, specify the frequency (One time/Daily/Weekly/Monthly), start time, and start date of the scheduled download.

6.6 Click OK.

7 Optionally, create, delete, or edit other jobs in the “Scheduled Agent Jobs” dialog box.

8 Click Update Schedule.

➔ The jobs will run as specified in the “Scheduled Agent Jobs” dialog box.

End of Procedure 4-11

If you encounter problems with a scheduled job, the following resources are available:

- AppTransaction Xpert log. The scheduler generates log messages when it executes a scheduled job. To view this log, open the Log Viewer (choose Help > Show All Logs), then go to the ACE tab.
- Logs or other diagnostic information generated by the operating system. The problem might lie in the scheduler (such as cron on Solaris or the Windows task scheduler).
- Frequently asked questions can be searched in the Knowledge Base on the Support website.

Related Topics

- *Capturing Traffic with AppTransaction Xpert*

Downloading Packets from High Speed Captures on AppResponse Xpert Appliances

You can view and download traffic from AppResponse Xpert appliances with high speed capture using Capture Manager. This workflow is provided in case you need basic pre-download filtering—time window, IP addresses, and/or protocols—only, and do not want to run AppResponse Xpert.

Note—In most cases, it is best to select AppResponse Xpert traffic in the AppResponse Xpert console, not Capture Manager. AppResponse Xpert provides extensive functionality for identifying problematic transactions (and filtering out irrelevant traffic) before sending the traffic of interest to AppTransaction Xpert. For more information, see the AppResponse Xpert documentation: User Guide > Viewing AppResponse Xpert Traffic in AppTransaction Xpert.

Note the following:

- An AppResponse Xpert appliance with high speed capture supports only one continuous capture process at any one time.
- All capture operations—starting, stopping, configuring—are performed in the web UI of the AppResponse Xpert appliance. Previewing and downloading are the only operations supported from Capture Manager.
- AppResponse Xpert appliances with high speed capture do not support on-demand captures.
- For information about capturing and viewing traffic on other types of AppResponse Xpert appliances, see the following:
 - AppTransaction Xpert *documentation*: Configuring an AppResponse Xpert Capture
 - AppResponse Xpert *documentation*: User Guide > Viewing AppResponse Xpert Traffic in AppTransaction Xpert

The following procedure describes the workflow for downloading traffic from AppResponse Xpert appliances with high speed capture.

Procedure 4-12 Downloading Traffic from an AppResponse Xpert Appliance with High Speed Capture

- 1 Open Capture Manager using one of the following methods:
 - From the AppTransaction Xpert System window, choose File > Capture Manager...
 - From the Transaction Analyzer window, choose Capture > Capture Manager
- 2 Click the AppResponse Xpert tab.

3 Add an appliance with high speed capture:**3.1** Click Add Appliance...

➡ The Editor AppResponse Xpert Appliance Entry dialog box appears.

3.2 Enter the requested information: hostname or IP address of the appliance, TCP port, and description.

By default, AppResponse Xpert 4100 appliances use TCP port 24701 to communicate with Capture Manager. You do not need to change the “TCP port” field unless the appliance was specifically configured to use a different port.

3.3 Click OK to return to Capture Manager.**4** Verify that the appliance is currently capturing: select the appliance in the Capture Agents treeview, then click Update Status. The Status field should report that one capture is currently active.

To start, stop, and configure captures on appliances, log in to the web UI (https://<appliance_hostname>:8443) and select System > Capture page.

5 Select the appliance in the Capture Agents treeview and click Download/Preview...

➡ The Preview AppTransaction Xpert Captures dialog box appears. (Note that there is only one continuous capture on the appliance.)

6 Select the capture and then click Preview.

➡ The Specify Traffic to Preview for Capture window appears.

7 Specify the traffic that you want to preview.

Note—It is good practice to filter as much irrelevant traffic as possible in this window. You can apply the following filters:

- Time (“Include the following time range” radio buttons)
- IP addresses and conversations (“Include the following IP addresses and/or IP conversations” checkbox and table)
- IP address ranges (“Include the following IP address ranges” checkbox and table)
- Top IP conversations by throughput (“Display the top X IP conversations by throughput” field)

8 Click Preview.

➡ The selected traffic appears. For more information, see Continuous Capture: Preview and Download.

End of Procedure 4-12

Related Topics

- *Capturing Traffic with AppTransaction Xpert*