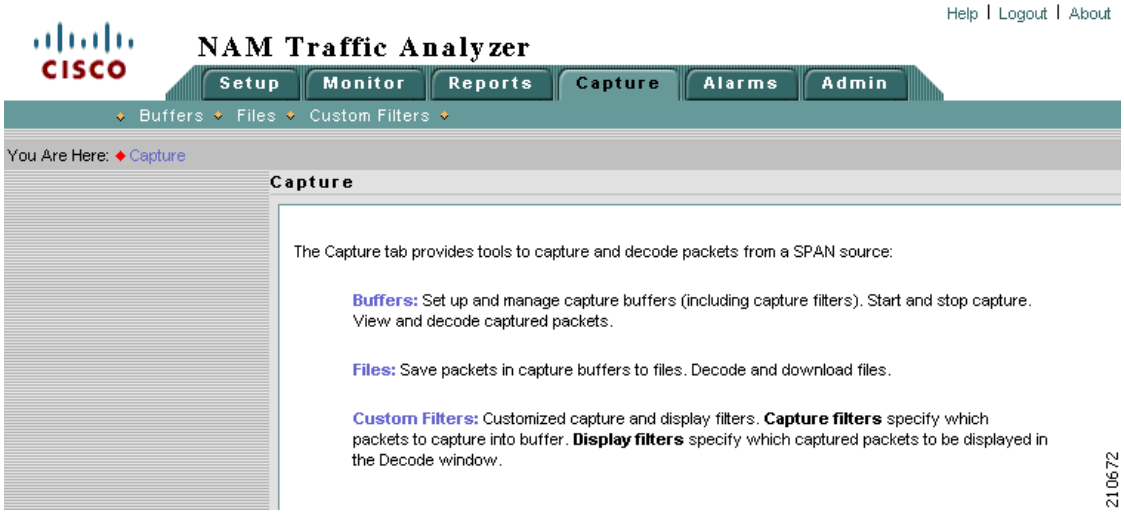
CHAPTER 6

# Capturing and Decoding Packet Data

The Capture tab allows you to set up multiple buffers for capturing, filtering, and decoding packet data, manage the data in a file control system, and display the contents of the packets.

The Capture Tab (Figure 6-1) shows the options available for capturing and decoding packet data.

***Figure 6-1 Capture Tab***




From the Capture tab, you can select three options:

- Buffers, page 6-2

  Use the Buffers option to access the basic operations for capturing, viewing and decoding packet data on the NAM.

- Files, page 6-14

  Use the Files option to save, decode, or download files.

- Custom Capture Filters, page 6-19

  Use the Custom Filters option to create customized capture and display filters.

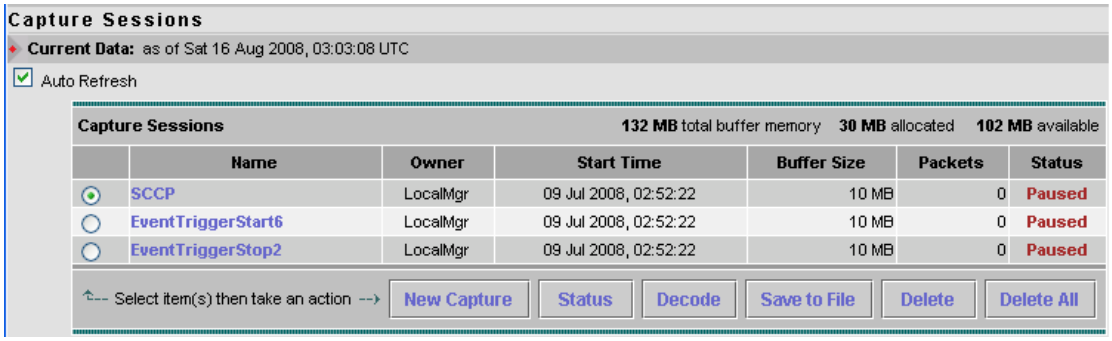
**Note** NAM 4.0 supports IPv6 for all capture functionality.

# Buffers

The Capture Buffers (Figure 6-2) window shows the list of capture buffers. You can configure multiple capture buffers and multiple automatic capture buffers.

**Note** If you check the Auto Refresh check box, the Capture Buffers window refreshes automatically every 60 seconds.

***Figure 6-2 Capture Buffers***




Capture Buffer Fields, Table 6-1, describes the Capture Buffers fields.

***Table 6-1 Capture Buffer Fields***

| Operation | Description |
|---|---|
| Name | Name of the capture buffer |
| Owner | Owner of the buffer |
| Start Time | Time capture starts |
| Buffer Size | Size of the buffer<br>**Note** *Capture to files* indicates the capture is being stored in one or more files and is a clickable link to those files. |
| Packets | Number of packets |
| Status | The current status of the capture:<br>• Running—Packet capture is in progress<br>• Paused—Packet capture is paused. Captured packets remain in buffer, but no new packets are captured<br>• Cleared—Capture is stopped (by user) and capture buffer is cleared<br>• Locked—Capture is locked (stopped) because the buffer is full |

Capture Buffer Operations (Table 6-2) describes the operations that you can perform from the Capture Buffers window.

*Table 6-2 Capture Buffer Operations*

| Operation | Description |
|---|---|
| New Capture | Click to create a new capture buffer. See Configuring Capture Settings. |
| Status | Click to display status and settings of selected capture. |
| Decode | Click to view decoded packets. See Viewing Packet Decode Information. |
| Save to File | Click to save a buffer to a file on the NAM hard disk. See Files. |
| Delete | Click to delete a buffer. |
| Delete All | Click to delete all buffers. |

# Configuring Capture Settings

The Capture Settings window enables you to configure the settings for a new capture and control the capture process. You can also configure capture filters to narrow down the packets to be captured.

To configure a new capture buffer:

**Step 1** Go to the **Capture** > **Buffers** window.

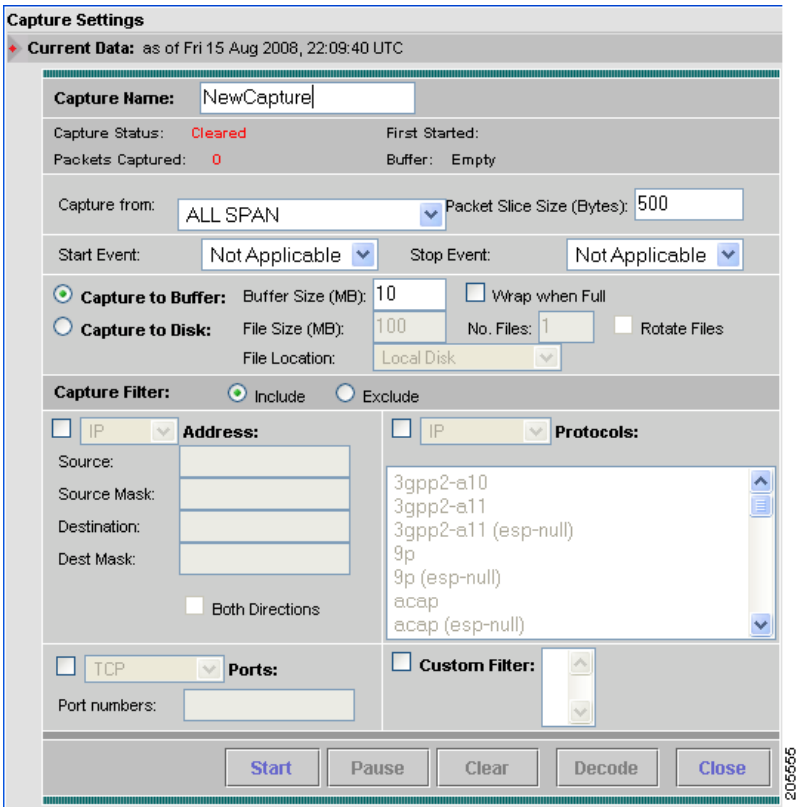
**Step 2** Choose **New Capture** to set up a new capture, or choose an existing buffer and click **Status** to modify, pause, clear, or restart capture settings.

The NAM Traffic Analyzer displays the Capture Settings (Figure 6-3) window. The Capture Settings window provides a field for you to enter a name for the capture and four status indicators described in Table 6-3.

*Table 6-3 Capture Settings Status Indicators*

| Status Indicator | Description |
|---|---|
| Capture Status | The current status of the capture:<br>• Running—Packet capture is in progress.<br>• Paused—Packet capture is paused. Captured packets remain in buffer, but no new packets are captured.<br>• Cleared—Capture is stopped (by user) and capture buffer is cleared.<br>• Locked—Capture is locked because the buffer is full. |
| Packets Captured | The number of packets captured and stored in the capture buffer.<br>**Note** When the capture buffer is full and capture is in wrap-when-full mode, the number of packets captured may fluctuate as new packets arrive and old packets are discarded from the buffer. |
| First Started | Shows when the current capture started. You can pause and restart the capture as many times as necessary. If you stop the capture and start a new capture, this field shows the start time of the *new* capture. |
| Buffer | Current buffer or file state—Empty, Space Available, Full (Wrap), or Full (Locked). |

*Figure 6-3 Capture Settings*




**Step 3** Enter information in the Capture Settings Fields (Table 6-4) as appropriate.

*Table 6-4 Capture Settings Fields*

| Field | Description | Usage Notes |
|---|---|---|
| Capture Name | Name of the capture | Enter a capture name. |
| Capture from | Data source from which to capture packets | Choose an entry from the list. |
| Start Event | Alarm event that starts the capture | You can configure Alarm Events from the **Setup > Alarms > Alarm Event** window. When an alarm event theshold is crossed, the alarm event starts or stops the capture session.<br>**Note** When a capture is configured to start with a Start Event, the capture session waits in the *Paused* state until the Start Event occurs. |
| Stop Event | Alarm event that stops the capture | |
| Packet Slice Size | The slice size in bytes; used to limit the size of the captured packets. | Enter a value of 64 or higher. Enter zero (0) to not perform slicing.<br>If you have a small buffer but want to capture as many packets as possible, use a small slice size.<br>If the packet size is larger than the specified slice size, the packet is *sliced* before it is saved in the capture buffer. For example, if the packet is 1000 bytes and slice size is 200 bytes, only the first 200 bytes of the packet is stored in the capture buffer. |

*Table 6-4 Capture Settings Fields (continued)*

| Field | Description | Usage Notes |
|---|---|---|
| Capture to Buffer | Check to store captures in buffers | Enter values for **Buffer Size** and **Wrap when Full**. |
| Buffer Size | Size of the capture buffer in MB. | Enter a number from 1 up to your platform maximum. If system memory is low, the actual buffer size allocated might be less than the number specified here. After starting the capture, this field shows the actual buffer size allocated. NAM devices have the following buffer sizes:<br>NAM-1-250S — 200 MB<br>NAM-1 — 125 MB<br>with memory upgrade (MEM-C6KNAM-2GB) — 200 MB<br>NAM-2-250S — 500 MB<br>NAM-2 — 300 MB<br>with memory upgrade (MEM-C6KNAM-2GB) — 500 MB<br>NAM 2220 — 10 GB<br>NAM 2204 — 2 GB<br>NME-NAM-80S — 132 MB<br>NME-NAM-120S — 300 MB<br>NM-NAM — 70 MB |
| Wrap when Full | Check to wrap data in buffer when it exceeds buffer size | Check **Wrap when Full** to enable continuous capture.<br>**Note** When the buffer is full, older packet data is removed to make room for new incoming packets. |
| Capture to Disk | Check to store captures in files | Enter values for **File Size** and **No. Files**.<br>**Note** About 400MB of free disk space is reserved for working files. If available disk space is below 400MB, you will not be able to start new capture-to-disk sessions. |
| File Size (MB) | Maximum size of each capture file | File size can be from 1 to 2 GB or up to 10 GB for the NAM appliances. |
| File Location | Choose an option from the pull-down menu. | Local disk is the default, or choose a previously configured remote storage location. You can add (NFS and iSCSI) remote storage locations by clicking **Admin > System** and choosing Capture Data Storage from the Content menu. |
| No. Files | Number of files to use for continuous capture | Number of files can be from 1 to 200. |
| Rotate Files | Check to rotate files in continuous capture | Available only for remote storage or NAM 2200 Series appliances<br>See section Capture Data Storage, page 2-17, for information about configuring remote storage. |
| **Capture Filter**: Include | | Include filters capture only packets that match the filter conditions (recommended) |
| **Capture Filter:** Exclude | | Exclude filters capture packets that *exclude* the filter conditions (recommended) |

**Step 4** If capturing to buffers, check **Capture to Buffer**, enter MB size in **Buffer Size**, and check **Wrap when Full** if you want to continuously capture most recent data.

This type of capture stores packet data up to the size you set in Buffer Size. If you do not check **Wrap when Full**, capture will end when amount of data reaches size of buffer.

**Step 5** If capturing to files, check **Capture to File(s)**, and enter values in **File Size** and **No. Files**.

When capturing to multiple files, a suffix is added to the file name. For example, the first file for a capture named **CaptureA** would be labeled as **CaptureA_1** the second **CaptureA_2**, and so on.

**Step 6** If capturing to files, check **Rotate Files** to continuously capture the most recent packet data.

The Rotate Files option can only be used with remote storage or the NAM 2200 Series appliance's local disk. See the section Capture Data Storage, page 2-17, for information about configuring remote storage.

**Note** If you choose the **Rotate Files** option, when you reach the highest number file, the earliest file is overwritten. For example, if you specify **No. Files** to 10, file **CaptureA_1** is overwritten after the NAM writes capture data to file **CaptureA_10**. To determine the most recent capture, check each file's timestamp.

**Step 7** In the Capture Filter pane, check Include or Exclude.

Include filters capture only packets that match the filter conditions. Exclude captures packets that *exclude* the filter conditions.

**Step 8** Choose one of the following check boxes to enable the applicable filter types:

- **Address** to filter traffic based on a type of IP, IPIP4, IPv6, GRE.IP, or MAC address. (See the "Capturing Using an Address Filter" section on page 6-7.)
- **Protocols** to filter traffic based on specific protocols. (See the "Capturing Using a Protocol Filter" section on page 6-9.)
- **Ports** to use a port filter. (see the "Capturing Using a Port Filter" section on page 6-9.)
- **Custom Filter** to use a customized filter. (See the "Capturing Using a Custom Filter" section on page 6-9.)

  For more information on creating and editing a custom capture filter, see the "Custom Capture Filters" section on page 6-19.

**Step 9** Choose one of the operations listed in Table 6-5, Capture Settings Operations.

*Table 6-5 Capture Settings Operations*

| Operation | Description |
|---|---|
| **Start** | Click to start a capture operation. |
| **Pause** | Click to pause a capture operation. Capture data remains in the capture buffer, but no new data is stored. Click Start to resume the capture. |
| **Clear** | Click to stop a capture and clear the capture buffer. You must clear the capture buffer before you change capture settings. |
| **Decode** | Click to display the capture buffer. (This could take a few minutes.)<br>**Note** Capture sessions appear in the *Paused* state when decoding a buffer. |
| **Close** | Click to close the capture window. |

For example, to capture only HTTP and HTTPS packets in the 111.122 Class B network, do the following:

**Step 1** Click the **Inclusive** check box.

**Step 2** Click the **Address** check box.

**Step 3** Click the IP button.

**Step 4** Choose the **Both Directions** check box.

**Step 5** In the Source, enter `111.122.0.0`.

**Step 6** In the Source Mask, enter `255.255.0.0`.

**Step 7** Click the **Protocol** check box.

**Step 8** Press **Shift-Click** to select HTTP and HTTPS from the list.

# Capturing Using an Address Filter

If you selected the **Address** check box, enter information in the Capture Settings Address Filter Dialog Box, Table 6-6, as appropriate.

**Note** When filtering on tunnel addresses such as IPIP4 or GRE.IP, the filters will match the addresses on the inner and outer IP header.

*Table 6-6 Capture Settings Address Filter Dialog Box*

| Field | Description | Usage Notes |
|---|---|---|
| Address | Indicated what address to filter by. | • Choose MAC to use the source/ destination MAC address of the packets.<br>• Choose IP to use the source/destination IP addresses of the packets.<br>• Choose IPIP4 for IP addresses including those tunneled over IP protocol 4.<br>• Choose GRE.IP for IP addresses including those tunneled over GRE.<br>• Choose IPv6 for addresses using IP version 6. |
| Both directions. | Indicates whether the filter is applied to traffic in both directions. | If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A.<br>If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A. |
| Source | Source address of the packets. | • For IP, IPIP4, and GRE.IP address, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255.<br>• For IPv6 address, enter a valid IPv6 address in any allowed IPv6 address format. For example:<br>– 1080::8:800:200C:417A<br>– ::FFF:129.144.52.38<br>**Note** See RFC 2373 for valid text representations.<br>• For MAC address, enter *hh hh hh hh hh hh*, where *hh* is a hexadecimal number from 0 to 9 or a to f. |
| Source Mask | The mask applied to the source address.<br>• If a bit in the Source Mask is set to 1, the corresponding bit in the address is relevant.<br>• If a bit in the Source Mask is set to 0, the corresponding bit in the address is ignored. | • For IP, IPIP4, and GRE.IP address, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255.<br>• For IPv6 address, enter a valid IPv6 address in any allowed IPv6 address format. The default mask (if blank) for IPv6 addresses is ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff<br>**Note** See RFC 2373 for valid text representations.<br>For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff. |

*Table 6-6 Capture Settings Address Filter Dialog Box (continued)*

| Field | Description | Usage Notes |
|---|---|---|
| Destination | Destination address of the packets. | • For IP, IPIP4, and GRE.IP address, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255.<br>• For IPv6 address, enter a valid IPv6 address in any allowed IPv6 address format. For example:<br>– 1080::8:800:200C:417A<br>– ::FFF:129.144.52.38<br>**Note** See RFC 2373 for valid text representations.<br>For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff. |
| Dest. Mask | The mask applied to the destination address.<br>• If a bit in the Dest. Mask is set to 1, the corresponding bit in the address is relevant.<br>• If a bit in the Dest. Mask is set to 0, the corresponding bit in the address is ignored. | • For IP, IPIP4, and GRE.IP address, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255.<br>• For IPv6 address, enter a valid IPv6 address in any allowed IPv6 address format. The default mask (if blank) for IPv6 addresses is ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff<br>**Note** See RFC 2373 for valid text representations.<br>For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff. |

# Capturing Using a Protocol Filter

If you selected the **Protocol** check box, select one or more protocols to capture from the drop-down list.

Use Shift + Click to select multiple protocols.

# Capturing Using a Port Filter

From the Capture Settings window, select the Ports check box and enter one or more ports separated by commas.

# Capturing Using a Custom Filter

**Step 1** Click the **Custom** check box.

**Note** The Address Filter and Protocol Filter check boxes are disabled if you select the Custom Filter check box and vice versa.

**Step 2** Choose one or more custom capture filters from the list. Use Shift + click to select multiple filters. If you select multiple custom filters, the filters' conditions will be ORed together (match any).

**Note** If the list is empty, see the "Creating Custom Capture Filters" section on page 6-19 for instructions on creating custom capture filters.

To view or edit the selected custom capture filter, choose **Custom Filters > Capture Filters**.

# Using Alarm-Triggered Captures

You can configure multiple alarm-triggered captures that start and stop automatically by alarm events you define.

To set up an alarm-triggered capture:

**Step 1** Create an alarm event from the **Setup > Alarms > Alarm Events** window.

Configure an Alarm Event for the type of event for which you want to capture data. See Setting Up Alarm Events, page 3-75, for more information.

**Step 2** Set a threshold for the event from the **Setup > Alarms > Alarm Thresholds** window.

Configure the threshold of parameters of interest in the associated Alarm Event. See Setting Alarm Thresholds, page 3-76, for more information.

**Step 3** Set up a capture buffer from the **Capture > Buffers** window. Click **New Capture**.

Choose the Start Event and/or the Stop Event for the associated Alarm Event. See Configuring Capture Settings, page 6-3, for more information.

# Viewing Packet Decode Information

After some packets have been captured in the buffer, you can use the Packet Decoder to view the packet contents.

The Packet Decoder window has four parts:

- Packet Decoder operations
- Packet browser pane
- Protocol decode (See the "Viewing Detailed Protocol Decode Information" section on page 6-14).
- Packet hexadecimal dump.

To view packet decode information:

**Step 1** Choose **Capture > Buffers** or **Capture > Files**.

**Step 2** Choose a capture buffer or file then click **Decode**.

The Packet Decoder window displays as shown in Figure 6-4.

*Figure 6-4 Packet Decoder Window*

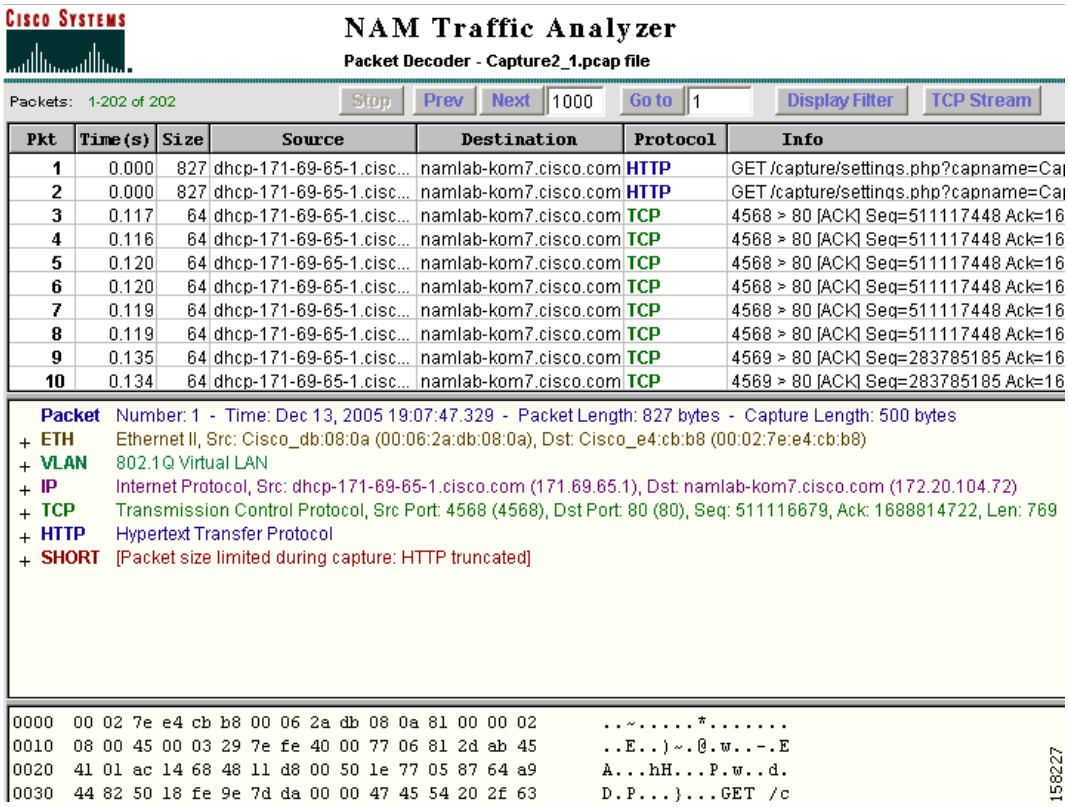



Table 6-7 describes the packet decoder operations.

**Note** If you enable DNS on the **Admin > System > Preferences** window, packet decoding can take a very long time due to DNS name resolution.

*Table 6-7 Packet Decoder Operations*

| Button | Description |
|---|---|
| Stop | Stop packet loading |
| Prev | Load and decode the previous block of packets from the NAM |
| Next | Load and decode the next block of packets from the NAM |
| Go To | Load and decode a block of packets starting from the specified packet number. |
| Display Filter | Launch the Display Filter dialog. See Filtering Packets Displayed in the Packet Decoder, page 6-12. |
| TCP Stream | Follow the TCP stream of the selected TCP packet.<br>**Note** This might take a long time depending on the traffic pattern. |

Table 6-8 describes the information displayed in the packet browser pane.

*Table 6-8 Packet Browser*

| Field | Description |
|---|---|
| Pkt | Packet numbers, listed numerically in capture sequence. If the decode (display) filter is active, the packet numbers might not be consecutive. |
| Time | Time the packet was captured relative to the first packet displayed (not the first packet in the buffer).<br>**Note** To see the absolute time, see the Detail window. |
| Size | Size of the packet, in bytes. |
| Source | Packet source, which might be displayed as hostname, IP, IPX, or MAC address.<br>**Note** To turn hostname resolution on and off for IP addresses, click the Setup tab and change this setting under Preferences. |
| Destination | Packet destination, which might be displayed as hostname, IP, IPX, or MAC address. |
| Protocol | Top-level protocol of the packet. |
| Info | Brief text information about the packet contents. |

## Browsing Packets in the Packet Decoder

You can use the packet browser to browse the list of captured packets and do the following:

- Filter by protocol, IP address, MAC address, and custom display filter.
- Use the **Next**, **Previous**, and **Go To** buttons to load packets from the capture buffer.

**Note** The capture must be paused or stopped for you to use these features.

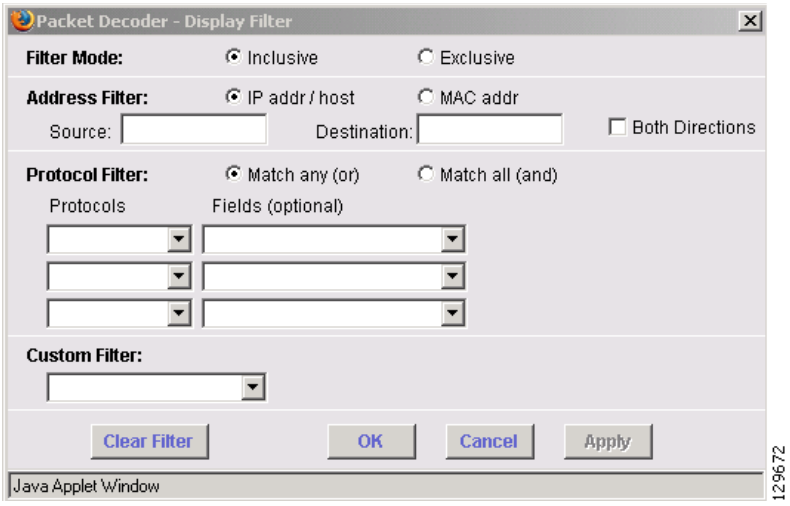
## Filtering Packets Displayed in the Packet Decoder

To filter packets displayed in the packet decoder:

**Step 1** From the Packet Decoder window, click the Display Filter button:

The Packet Decoder - Display Filter Window (Figure 6-5) displays.

*Figure 6-5 Packet Decoder - Display Filter Window*




**Step 2** Do the following:

- Choose a **Filter Mode**:
  - **Inclusive** displays packets that match the condition(s.)
  - **Exclusive** displays packets that do not match the condition(s).
- Choose an **Address Filter**:
  - **IP address** filters on IP address.
  - **MAC Address** filter on MAC address.
  - **Source** allows you to specify the source address, or leave it blank if not applicable.
  - **Destination** allows you to specify the destination address, or leave it blank if not applicable.
  - **Both Directions** allows you to match of packets travelling in both directions.
- Define a **Protocol Filter**.
  - Choose **Match any** to display packets that match any of the protocols or fields

  or
  - Choose **Match all** to display packets that match all of the protocols or fields.
  - Choose a protocol from the **Protocols** list.

**Note** You can type the first few letters of the protocol name to go directly to the protocol. If you make a typo, type **ESC** or **SPACE** to reset.

  - Choose a protocol field from the Fields list, then specify the field value if applicable.
- Choose a **Custom Filter**. See Custom Display Filters for how to set up a custom display filter.

**Step 3** Specify the protocol name, IP address, MAC address, matching text, or custom decode filter.

**Step 4** Click **Filter**.

**Step 5** To display packets that *exclude* the filter conditions, select the **exclusive** check box next to the Filter button.

## Viewing Detailed Protocol Decode Information

To view detailed protocol information:

**Step 1** Highlight the packet number about which you want more information.

Detailed information about that packet is displayed in the Protocol Decode and hexadecimal dump panes at the bottom of the window.

**Note** If you highlight the details in the Protocol Decode pane, the corresponding bytes are highlighted in the hexadecimal dump pane below it.

**Step 2** To review the information, use the scrolling bar in the lower panes.

**Note** When you decode SCCP traffic, the NAM lists the protocol as *skinny*, not SCCP.

**Tip**

- Protocols are color coded both in the Packet Browser and the Protocol Decode pane.
- Click the protocol name in the Protocol Decode pane to collapse and expand protocol information.
- To adjust the size of any of the panes, click and drag the pane frame up or down.

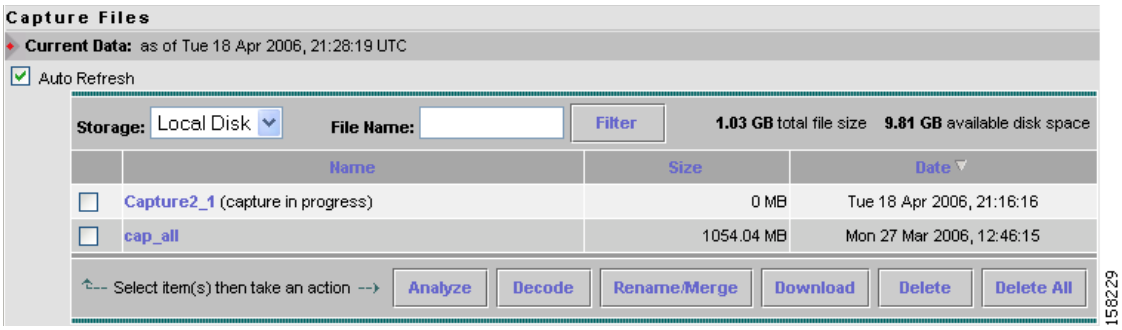
# Files

Use the Files option to analyze, decode, merge, download, or delete saved capture files. See the section Buffers, page 6-2 and Table 6-2 for information about how to save capture buffers to files. You can download files from the Sniffer **.enc** or **.pcap** file formats. See Setting Global Preferences, page 3-87, for information about setting the Sniffer download file format.

Choose **Capture** > **Files** to display the Capture Files window (Figure 6-6).

**Note** If you check the Auto Refresh check box, the Capture Files window refreshes automatically every 60 seconds.

*Figure 6-6 Capture Files Window*




The Capture Files window provides the following options:

- Choose a storage location from the pull-down list to view capture files in that location. Subdirectories of remote storage are listed only if the NAM has full access rights to those remote directories.
- Choose a capture and click **Analyze** to display the packets in a file.
- Choose a capture and click **Decode** to display the packets in a file.
- Click **Convert/Rename/Merge** to merge packets of files. The packets in the file are merged in chronological order.

**Note** Do not add a file suffix when you provide the filename. The suffix **.pcap** is added automatically.

- Click **Download** to download a file to your computer in Sniffer **.enc** or **.pcap** file format.
- Click **Delete** or **Delete All** to delete files.

**Note** Capture files on the NAM 2200 Series appliances are stored in native NAM format. You can convert the capture file format to **.pcap** using the **Convert/Rename/Merge** button on the **Capture > Files** window.

# Analyzing Capture Files

The Analyze button of the Capture Files window enables you to obtain different statistics including traffic rate (bytes/second) over a capture period, lists of hosts, conversations, and applications associated with network traffic. Figure 6-7 shows an example of the Capture Analysis window.

This window also enables you to drill down for a more detailed look at a particular set of network traffic. The pane above the **Traffic over Time** graph displays the time shown in the graph in the **From:** and **To:** fields. It also provides fields for Protocol and Host/subnet, and a **Drill-Down** button.

Each slice in the **Traffic over Time** graph displays the amount of traffic for the amount of time set in the Granularity of the capture file.

You can view more detail about a specific time frame by entering the time in the **From:** and **To:** fields and clicking **Drill-Down**. You can also drill down on a specific **Protocol** or **Host/subnet** address.

*Figure 6-7 Capture Statistical Analysis Window*

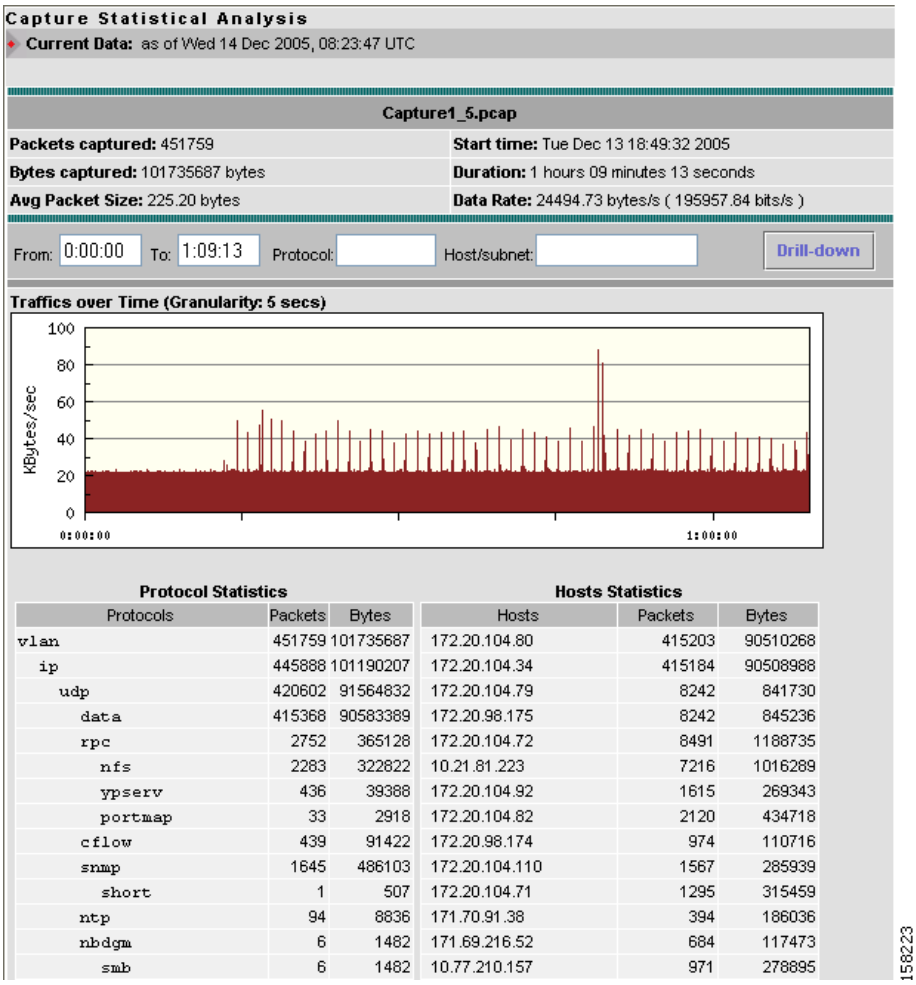



Table 6-9 describes the different areas of the capture analysis window.

*Table 6-9 Capture Analysis Window Fields*

| Field | Description |
|---|---|
| Capture Overview | Provides a summary of the displayed capture including number of packets captured, bytes captured, average packet size, capture start time, duration of capture, and data transfer rate (both bytes and bits per second) |
| Traffic over Time | Displays a graphic image of network traffic (KB/second) |
| Protocol Statistics | Displays packets and bytes transferred for each protocol |
| Hosts Statistics | Displays packets and bytes transferred for each host address |

# Decoding Capture Files

Decoding capture files is described in section Viewing Packet Decode Information, page 6-10.

# Renaming or Merging Capture Files

Use the **Rename/Merge** button to rename a single capture file or merge multiple capture files into one file.

**Note** On NAM 2200 Series appliances, this button is labeled **Convert/Rename/Merge**.

## Renaming Capture Files

To rename a capture file:

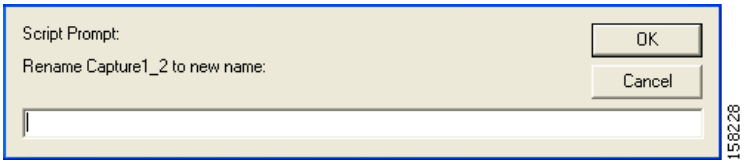
**Step 1** Choose **Capture > Files**.

**Step 2** Choose a capture file from the list of captures.

**Step 3** Click **Convert/Rename/Merge**.

A dialog box displays and asks you to enter the new name for the selected capture file.

***Figure 6-8 Rename Capture File Dialog Box***




**Step 4** Enter a new name for the capture file and click **OK**.

## Merging Capture Files

To merge multiple capture files into one capture file:

**Step 1** Choose **Capture > Files**.

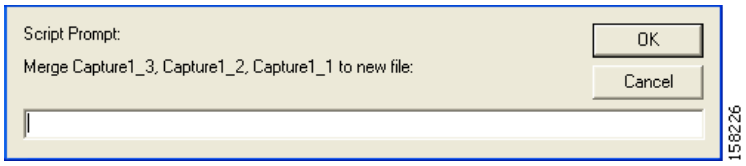
**Step 2** Choose two or more capture files from the list of captures.

**Step 3** Click **Convert/Rename/Merge**.

A dialog box displays and asks you to enter the new name for the merged capture files.

**Note** Merged files cannot exceed 2 GB.

*Figure 6-9 Merging Capture Files Dialog Box*




**Step 4** Enter a name for the merged capture files and click **OK**.

The capture files are merged in timestamp order from oldest to most recent.

# Downloading Capture Files

The following procedure describes how to download a capture file to your computer. You can only download one capture file at a time.

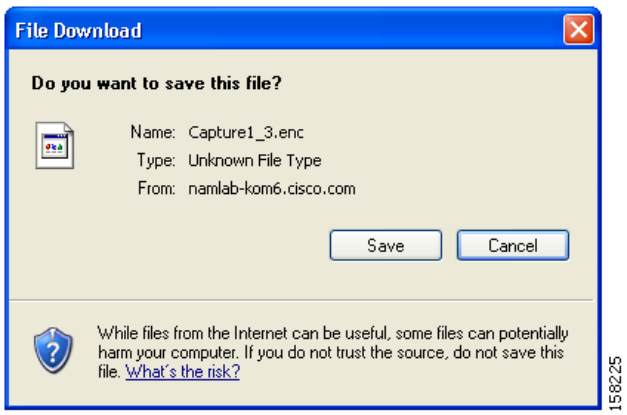
**Step 1** Choose **Capture > Files**.

**Step 2** Choose a capture file from the list of captures.

**Step 3** Click **Download**.

A **File Download** dialog box displays and asks "**Do you want to save this file?**"

*Figure 6-10 Download Capture File Dialog Box*




**Step 4** Click **Save**.

A **Save As** dialog box opens and provides a way for you to rename and save the file at a location of your choice.

# Deleting a Capture File

To delete a capture file:

**Step 1** Choose **Capture > Files**.

**Step 2** Choose a capture file from the list of captures.

**Step 3** Click **Delete**.

A dialog box displays and asks "**Delete the following file(s)?**" and displays the file name.

**Step 4** Click **OK** to delete the file or **Cancel** to allow the file to remain.

## Deleting All Capture Files

To delete all capture files at once:

**Step 1** Choose **Capture > Files**.

**Step 2** Choose a capture file from the list of captures.

**Step 3** Click **Delete All**.

A dialog box displays and asks "**Delete all capture file(s)?**"

**Step 4** Click **OK** to delete all the files or **Cancel** to allow them to remain.

# Custom Capture Filters

You can use custom capture filters to create and save specialized filters to disregard everything except the information you are interested in when you capture data.

For more information about using custom filters when capturing data, see the "Capturing Using a Custom Filter" section on page 6-9.

See these topics for help setting up and managing custom capture filters:

- Creating Custom Capture Filters, page 6-19
- Editing Custom Capture Filters, page 6-22
- Deleting Custom Capture Filters, page 6-22

## Creating Custom Capture Filters

To create a custom capture filter:

**Step 1** Choose **Capture > Custom Filters**.

The Custom Capture Filters dialog box is displayed.

**Step 2** Click **Create**.

The Custom Capture Filter Dialog Box (Table 6-10)displays.

**Step 3** Enter information in each of the fields as appropriate.

*Table 6-10 Custom Capture Filter Dialog Box*

| Field | Description and Usage Notes |
|---|---|
| Filter Name | Enter a name of the new filter. |
| Description | Brief description of the filter.<br>Enter a description from 1 to 35 characters. |
| Protocol | The protocol to match with the packet.<br>Choose the encapsulation from the drop-down list, then select the protocol. |
| Data | The data pattern to be matched with the packet. Use the Offset field to specify the starting location for the data to be checked.<br>Enter `hh hh hh ...`, where `hh` represents hexadecimal numbers from 0 to 9 or a to f.<br>For example, to designate the decimal value *15*, use the hexadecimal value *0f*. For the decimal value *255*, use the hexadecimal value *ff*. For the decimal value *16*, use the hexadecimal value *10*. See Tips for Creating Custom Capture Filter Expressions, page 6-21, for more examples.<br>Leave blank if not applicable.<br>If the packet is too short and does not have enough data to match, the packet match fails. |
| Data Mask | The mask applied to the data matching.<br>Enter `hh hh hh ...`, where `hh` represents hexadecimal numbers from 0 to 9 or a to f.<br>Leave blank if all data bits are relevant.<br>If a bit in the Data Mask is set to 1, the corresponding bit in the packet is relevant in the matching algorithm.<br>If a bit in the Data Mask is set to 0, the corresponding bit in the packet is ignored.<br>If you do not specify the Data Mask, or if it is shorter than the Data field, the Data Mask is padded with "1" bits up to the length of the Data field. For example, if you enter a four-byte value in the Data field and leave the Data Mask field blank, that is the same as specifying a Data Mask of *ff ff ff ff*. |
| Data Not Mask | The mask applied to reverse data matching.<br>Enter `hh hh hh ...`, where `hh` represents hexadecimal numbers from 0 to 9 or a to f.<br>Leave blank for no reverse data matching.<br>For those bits in the Data Not Mask that are set to 0 (or not specified), the relevant bits in the packet must match the corresponding bit in the Data field.<br>For those bits in the Data Not Mask that are set to 1, at least one relevant bit in the packet must be different than the corresponding bit in the Data field.<br>If you do not specify the Data Not Mask, or if it is shorter than the Data field, the Data Not Mask is padded with "0" bits up to the length of the Data field. |
| Offset | Enter a decimal number, the offset (in bytes, from the Base) where packet data-matching begins.<br>This offset applies to the Data, Data Mask, and Data Not Mask fields. |

*Table 6-10 Custom Capture Filter Dialog Box (continued)*

| Field | Description and Usage Notes |
|---|---|
| Base | Choose absolute or a protocol, the base from which the offset is calculated.<br>If you select absolute, the offset is calculated from the absolute beginning of the packet (the beginning of the Ethernet frame). You must account for an 802.1q header when calculating an offset for NAM-1 and NAM-2 devices.<br>If you select protocol, the offset is calculated from the beginning of the protocol portion of the packet. If the packet does not contain the protocol, the packet fails this match. |
| Status | The status to match with the packet.<br>Enter a number from 0 to 65535; leave blank if not applicable.<br>For Ethernet packet captures, the status bits are:<br>Bit 0—Packet is longer than 1518 octets.<br>Bit 1—Packet is shorter than 64 octets.<br>Bit 2—CRC or alignment error.<br>For example, an Ethernet fragment has a status value of 6 (bits 1 and 2 set). |
| Status Mask | The mask applied to the status matching. Enter a number from 0 to 65535; leave blank if all status bits are relevant.<br>If a Status Mask bit is set to 1, the corresponding bit in the packet status is relevant in the matching algorithm.<br>If a Status Mask bit is set to 0, the corresponding bit in the packet status is ignored.<br>If you do not specify a Status Mask, or if it is shorter than the Status field, the Status Mask is padded with "1" bits up to the length of the Status field. |
| Status Not Mask | Enter a number from 0 to 65535, the mask applied to reverse status matching.<br>Leave blank for no reverse status matching.<br>For those bits in the Status Not Mask that are set to 0 (or not specified), the relevant status bits of the packet must match the corresponding bit in the Status field.<br>For those bits in the Status Not Mask that are set to 1, at least one relevant bit of the status packet must be different than the corresponding bit in the Status field.<br>If you do not specify a Status Not Mask, it is padded with "0" bits. |

**Step 4** Click **Apply** to create the filter, or click **Reset** to cancel the changes.

## Tips for Creating Custom Capture Filter Expressions

The TOS value is stored in byte 1 (the second byte) in the IP header. To match the IP packet with a TOS value of 16 (0x10), enter:

Data—10
Offset—1
Base—IP

With nothing in the Data Mask, its effective value is *ff*.

The source address of an IP packet is stored in bytes 12 to 15 in the IP header. To match IP packets with a source address of 15.16.17.18, enter:

Data—0f 10 11 12
Offset—12
Base—IP

To match IP packets with a source address of 15.*.*.18 (where * is any number from 0 to 255), enter:

Data—0f 00 00 12
Data Mask—ff 00 00 ff
Offset—12
Base—IP

To match IP packets with a source address of 15.16.17.18 and a destination address different than 15.16.17.19, enter:

Data—0f 10 11 12 0f 10 11 13
Data Mask—ff ff ff ff ff ff ff ff
Data Not Mask—00 00 00 00 00 00 00 00
Offset—12
Base—IP

# Editing Custom Capture Filters

To edit custom capture filters:

**Step 1** Choose **Capture > Custom Filters**.

The Custom Capture Filters dialog box is displayed.

**Step 2** Choose the filter to edit, then click **Edit**.

The Custom Capture Filter dialog box (see Table 6-10 on page 6-20) is displayed.

**Step 3** Enter information in each of the fields as appropriate.

**Step 4** Do one of the following:

- To apply the changes, click **Apply**.
- To cancel the changes, click **Reset**.

# Deleting Custom Capture Filters

To delete custom capture filters:

**Step 1** Choose **Capture > Custom Filters**.

The Custom Capture Filters dialog box is displayed.

**Step 2** Choose the filter to delete, then click **Delete**.

**Step 3** In the confirmation dialog box, do one of the following:

- To delete the filter, click **OK**.

- To cancel, click **Cancel**.

# Custom Display Filters

Use custom display filters to create and save customized filters to use in the Decode window to limit which packets are to be displayed.

See these topics for help setting up and managing custom display filters:

- Creating Custom Display Filters, page 6-23
- Editing Custom Display Filters, page 6-27
- Deleting Custom Display Filters, page 6-27

## Creating Custom Display Filters

To create custom display filters:

**Step 1** Choose **Capture > Custom Filters**.

**Step 2** In the contents, click **Display Filters**.

The Custom Display Filters dialog box is displayed.

**Step 3** Click **Create**.

The Custom Decode Filter Dialog Box, Table 6-11, displays.

**Step 4** Enter information in each of the fields as appropriate.

*Table 6-11 Custom Decode Filter Dialog Box*

| Field | Description | Usage Notes |
|---|---|---|
| Filter Name | The name of the capture filter. | Enter the name of the filter to be created. |
| Description | The description of the capture filter. | Enter a description of the filter. |
| Protocol | The protocol to match with the packet. | Choose a protocol from the list. (Select **All** to match all packets regardless of protocol.) |
| Address (MAC or IP) | Indicates whether to filter by MAC or IP address. | Choose MAC to filter using the source/destination MAC address of the packets.<br>Choose IP to filter using the source/destination addresses of the packets. |
| Both Directions | Indicates whether the filter is applied to traffic in both directions. | If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A.<br>If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A. |

*Table 6-11 Custom Decode Filter Dialog Box (continued)*

| Field | Description | Usage Notes |
|---|---|---|
| Source | Source address of the packets. | For IP address, enter *n.n.n.n*, where *n* is 0 to 255 or *n.n.n.n/s* where *s* is the subnet mask (0 to 32).<br>For MAC address, enter *hh hh hh ...*, where *hh* are hexadecimal numbers from 0 to 9 or a to f. |
| Destination | Destination address of the packets. | For IP address, enter *n.n.n.n*, where *n* is 0 to 255 or *n.n.n.n/s* where *s* is the subnet mask (0 to 32).<br>For MAC address, enter *hh hh hh hh hh hh*, where *hh* are hexadecimal numbers from 0-9 or a-f. |
| Offset | The offset (in bytes) from the Base where packet data-matching begins. | Enter a decimal number. |
| Base | The base from which the offset is calculated.<br>If you select absolute, the offset is calculated from the absolute beginning of the packet (for example, the beginning of the Ethernet frame).<br>If you select protocol, the offset is calculated from the beginning of the protocol portion of the packet. If the packet does not contain the protocol, the packet fails this match. | Choose **absolute** or a protocol. |

*Table 6-11 Custom Decode Filter Dialog Box (continued)*

| Field | Description | Usage Notes |
|---|---|---|
| Data Pattern | The data to be matched with the packet. | Enter *hh hh hh . . .*, where *hh* are hexadecimal numbers from 0-9 or a-f.<br>Leave blank if not applicable. |
| Filter Expression | An advanced feature to set up complex filter conditions.<br>The simplest filter allows you to check for the existence of a protocol or field. For example, to see all packets that contain the IPX protocol, you can use the simple filter expression **ipx**. | See the "Tips for Creating Custom Decode Filter Expressions" section on page 6-25. |

**Step 5** Do one of the following:

- To create the filter, click **Apply**.
- To cancel the changes, click **Reset**.

## Tips for Creating Custom Decode Filter Expressions

You can construct custom decode filter expressions using the following logical and comparison operators listed in Table 6-12.

*Table 6-12 Logical and Comparison Operators*

| Operator | Meaning |
|---|---|
| and | Logical AND |
| or | Logical OR |
| xor | Logical XOR |
| not | Logical NOT |
| == | Equal |
| != | Not equal |
| > | Greater than |

You can also group subexpressions within parentheses. You can use the following fields in filter expressions:

| Field | Filter By | Format |
|---|---|---|
| eth.addr<br>eth.src<br>eth.dst | MAC address | *hh:hh:hh:hh:hh:hh*, where h is a hexadecimal number from 0 to 9 or a to f. |

| Field | Filter By | Format |
|---|---|---|
| ip.addr<br>ip.src<br>ip.dst | IP address | *n.n.n.n or n.n.n.n/s* , where n is a number from 0 to 255 and s is a 0-32 hostname that does not contain a hyphen. |
| tcp.port<br>tcp.srcport<br>tcp.dstport | TCP port number | A decimal number from 0 to 65535. |
| udp.port<br>udp.srcport<br>udp.dstport | UDP port number | A decimal number from 0 to 65535. |
| *protocol* | Protocol | Click the Protocol list in the Custom Decode Filter dialog box to see the list of protocols on which you can filter. |
| *protocol* [*offset*:*length*] | Protocol data pattern | *hh:hh:hh:hh...*, where hh is a hexadecimal number fro 0 to 9 or a to f.<br>*offset* and *length* are decimal numbers.<br>*offset* starts at 0 and is relative to the beginning of the *protocol* portion of the packet. |
| frame.pkt_len | Packet length | A decimal number that represents the packet length, not the truncated capture packet length. |

#### Examples of Custom Decode Filter Expressions

- To match SNMP packets from 111.122.133.144, enter:

  ```
  snmp and (ip.src == 111.122.133.144)
  ```

- To match IP packets from the 111.122 Class B network, enter:

  ```
  ip.addr == 111.122.0.0/16
  ```

- To match TCP packets to and from port 80, enter:

  ```
  tcp.port == 80
  ```

- The TOS value is stored in byte 1 (the second byte) in the IP header. To match the IP packet with the TOS value 16 (0x10), enter:

  ```
  ip[1:1] == 10
  ```

- The TCP acknowledgement number is stored in bytes 8 through 11 in the TCP header. To match the TCP packet with acknowledgement number 12345678 (0xBC614E), enter:

  ```
  tcp[8:4] == 00:BC:61:4E
  ```

**Note** You can use a filter expression with other fields in the Custom Decode Filter dialog box. In this case, the filter expression is ANDed with other conditions.
Invalid or conflicting filter expressions result in no packet match.

## Editing Custom Display Filters

To edit custom display filters:

**Step 1** **Choose Capture > Custom Filters**.

**Step 2** In the contents, click **Display Filters**.

The Custom Display Filters dialog box is displayed.

**Step 3** Choose the filter to edit, then click **Edit**.

**Step 4** Change the information in each of the fields as appropriate.

**Step 5** Do one of the following:

- To apply the changes, click **Apply**.
- To cancel the changes, click **Reset**.

## Deleting Custom Display Filters

To delete custom display filters:

**Step 1** Choose **Capture > Custom Filters**.

**Step 2** In the contents, click **Display Filters**.

The Custom Display Filters dialog box is displayed.

**Step 3** Choose the filter to delete, then click **Delete**.

**Step 4** In the confirmation dialog box, do one of the following:

- To delete the filter, click **OK**.
- To cancel, click **Cancel**.