9 Filtering Traffic

AppTransaction Xpert produces the most accurate results when the transaction analyzer model contains only one user-level transaction, and includes only the traffic that is relevant to that transaction. Therefore, it is important to ensure that a packet trace contains no irrelevant traffic. To achieve the most accurate results, you can filter traffic.

You can filter traffic during the following phases:

- Capture phase
- Using Trace Explorer (post-capture, or during import)
- In Transaction Analyzer (post-import)

Note—When capturing traffic, err on the side of caution—filter only traffic that you know is irrelevant. If any irrelevant traffic remains, you can filter the traffic from within Transaction Analyzer.

This section includes the following topics:

- Packet Filtering
- Filtering Packet Traces in Trace Summary/Trace Explorer
- Multi-Tier Correlation—Overview
- Multi-Tier Correlation using String Filtering
- Multi-Tier Correlation using a Reference File
- Multi-Tier Correlation Temporal Filtering (Experimental)

Packet Filtering

Packet filters are useful for filtering irrelevant traffic. Use packet filters when:

- Capturing traffic with AppTransaction Xpert capture agents—
  You can apply a filter to a capture agent in the Remote Application Capture Agent Editor dialog box, as described in Configuring a Capture Agent.
- Importing capture data into AppTransaction Xpert—
  You can apply a filter to a packet trace in the Merge Capture Files Dialog Box.
- Viewing capture data in Trace Explorer and Transaction Analyzer—
  You can apply a filter to a packet trace by choosing Edit > Filter Trace…

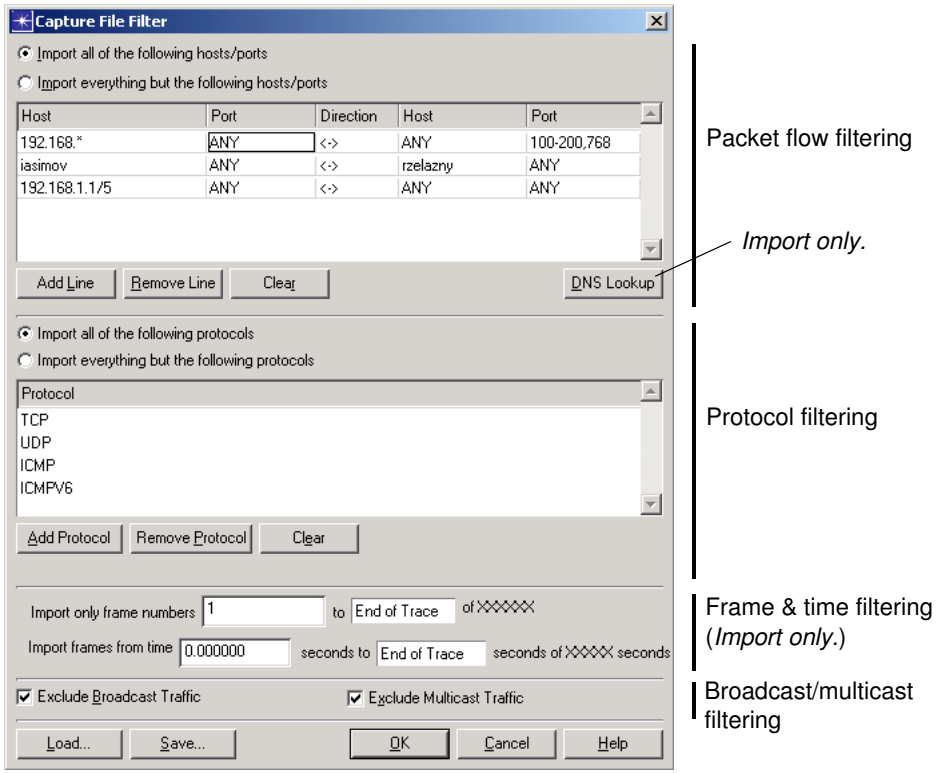
By default, AppTransaction Xpert captures and imports nearly all non-broadcast, non-multicast packets. Filtering is configured in the Capture File Filter dialog box. (See Figure 9-1.) You can filter packets based on hosts, ports, direction, and protocols. You can also save a defined filter and reuse it when creating other Transaction Analyzer models.

Packet Trace Filters

A packet trace filter consists of criteria specifying the traffic to filter (to include or to exclude). Criteria is specified in the Capture File Filter dialog box, which contains sections for specifying several types of criteria:

- Packet flow (host, port, and direction)
- Protocols
- Frame numbers and time ranges
- Broadcast/multicast traffic

Figure 9-1 Capture File Filter Dialog Box (Capture and Import Version)



The specified criteria is combined to create the composite filter, as follows:

1) All lines in the packet flow filtering table are logically OR'ed to create the packet flow criteria.

2) All lines in the protocol filtering table are logically OR'ed to create the protocol criteria.

3) All sections of the dialog box are logical AND'ed to create the composite filter.

For example, if the packet flow filtering table is configured to import all packets originating from host A and the protocol filtering table is configured to import only those packets that do not have UDP data, the resulting filter will import only those packets originating from host A that do not have UDP data (these might be TCP, DLC, and others).

Use the following procedure to specify a filter for capturing traffic with a capture agent or importing captured traffic into AppTransaction Xpert.

Procedure 9-1 Specifying a Packet Trace Filter for Captures and Imports

1 Choose whether packet flow filtering is used to include or exclude packet flows from the capture by selecting one of these radio buttons:

- Import all of the following hosts/ports
- Import everything but the following hosts/ports

2 In the packet flow filtering table, specify the source and destination hosts and ports, as follows:

- Set each Host cell to one of the following:
  - "ANY"
  - IP address—this can be a full address, a partial address ending in a * wildcard (such as 172.* or 192.168.42.*), or an address using slash notation (such as 192.168.1.1/9, where /9 is equivalent to matching the IP address using a mask of 255.128.0.0)
  - DNS name (capture filters only)
- Set each Port cell to one of the following:
  - a single port number
  - a range of port numbers (such as 100-249)
  - a comma-separated list of any combination of single port numbers and port ranges

Note—To sort the table, click on a column heading.

3 Specify the direction of packet flow (unidirectional or bidirectional) by clicking in the Direction cell and selecting a direction.

4 To add another packet flow filter, click the Add Line button and repeat steps 2 and 3.

5 Choose whether protocol filtering is used to include or exclude protocols from the capture by selecting one of these radio buttons:

- Import all of the following protocols
- Import everything but the following protocols

6 Specify the protocols of interest:

- To add another protocol, click the Add Protocol button and select a protocol. (Select "<UNSPECIFIED>" to match all protocols.)
- To change a protocol, select it and choose a different protocol from the pop-up list.
- To remove a protocol, select it and click the Remove Protocol button.

7 If needed, specify frame number and time stamp ranges for filtering.

8 Set the "Exclude Broadcast Traffic" and "Exclude Multicast Traffic" checkboxes as needed.

9 Click Save… to save the filter.

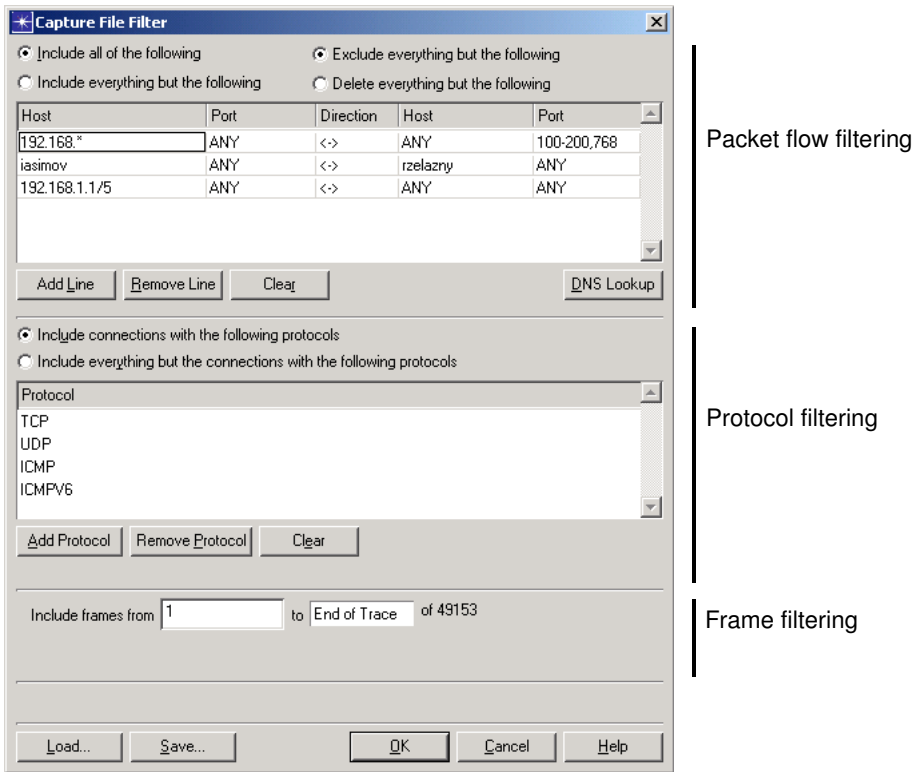
10 Click OK to close the dialog box.

End of Procedure 9-1

Use the following procedure to specify a filter for viewing captured traffic in Trace Explorer.

Procedure 9-2 Specifying a Packet Trace Filter for Trace Explorer

Figure 9-2 Capture File Filter Dialog Box (Trace Explorer Version)



1 Choose whether packet flow filtering is used to include or exclude packet flows from the trace by selecting one of these radio buttons:

- Include all of the following
- Include everything but the following

For either selection, you can use the radio buttons on the right side to specify whether packet flows not included are excluded (simply ignored) or deleted from the trace.

2 In the packet flow filtering table, specify the source and destination hosts and ports, as follows:

- Set each Host cell to one of the following:
  - “ANY”
  - DNS name

- IP address—this can be a full address, a partial address ending in a * wildcard (such as 172.* or 192.168.42.*), or an address using slash notation (such as 192.168.1.1/9, where /9 is equivalent to matching the IP address using a mask of 255.128.0.0)

- Set each Port cell to one of the following:
  - a single port number
  - a range of port numbers (such as 100-249)
  - a comma-separated list of any combination of single port numbers and port ranges

Note—To sort this table, click on a column heading.

3 Specify the direction of packet flow (unidirectional or bidirectional) by clicking in the Direction cell and selecting a direction.

4 To add another packet flow filter, click the Add Line button and repeat steps 2 and 3.

5 Choose whether protocol filtering is used to include or exclude protocols from the capture by selecting one of these radio buttons:
- Include connections with the following protocols
- Include everything but the connections with the following protocols

6 Specify the protocols of interest:
- To add a protocol, click the “Add Protocol” button and select a protocol. (Select “<UNSPECIFIED>” to match all protocols.)
- To change a protocol, select it and choose a different protocol from the pop-up list.
- To remove a protocol, select it and click the “Remove Protocol” button.

7 If needed, specify a frame number range for filtering.

8 Click Save… to save the filter.

9 Click OK to close the dialog box.

End of Procedure 9-2

Note—To capture VLAN traffic from an AppTransaction Xpert capture agent using an IP-based filter, you must set the “ace_capture_vlan_bpf_enable” preference to TRUE.

Related Topics

- *Filtering Traffic*

Filtering Packet Traces in Trace Summary/Trace Explorer

Use Trace Summary and Trace Explorer to browse large packet traces, find user-level transactions of interest, and create Transaction Analyzer models from those transactions.

Trace Explorer is a *stand-alone* window for browsing packet traces and extracting relevant traffic. Trace Explorer is especially helpful when working with large packet traces that may take longer to open directly to AppTransaction Xpert.

Trace Summary is used after import to browse and filter traffic.

Related Topics

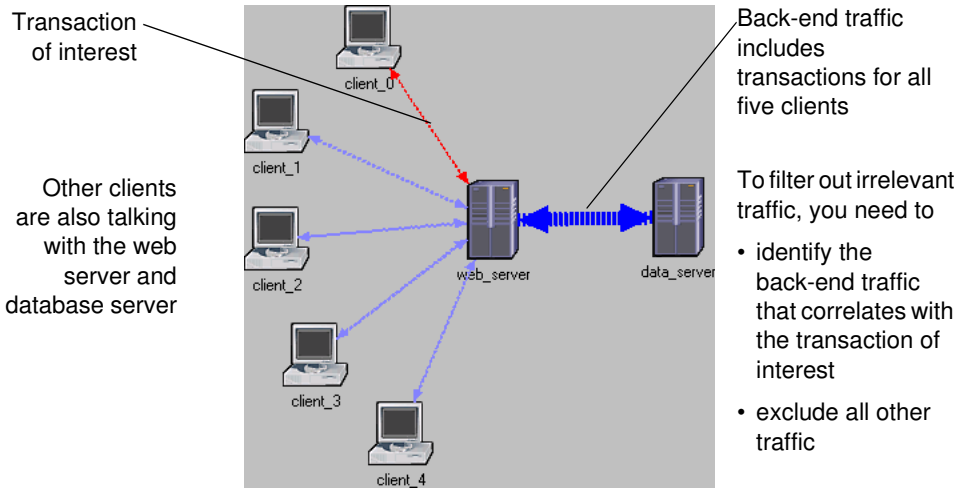
- *Filtering Traffic*

Multi-Tier Correlation—Overview

Multi-tier correlation is a method for excluding irrelevant traffic from a Transaction Analyzer model file, based on traffic that was captured in a production environment. The goal is to create a file that models the effects of a busy network but excludes all irrelevant traffic. This method is useful when you want to diagnose your production environment and how it affects your applications.

Multi-tier correlation is a solution to a common problem when capturing multi-tier applications in production environments. When you try to capture at a tier that does not communicate with the client directly, it is often difficult to filter out irrelevant traffic. (When capturing at the client tier, you can filter traffic using IP addresses.) Filtering traffic is especially difficult when a tier handles multiple transactions simultaneously, as shown in the following figure.

Figure 9-3 Multi-Tier Application in a Production Environment: Example



Multi-tier correlation enables you to create a *clean* Transaction Analyzer model file by identifying and extracting the traffic that correlates to the transaction of interest, and excluding all other traffic.

The following methods are available for performing multi-tier correlation:

- Multi-Tier Correlation using String Filtering—When using this method, you correlate traffic by searching for connections with packets that contain a specific string. The search string acts as a *flag* that identifies individual packets as part of the transaction of interest.
- Multi-Tier Correlation using a Reference File—When using this method, you correlate traffic by matching packets in two separate Transaction Analyzer model files. To use this method, you must create two files of the transaction: a production file that includes extraneous traffic, and a reference file (captured in a *clean* environment) that includes only traffic relevant to the transaction of interest.
- Multi-Tier Correlation Temporal Filtering (Experimental)—When using this method, you correlate traffic by using the timing of messages across tier pairs. First you filter out traffic from the client tier to the first server tier that is not part of the transaction of interest. Then you run one of the three temporal correlation workflows to isolate the transaction of interest on the back-end tiers. All three approaches revolve around a system of scoring messages based on how well they line up with the traffic in the preceding tier pairs.

Related Topics

- *Filtering Traffic*

Multi-Tier Correlation using String Filtering

String filtering is a method in which you correlate packets that contain a specific string. If you know that the transaction of interest uses a specific string, you can identify and extract every connection that contains one or more packets with that string. Unlike the reference file method, this method does not require a second Transaction Analyzer model file.

This method is most useful when

- the transaction uses one or more connections that are not used by other transactions
- these connections use a specific string or sequence of bytes that identify them as part of the transaction
- the transaction does not involve connection multiplexing at any tiers whose traffic you want to correlate

---

Procedure 9-3 Correlating Traffic using String Filtering

1. Open the Transaction Analyzer model containing the traffic that you want to correlate.
2. Choose Advanced > Multi-Tier Correlation > Using String Filtering.

   You are then guided through the correlation and extraction process:

   - Step 1: Select the tier pairs that contain the traffic to correlate (see Select Tier Pairs to Filter Dialog Box)
   - Step 2: Enter the search string or hexadecimal pattern for correlating the traffic (see Choose Search Pattern Dialog Box)
   - Step 3: View the correlation results and exclude the unmatched traffic (see View Results and Exclude Unmatched Dialog Box)

   Note—It is good practice to save the extracted production task under a different name so you still have a copy of the original task.

End of Procedure 9-3

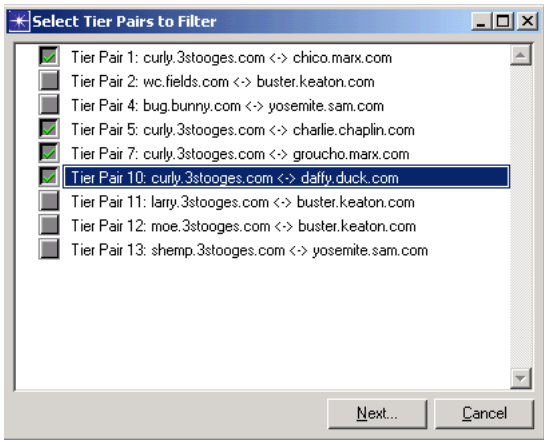
Related Topics

- *Multi-Tier Correlation using a Reference File*

Select Tier Pairs to Filter Dialog Box

The Select Tier Pairs to Filter dialog box appears immediately after you choose Advanced > Multi-Tier Correlation > Using String Filtering. This dialog box lists all tier pairs in the transaction analyzer model, and prompts for the tier pairs that contain the traffic that you want to correlate. (The correlation operation has no effect on tier pairs that are not selected.)

Figure 9-4 Select Tier Pairs to Filter Dialog Box



After you select the tier pairs, click Next to open the next window (see Choose Search Pattern Dialog Box).

Choose Search Pattern Dialog Box

The Choose Search Pattern dialog box appears after you click Next in the Select Tier Pairs to Filter Dialog Box. This dialog box prompts for the string or byte sequence to search for in the selected tier pairs.

To correlate traffic accurately, you must search on a string that is expected to appear only in the transaction of interest, based on your knowledge of the application. Examples of possible strings include a transaction ID or the search string used in a database query. To see the packets that correlate to a string or byte sequence, you can do a preliminary search using the Find Packets operation (Edit > Find Packets). To search for a hexadecimal string, you can obtain possible values by viewing hexadecimal decodes in the Protocol Decode Viewer. For more information, see Protocol Decodes.

Figure 9-5 Choose Search Pattern Dialog Box

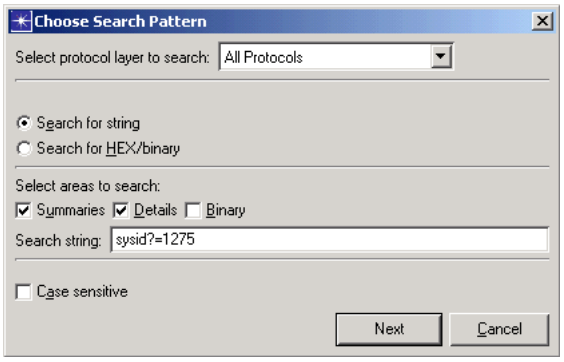


Table 9-1 Choose Search Pattern Dialog Box

Option / Field	Description
Select protocol layer to search	Restricts the search to a specific protocol layer. Only packets that contain the search pattern within this protocol layer are marked for correlation.
Search for string Search for HEX/binary	Specifies whether to search on ASCII text or a hexadecimal/binary sequence of bytes
Select areas to search	Selects the packet sections to search. The available options are: • Summaries—Search protocol summary information, as shown in the Decode Summary column (“Search for string” option only) • Details—Search all protocol data, as shown in the protocol decodes for individual frames (“Search for string” option only) • Binary—Search the binary/hexadecimal bytes in each frame, as shown in the HEX decodes for individual frames You can view the summary, details and binary contents of frames in the Protocol Decode Viewer (see Protocol Decode Viewer).
Search string	Specifies the search string for correlating traffic. All connections with at least one packet that contains this string are marked for correlation.
Case sensitive	Specifies to use case-sensitive searching

View Results and Exclude Unmatched Dialog Box

The View Results and Exclude Unmatched dialog box appears after you click Next in the Choose Search Pattern Dialog Box, and shows the results of the correlation based on the specified search string. The table shows the number of matched and unmatched connections for each tier pair. You can view matched traffic in the Protocol Decode Viewer and exclude unmatched connections.

If you are not satisfied with the correlation, click Cancel and repeat this procedure using a different search string. Otherwise, click Exclude Unmatched to exclude the unmatched connections.

Figure 9-6 View Results and Exclude Unmatched Dialog Box

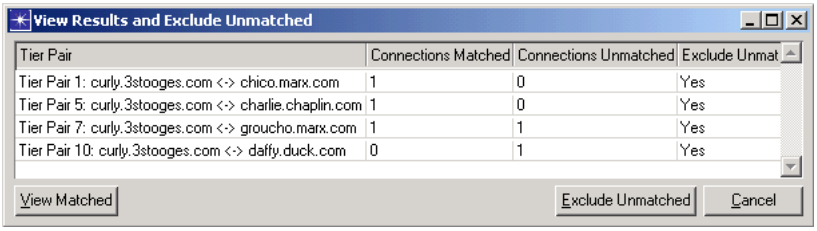


Table 9-2 View Results and Exclude Unmatched Dialog Box

Column	Description
Tier Pair table	Shows all tier pairs selected for correlation. For each tier pair, this table shows: • Connections Matched—The number of connections that contain packets with the search string • Connections Unmatched—The number of connections that contain no packets with the search string • Exclude Unmatched?—By default, this field is set to Yes. If you do not want to exclude the unmatched connections for a tier pair, set the field to No.
View Matched	Views all matched traffic in the Protocol Decode Viewer
Exclude Unmatched	Excludes unmatched connections from the Transaction Analyzer model file

Multi-Tier Correlation using a Reference File

This multi-tier correlation method requires two separate files:

- A *production task*—A task of your application that includes extraneous traffic that you cannot filter by IP address.
- A *reference task*—A task of your application that contains only traffic that is relevant to the application. AppTransaction Xpert uses this task to determine the relevant traffic in your production task. You should capture this application in a *clean* environment: in a lab or on the main network during off-hours.

  If you cannot produce a reference task of the transaction, then correlate the traffic using the string-filtering method described in Multi-Tier Correlation using String Filtering.

To correlate the production and reference traffic, AppTransaction Xpert compares the application data in individual packets. This means that traffic for the application of interest should be roughly equivalent in both tasks. In this case, “roughly equivalent” means that relevant packets contain similar application data in both tasks. Therefore, this feature is most useful when the following conditions are true:

- You can reproduce the same transaction in both environments. Some transactions such FTP downloads or database queries can be reproduced easily. Other transactions such as voice or video-conferencing sessions are not easily reproduced.
- AppTransaction Xpert can correlate the tasks most accurately if the hosts segment and transfer data consistently in both transactions. Therefore, the segmentation behavior (such as TCP window size and maximum segment size) on the relevant hosts should be consistent in both transactions. For example, if a server downloads the same file using different default packet sizes, AppTransaction Xpert cannot correlate the traffic accurately.

It’s not necessary for all packets to match exactly or for hosts to always transmit packets in the same order. However, for AppTransaction Xpert to correlate the traffic automatically and accurately, the individual packets should be roughly equivalent.

Note—For AppTransaction Xpert to correlate the two tasks, both packet traces must be in a supported binary file type. Additionally, both packet traces must be full capture length, so that the full application payload is included in each packet trace.

For more information, see Supported Packet Trace Formats.

Workflow Description

After creating the production and reference tasks, the Multi-Tier Correlation Wizard guides you through the correlation and extraction process, which has two phases:

1) Correlate traffic—The Correlation Wizard prompts for the information needed to correlate traffic in the production task with the “equivalent” traffic in the reference task.

2) Extract traffic—After you specify the correlated and uncorrelated traffic in the production task, the final step is to extract the uncorrelated traffic. The extracted production task models the application of interest in a busy network.

Procedure 9-4 Correlating Traffic with a Reference Task

1 Open the production task in Transaction Analyzer.

2 In the Tree View tabbed page, choose Advanced > Multi-Tier Correlation > Using Reference Trace.

This Multi-Tier Correlation Wizard appears and guides you through the correlation and extraction process:

- Step1: Select the reference task (see Select Reference Task Dialog Box)
- Step 2: Correlate the production and reference tiers; specify order of tier talking if desired (see Configure Tiers Dialog Box)
- Step 3: Remove uncorrelated or irrelevant tier pairs; specify advanced correlation options (see Configure Tier Pairs Dialog Box)
- Step 4: View, revise and edit the correlation (see Manage Correlation Dialog Box and Tier Pair Correlation Assistant)
- Step 5: Exclude the uncorrelated traffic from the production task (Extract Correlated Traffic Dialog Box)

This operation makes the following changes to the production task:

- All uncorrelated frames are excluded
- If reordering is enabled, then some frames may be reordered.

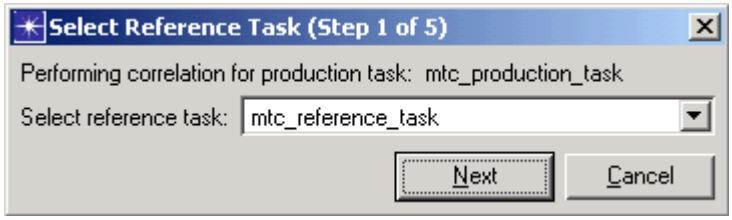
Note—It is a good idea to save the extracted production task under a new name so you still have a copy of the original task.

End of Procedure 9-4

Select Reference Task Dialog Box

This dialog box appears when you choose Advanced > Multi-Tier Correlation > Using Reference Trace. Select the Transaction Analyzer model file to use as the reference task, then click Next to see the Configure Tiers Dialog Box.

Figure 9-7 Select Reference Task Dialog Box



Note—If your reference task does not appear in this pull-down menu, then the model directory list does not include the directory where the task resides. In this case, click Cancel and choose File > Model Files > Add Model Directory. When you choose Advanced > Multi-Tier Correlation again, the task will appear in the pull-down menu.

Configure Tiers Dialog Box

The Configure Tiers dialog box appears after you select your reference task and then click Next in the Select Reference Task Dialog Box. You use this dialog box to map tier names between the production task and reference tasks, and to specify the order of tier talking in the production task.

Figure 9-8 Configure Tiers Dialog Box

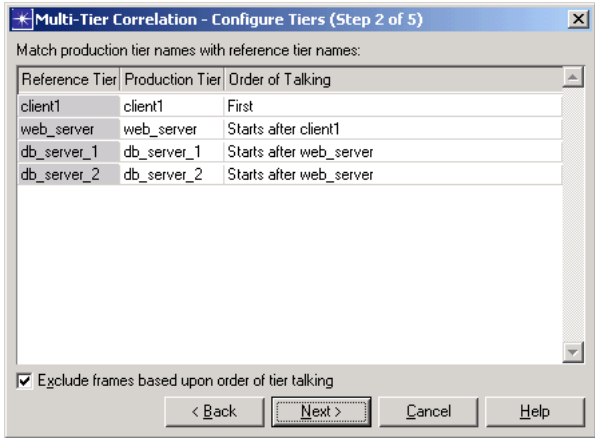


Table 9-3 Configure Tiers Dialog Box

Option / Field	Description
Production Tier	Set the Production Tier pull-down menu to map each tier in the production task to its corresponding tier in the reference task.

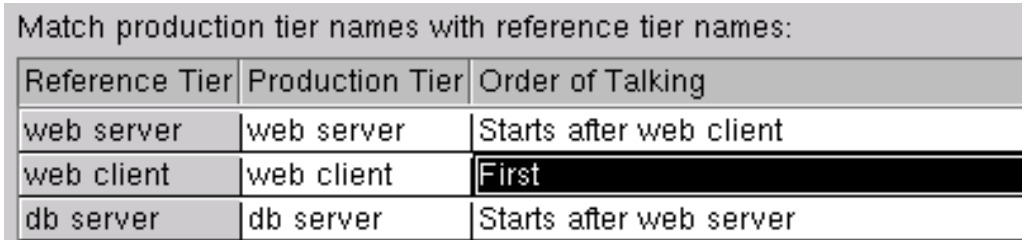
Table 9-3 Configure Tiers Dialog Box (Continued)

Option / Field	Description
Order of Talking	Specify the order of talking for each production tier. If the tiers always talk in a fixed order, set the menu options to specify the order of talking; if you are unsure of the order for a specific tier, set the field to “Unknown”. If you uncheck the “Exclude frames based on order of talking” checkbox, this row is disabled. For more information, see Order of Talking: An Example.
Exclude frames based on order of talking	If this checkbox is enabled, AppTransaction Xpert identifies and excludes production traffic that falls outside the order of talking. If the tiers in your application do not talk in a predictable sequence, you should uncheck this option.

Order of Talking: An Example

A web-based database transaction normally consists of a predictable sequence of phases: web client sends request to web server (phase 1), web server forwards request to database server (phase 2), and so on. In this case, you would specify the order of talking as shown in the following figure.

Figure 9-9 Order of Talking Example



AppTransaction Xpert uses this knowledge to identify and mark the following traffic as uncorrelated:

- All web-server traffic before the client sends the initial request (phase 1)
- All database-server traffic before the web server forwards the request (phase 2)

Configure Tier Pairs Dialog Box

The Configure Tier Pairs dialog box appears after you specify the tier correlation and order of talking, and then click Next in the Configure Tiers Dialog Box. Use this dialog box to remove tier pairs from the correlation and edit the tier correlation that you specified previously.

Figure 9-10 Configure Tier Pairs Dialog Box

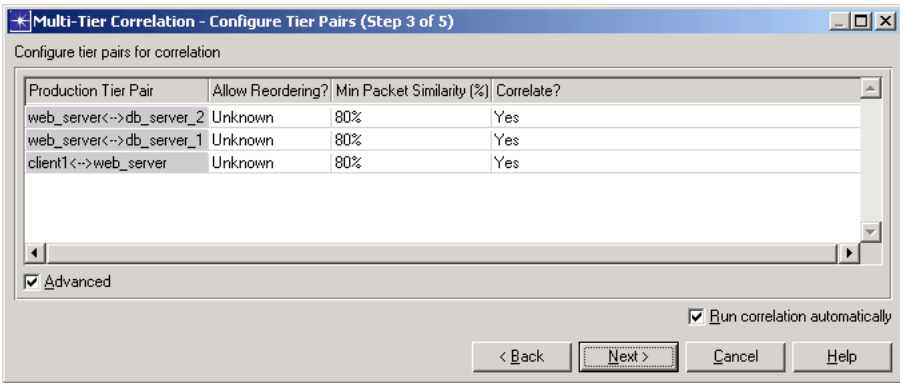


Table 9-4 Configure Tier Pairs Dialog Box

Option / Field	Description
Allow Reordering	Specifies whether AppTransaction Xpert reorders frames in the production task to match the frame order in the reference task. The possible settings are: • Yes—After AppTransaction Xpert correlates the two tasks, it reorders production frames (if necessary) to match the order of reference frames. • No—After the correlation, AppTransaction Xpert does not reorder any production frames. • Unknown—During correlation, AppTransaction Xpert tries to determine whether any production frames are in a different order from the reference task.
Correlate	If set to No, AppTransaction Xpert does not try to correlate traffic on that tier pair. Instead, it assumes that all traffic on that tier pair is relevant. You should set this option to No if the tier pair contains no irrelevant traffic.
Min Packet Similarity	Specifies the minimum similarity threshold that AppTransaction Xpert uses to include a packet in the correlation set. AppTransaction Xpert compares the application payload data to determine whether a production packet is similar to a reference packet. A higher setting results in faster correlations, but might cause some similar packets to be uncorrelated.

Table 9-4 Configure Tier Pairs Dialog Box (Continued)

Option / Field	Description
Run Correlation Automatically	If this option is enabled, AppTransaction Xpert correlates the production and reference tasks after you click Next. You can edit the correlation in the Manage Correlation Dialog Box. If you want to specify the entire correlation manually, disable this checkbox.

Manage Correlation Dialog Box

The Manage Correlation dialog box appears after you click Next in the Configure Tier Pairs Dialog Box. This dialog box enables you to view and edit the current correlation. When you are satisfied with the correlation of all tier pairs, click Next to proceed to the Extract Correlated Traffic Dialog Box.

Figure 9-11 Manage Correlation Dialog Box

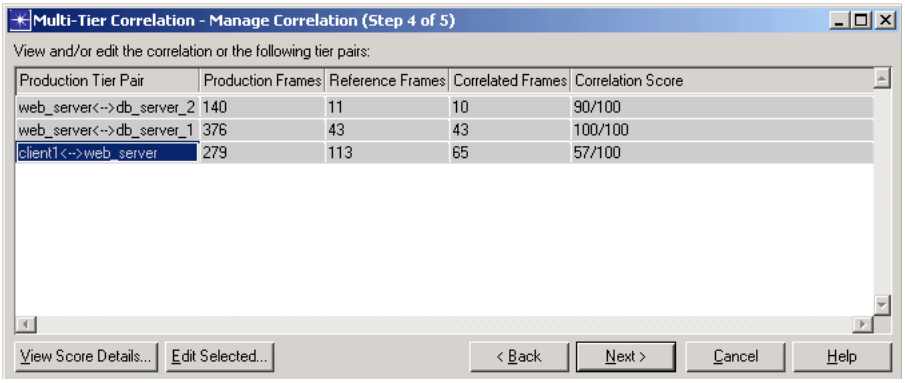


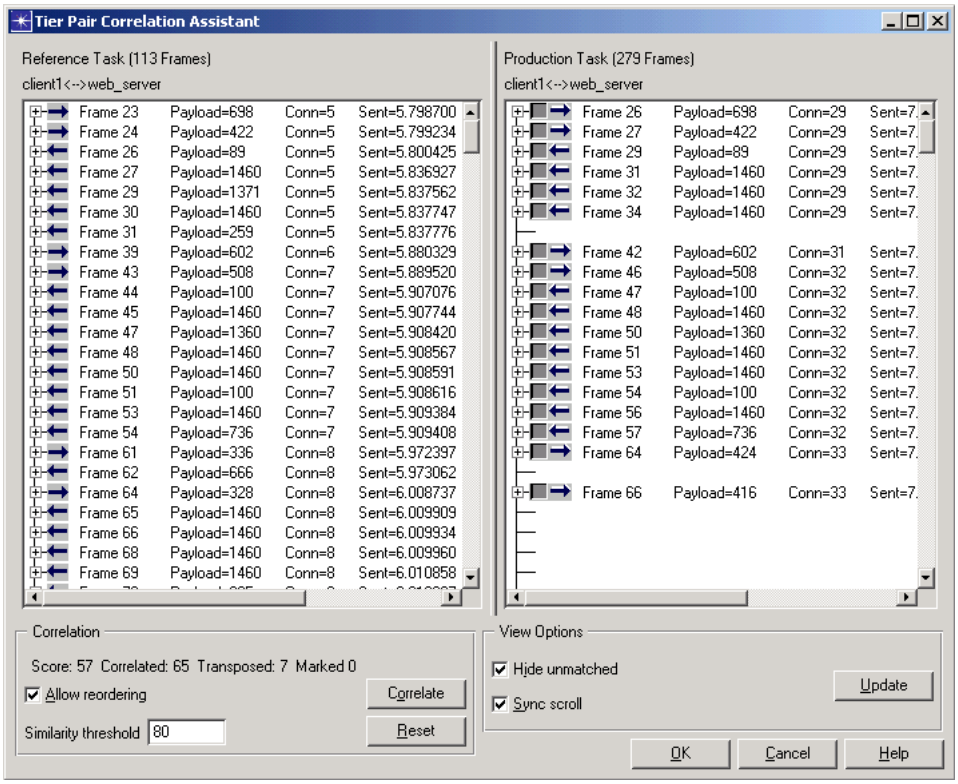
Table 9-5 Manage Correlation Dialog Box

Option / Field	Description
Production Frames	The total number of production frames for that tier pair
Reference Frames	The total number of reference frames for that tier pair
Correlated Frames	The total number of reference frames currently included in the correlation set. If you disabled manual correlation in the Configure Tiers Dialog Box, this number is 0 when the window initially opens.
Correlation Score	The correlation score (out of 100) for the tier pair. If every reference frame is correlated, the score is 100/100.
Edit Selected	View or manually edit the correlation for the selected tier pair. For more information, see Tier Pair Correlation Assistant.
View Score Details	View details of the current correlation

Tier Pair Correlation Assistant

The Tier Pair Correlation Assistant dialog box appears when you select a tier pair and then click Edit Selected in the Manage Correlation Dialog Box. Use this window to view or manually edit the current correlation for a tier pair. The Reference Task (left) and Production Task (right) treeviews show the frames in the corresponding tasks.

Figure 9-12 Tier Pair Correlation Assistant



The Tier Pair Correlation Assistant dialog box uses the following conventions:

- By default, the two treeviews are aligned based on the current correlation. If a reference frame and a production frame share the same row (across both treeviews), the two frames are correlated. If a production frame is not correlated, the corresponding row in the Reference Task treeview is empty.

  If the current correlation includes a reordered frame, the Reference Task treeview shows a yellow arrow, indicating that the correlated production frame was reordered.

  To disable the Reference Task/Production Task treeview alignment, uncheck the “Sync scroll” checkbox.

- By default, the Production Task treeview shows correlated and uncorrelated frames. To show only correlated frames, check the “Hide unmatched” checkbox.

You can run the following operations in this window:

- Reset the current correlation—Click Reset. This uncorrelates all production frames.
- Correlate all frames automatically—Click Correlate. (The other correlation options are described in Configure Tier Pairs Dialog Box.)
- Mark a production frame for extraction—Right-click on a frame in the Production Task treeview and choose “Mark for Extraction”. A marked frame will be extracted unconditionally, regardless of whether it correlates to a reference frame.
- Correlate two frames manually—See Procedure 9-5
- Uncorrelate a production frame—Right-click on the frame in the Production Task treeview, choose “Undo Correlation” and then click “Update”.

Procedure 9-5 Correlating Two Frames Manually

1 To view uncorrelated production frames, uncheck the “Hide unmatched” checkbox.

2 To scroll the two treeviews independently, check the “Sync scroll” checkbox.

3 Select the frame that you want to correlate in either treeview.

4 To find similar frames in the other task:

4.1 Right-click on the selected frame and choose “Find Similar in Production” or “Find Similar in Reference”.

➥ The Similar Frames window appears and shows all similar frames (based on the “Similarity Threshold” setting).

4.2 Note the number of the frame that you want to correlate. Generally, you want to correlate the frame with the highest similarity score.

4.3 Click Close to return to the Tier Pair Correlation Assistant.

5 In the opposite treeview, scroll to and select the frame that you want to correlate.

6 Right-click on either frame and choose “Correlate with Selected Production/Reference Frame.”

➥ The two frames are correlated. The status fields in the Correlation box reflect the new correlation status.

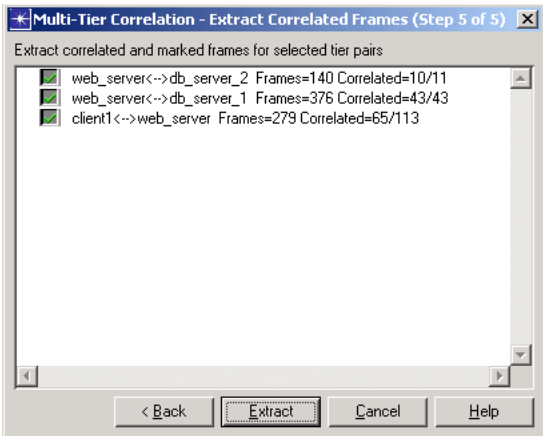
7 Click the Update field to verify that the treeviews reflect the current correlation.

End of Procedure 9-5

Extract Correlated Traffic Dialog Box

The Extract Correlated Frames dialog box shows all tier pairs that you marked for correlation in the Configure Tier Pairs Dialog Box.

Figure 9-13 Extract Correlated Frames Dialog Box



Each line shows

- tier names
- total number of production frames for the tier pier
- number of correlated frames and total number of reference frames. Thus “Correlated=64/113” indicates a total of 113 reference frames for that tier pair, of which 64 are correlated with frames in the production task.

If a tier pair includes correlated frames, the corresponding checkbox is checked. To include all traffic on a tier pair in the extracted production task, uncheck the checkbox.

When ready to extract the frames, click Extract. AppTransaction Xpert then creates an extracted production task that includes only frames that correlate to the reference task (all uncorrelated frames are excluded).

Related Topics

- *Multi-Tier Correlation using String Filtering*

Multi-Tier Correlation Temporal Filtering (Experimental)

The temporal filtering method for performing multi-tier correlation uses the timing of messages to perform correlation across tier pairs. This workflow helps isolate an individual transaction in a packet trace captured in a production environment.

At a high level, the recommended workflow is:

1) Filter out traffic from the client tier to the first server tier that is not part of the transaction of interest.

2) Run one of the three temporal correlation workflows to isolate the transaction of interest on the back-end tiers.

There are three variations of the temporal correlation—a Basic Method and two Advanced Methods (“Build Up” and “Filter Out”). All three approaches revolve around a system of scoring messages based on how well they line up with the traffic in the preceding tier pairs. You start by scoring the messages. After you review the message scoring, you can tweak parameters and re-score the messages, or you can filter out messages that are below a threshold of your choice.

The basic approach scores all back-end messages across all back-end tier pairs with a single operation. This approach is designed to be relatively conservative by default, so accepting defaults will remove messages that are clearly unrelated to the front-end transaction of interest, but it may not filter out all unrelated messages.

The two other approaches (build up and filter out) are designed to be iterative. For each iteration, start by defining a *working set* of messages that you want to analyze and then operate on that working set. Typically, a working set is two tier pairs that have a tier in common (i.e., two adjacent tier pairs). To define the working set, use the user interface to exclude all messages except for those that you want in the working set. Then, use the scoring tools to help decide which messages within the working set are part of the transaction. In the build up approach, all messages start as excluded, so you need to *mark* the packets that you want to include. In the filter out approach, all messages start as included, so you filter out packets that you determine are not part of the transaction.

The following table lists the properties used to calculate packet scoring.

Figure 9-14 Packet Scoring used for Temporal Filtering

Property	Specifies…
Guard Proportion (0-1.0) (Default: 0.05)	Whether regularly timed packet connections occur after the initial request. Scoring is higher when the packet connects occur regularly timed after the initial request.
Alignment Bonus (0-2.0) (Default: 0.1)	Whether the packet connections are within the duration of the activity. Scoring is higher when the packet connections occur during the activity.
Early Start Penalty Multiplier (Default: 1.0)	Whether the packet connections occur before the duration of the activity. Scoring is lower when the packet connections occur before the activity.
Late End Penalty Multiplier (Default: 0.5)	Whether packet connections occur after the duration of the activity. Scoring is higher when the packet connections occur after the activity.

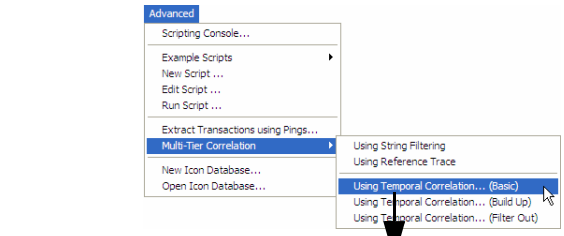
All three options of temporal filtering enable you to adjust the settings used to calculate packet scoring.

Note—The multi-tier correlation temporal filtering feature is included as an experimental feature in AppTransaction Xpert. During this phase, customers can use this feature “as-is” while it is decided whether to include this or similar functionality in future releases. If you encounter any issues while using this feature, contact Technical Support. However, because the feature is experimental, solutions may not be provided for all reported problems.

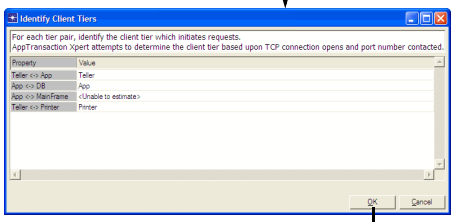
Basic Method

Use this method to apply the same scoring parameters to all packets in a multi-tier packet trace file.

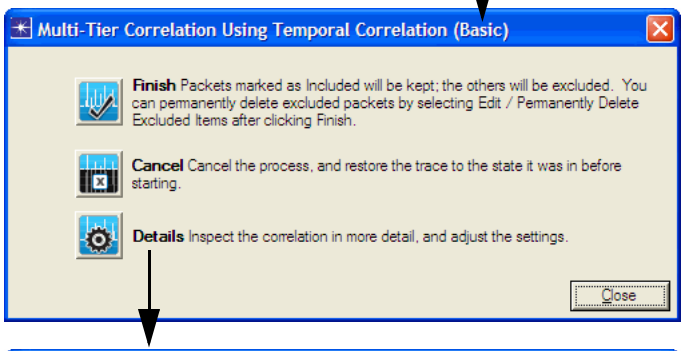
Figure 9-15 Multi-Tier Temporal Filtering: Basic



Choose Advanced > Multi-Tier Correlation > Using Temporal Correlation… (Basic)



For each tier-pair, identify the client tier.
(The client tier is the tier that initiates requests.)



Select an option:
- Finish
- Cancel
- Details

Select an option:
- Set Cutoff
- Show Scoring
- Show inclusions and Exclusions
- Show Average Scores Per Connection
- Show Selected Packets Score
- Recalculate Packet Scores
- Finish
- Cancel

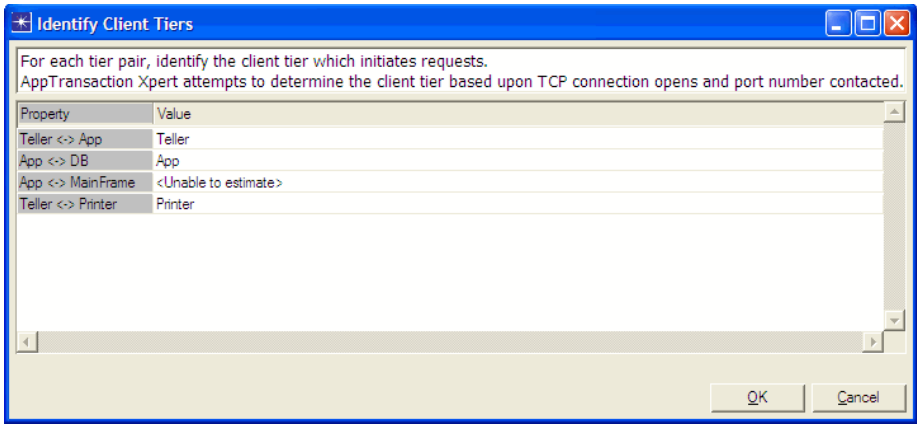
Procedure 9-6 Temporal Filtering: Basic

1 Open the Transaction Analyzer model with multiple tiers.

2 Click the “Data Exchange Chart” tab.

3 Choose Advanced > Multi-Tier Correlation > Using Temporal Correlation… (Basic).

4 The “Identify Client Tiers” dialog box appears, which lists each tier pair.



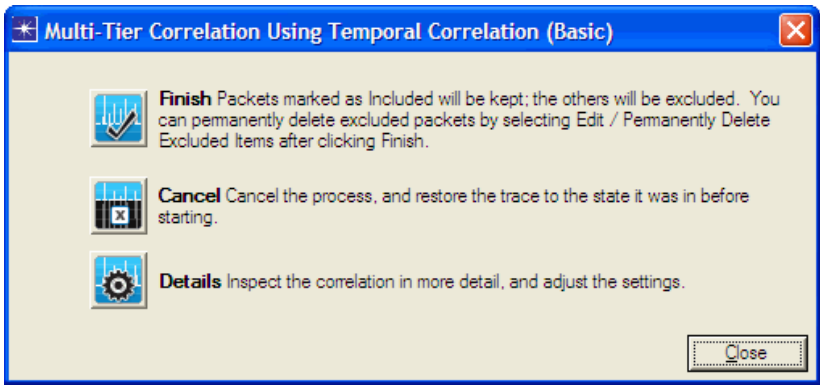
5 For each tier pair, identify the client tier. (The client tier is the tier that initiates requests.)

To define the client tier, click the value column for each tier pair and choose the client from the pull-down list.

6 Click OK.

➥ The Data Exchange Chart refreshes and the color-coding shows the packets that are included (in green) and excluded (in grey).

➥ The “Multi-Tier Correlation Using Temporal Correlation (Basic)” dialog box appears.



7 Click one of the following options:

- Finish—Choose this option to save the changes and to exclude the packets not marked as included.

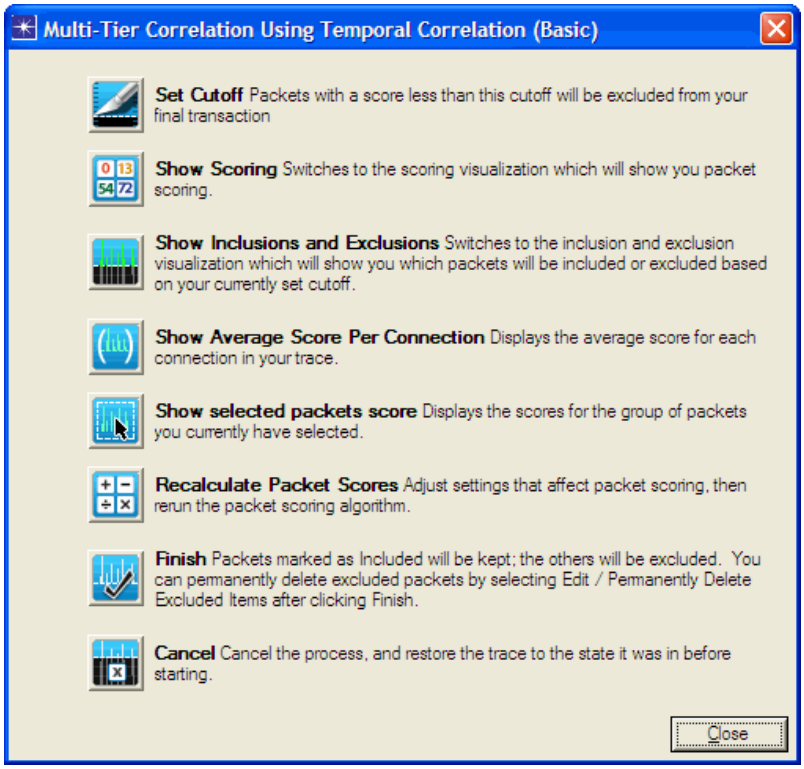
  ➥ The Data Exchange Chart refreshes and shows the updated payload size information for the included packets.

- Cancel—Choose this option to cancel the changes.

  ➥ The Data Exchange Chart refreshes and shows all packets that were included before performing the basic temporal filtering operation.

- Details—Choose this option to perform additional filtering based on scores.

  ➥ The "Multi-Tier Correlation Using Temporal Correlation (Basic)" dialog box appears.



8 Choose one of the following scoring options:

- Set Cutoff—Defines a minimum score for packets to be included in the transaction. After entering a value and pressing OK, the Data Exchange Chart is updated to reflect any changes. The default is "10.0".

- Show Scoring—Toggles the color coding of the Data Exchange Chart to show scoring.

- Show Inclusions and Exclusions—Toggles the color coding of the Data Exchange Chart to show the packets which will be included or excluded, based on the currently set cutoff score.

- Show Average Scores Per Connection—Displays the average scores for all the connections in the packet trace. Optionally, you can export the data.

- Show Selected Packets Score—Displays the scores for the currently selected packets.
- Recalculate Packet Scores—Adjusts the settings that affect packet scoring and recalculates the packet scores.
- Finish—Applies the filter and excludes any packets with a score below the set cutoff.
- Cancel—Cancels the temporal filtering process and restores the trace to its original state.

9 When complete, save the updated model under a different name (File > Save As…) so you still have the original model.

End of Procedure 9-6

Advanced Methods

Use this method to examine individual sets of packets (called *working sets*) in a multi-tier packet trace and to optionally apply different scoring parameters to the individual sets.

Creating and examining working sets is an iterative process. First you create a working set. Then you can examine the packets in the working set. Then you can create another working set and examine it. Or you can reload the previous working set to examine it some more.

After examining all packets in working sets, the final step is to click Finish, which excludes any packets that are not included in at least one working set.

The advanced method includes two options. Select the option that works best for you and the packet trace file.

- **Build Up—**Allows you to include packets that are above a score threshold.

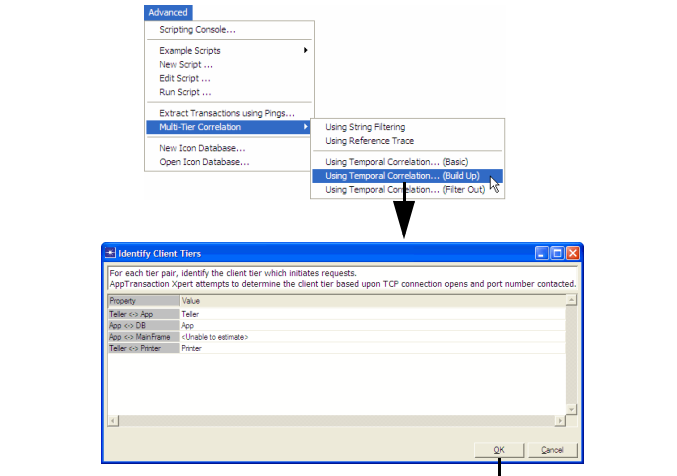
  For an overview, see Figure 9-16 Multi-Tier Temporal Filtering: Build Up.

- **Filter Out—**Allows you to exclude packets that are below a score threshold.

  For an overview, see Figure 9-17 Multi-Tier Temporal Filtering: Filter Out.

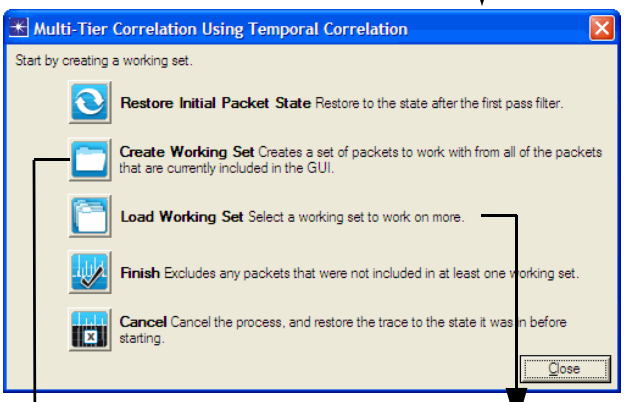
For step-by-step instructions, see Procedure 9-7 Temporal Filtering: Build Up / Filter Out.

Figure 9-16 Multi-Tier Temporal Filtering: Build Up

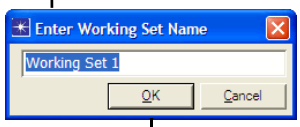


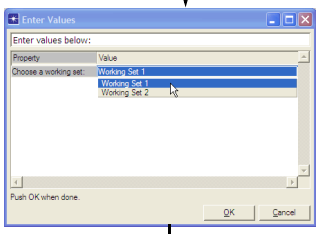
Choose Advanced > Multi-Tier Correlation > Using Temporal Correlation… (Build Up)

For each tier pair, identify the client tier.
(The client tier is the tier that initiates requests.)

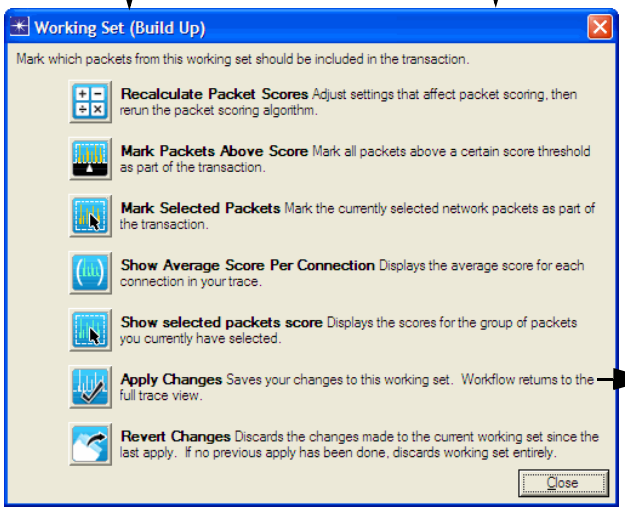


Select an option:
- Restore Initial Packet State
- Create Working Set
- Load Working Set
- Finish
- Cancel





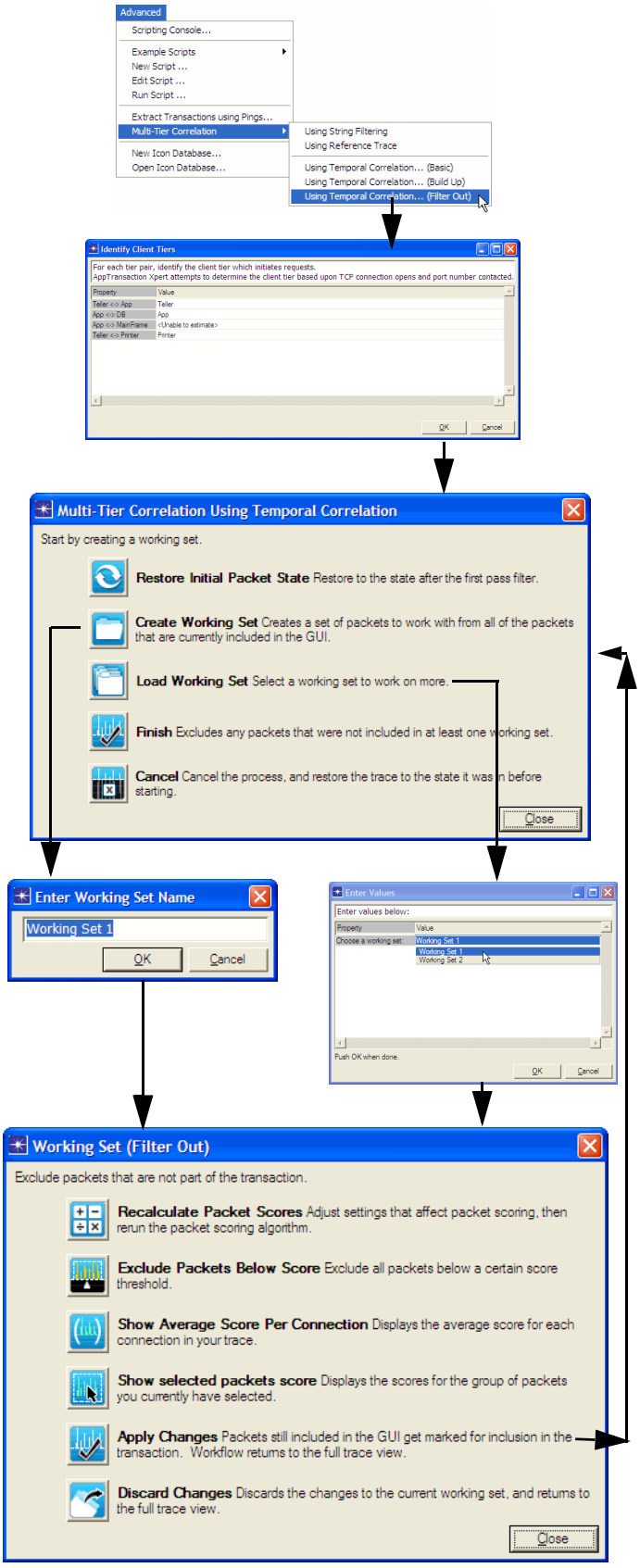
Create or load a working set.



Select an option:
- Recalculate Packet Scores
- Include Packets Above Score
- Include Selected Packets
- Show Average Score Per Connection
- Show Selected Packets Score
- Apply Changes
- Revert Changes

(Yellow highlight indicates items specific to the Build Up option. Compare with the Filter Out option.)

Figure 9-17 Multi-Tier Temporal Filtering: Filter Out



Choose Advanced > Multi-Tier Correlation > Using Temporal Correlation… (Filter Out)

For each tier pair, identify the client tier. (The client tier is the tier that initiates requests.)

Select an option:
- Restore Initial Packet State
- Create Working Set
- Load Working Set
- Finish
- Cancel

Create or load a working set.

Select an Advanced option:
- Recalculate Packet Scores
- Exclude Packets Below Score
- Show Average Score Per Connection
- Show Selected Packets Score
- Apply Changes
- Revert Changes

(Yellow highlight indicates item specific to the Filter Out option. Compare with the Build Up option.)

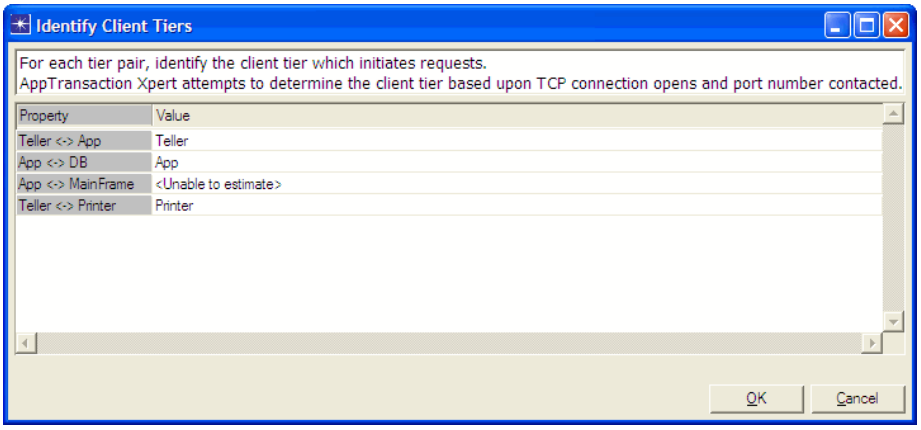
Procedure 9-7 Temporal Filtering: Build Up / Filter Out

1 Open the Transaction Analyzer model with multiple tiers.

2 Click the “Data Exchange Chart” tab.

3 Choose Advanced > Multi-Tier Correlation and select one of the options:
- Using Temporal Correlation… (Build Up)
- Using Temporal Correlation… (Filter Out)

➥ The “Identify Client Tiers” dialog box appears, which lists each tier pair.



4 For each tier pair, identify the client tier. (The client tier is the tier that initiates requests.)

To define the client tier, click the value column for each tier pair and choose the client from the pull-down list.

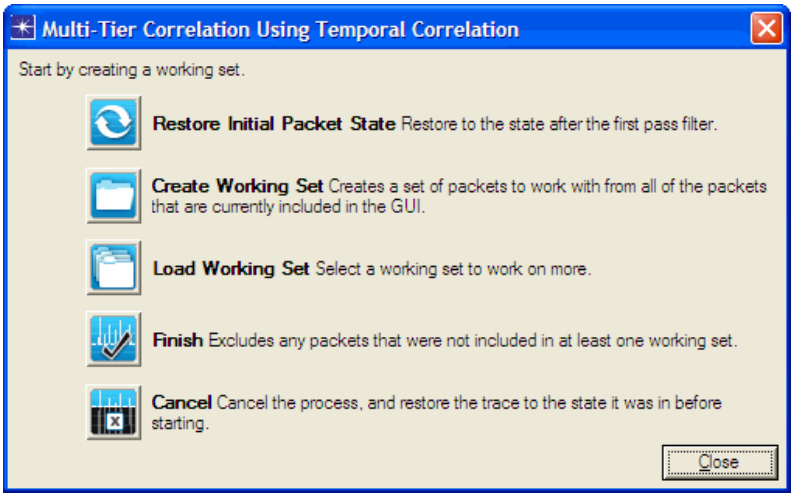
5 Click OK.

➥ The First Pass dialog box appears and informs you of the number of packets that have been excluded.

6 Click OK.

➥ The Data Exchange Chart refreshes and the color-coding shows the packets that are included (in green) and excluded (in grey).

➥ The "Multi-Tier Correlation Using Temporal Correlation" dialog box appears.



7 Click one of the following options:

- Restore Initial Packet State—Restores to the state after the first pass filter.
- Create Working Set—Creates a working set from the currently selected packets. For more information, see Working with Working Sets.
- Load Working Set—Loads a previously defined working set for further investigation. For more information, see Working with Working Sets.
- Finish—Excludes any packets that are not included in at least one working set.
- Cancel—Cancels the temporal filtering, and restores the trace to the state it was in before starting.

8 When complete, save the updated model under a different name (File > Save As…) so you still have the original model.

End of Procedure 9-7

Working with Working Sets

Use the *working set* feature to isolate a set of packets for in-depth examination of those packets. It is best to group related packets into a single working set and to create as many working sets as necessary to thoroughly examine the packets.

After examining packets in working sets, select the Finish button to exclude any packets that were not included in at least one working set.

The following procedure describes the general workflow for working set usage.

Procedure 9-8 Workflow: Working with Working Sets

1 Create a Working Set

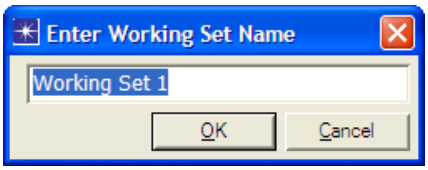
1.1 Select the Packets to Examine:
In the Data Exchange Chart, isolate the packets that you want to examine more closely. Typically, you want to examine packets that have not yet been reviewed (in grey).

To isolate packets for the working set, select packets and use one of the following right-click options:
- Exclude Selected Items
- Exclude Others

If necessary, repeat until only the packets you want to examine are displayed in the Data Exchange Chart.

1.2 From the "Multi-Tier Correlation Using Temporal Correlation" dialog box, click "Create Working Set"

➥ The Enter Working Set Name dialog box appears.



1.3 Enter the name of the working set and click OK.

➥ The Data Exchange Chart refreshes and displays the packets selected for the working set. The packets are color-coded based on the multi-tier correlation score.

➥ The Working Set dialog box appears with options that can be performed on the work set.

2 Examine the Working Set

2.1 Select one of the following options from the Working Set dialog box:

(Notice that options specific to Build Up or Filter Out are noted with the description of the options.)

- **Recalculate Packet Scores—**Adjusts the settings that affect packet scoring and reruns the packet scoring algorithm.
- **Include Packets Above Score—**Marks all packets above a certain threshold as included in the transaction. *(Build Up option only.)*
- **Include Selected Packets—**Includes the currently selected packets in the transaction. *(Build Up option only.)*
- **Exclude Packets Below Score—**Excludes all packets below a certain score threshold. *(Filter Out option only.)*
- **Show Average Score Per Connection—**Displays the average scores for all the connections in the trace.

- **Show Selected Packets Score—**Displays the scores for the selected packets.
- **Apply Changes—**Saves the inclusion choices for this working set and returns the full trace view.
- **Revert Changes—**Discards the changes made to the current working set since the last apply. If no previous apply has been done, discards all working sets entirely.

3 Repeat as Necessary

Repeat Step 1 (Create a Working Set) or load an existing working set and then repeat Step 2 (Examine the Working Set) as needed until all packets have been examined and excluded/included as required.

End of Procedure 9-8