



Capturing and Decoding Packets

You can use Packet Analyzer to capture packets to disk or memory buffers. Capture filters is used to select which packets to keep and which to drop. Packet Analyzer also supports built-in packet decoder which can decode captured packets from .pcap files on the disk or directly from a capture memory buffer. Decode filters shows only the interested packets and these interested packets are be written to a new .pcap file. You can then manage the data in local or remote storage and display the contents of the packets to collect troubleshooting information.

This chapter contains the following sections:

- [How Do I Solve My Problem?, page 4-1](#)
- [Manually Starting a Capture, page 4-2](#)
- [Using Alarm-Triggered Captures, page 4-3](#)
- [Scheduling Captures, page 4-3](#)
- [Troubleshooting Application Slowness Using Alarms, page 4-4](#)
- [Application Performance Monitoring Using Capture and Decode, page 4-5](#)
- [Creating and Managing Capture Sessions, page 4-6](#)
- [Working with Capture Files, page 4-15](#)
- [Utilizing Capture Data Storage, page 4-18](#)
- [Working with Capture Query, page 4-25](#)
- [Inspecting Packet Decode Information for Suspicious Traffic, page 4-28](#)

How Do I Solve My Problem?

This section provides an overview of how to collect and analyze packet data to ensure your network is running well or pinpoint network issues.

There are many ways to collect data and analyze it using Packet Analyzer. In order to collect data, the prerequisite is to have set up SPAN or ERSPAN through your Packet Analyzer dataports. For details on data source configuration, see [Understanding Packet Analyzer Traffic Sources, page A-1](#). Many users want a quick capture to analyze their packet data. See [Manually Starting a Capture, page 4-2](#) for details on how to get a quick capture.

[Table 4-1](#) provides an at-a-glance summary of capture tasks you can perform to ensure your network is optimized and trouble-free.

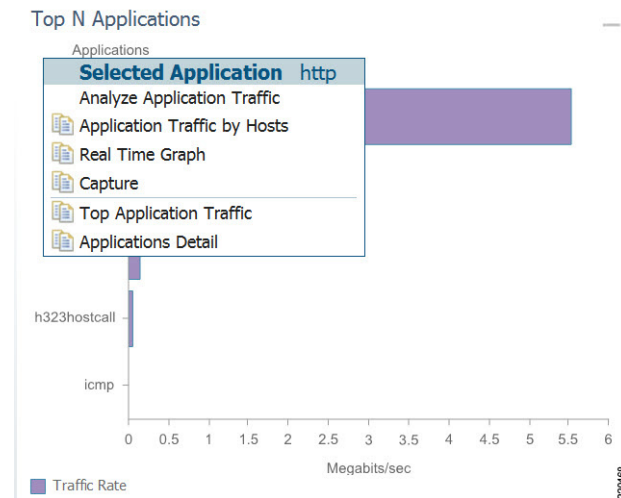
Table 4-1 *Data Collection and Analysis At-a-Glance*

Basics	Operation	Description
Capture the traffic quickly from any Packet Analyzer dashboard when anomalies are present	Quick Capture	Targets data collection based on the dashboard graph you select and provides a capture session and decode window to analyze the traffic immediately. See Manually Starting a Capture , page 4-2. Do not use quick capture if your context includes an NBAR application ID. Use Capture > Packet Capture/Decode > Sessions to configure and start your capture.
Proactively capture packet data to learn the cause of a network issue	Continuous capture or schedule capture	Allows you to set up data collection to: <ul style="list-style-type: none"> Collect data prior to a network problem Set up data collection based on an anomaly that reoccurs See Using Alarm-Triggered Captures , page 4-3 or Scheduling Captures , page 4-3.
Create hardware and software filters to focus on specific long-term packet data	Capture > Packet Capture/Decode > Sessions	On supported Packet Analyzer hardware, helps to limit the amount of packet data processing. See Configuring Hardware Filters , page 4-9 and Configuring Software Filters , page 4-7.
Storing packet data for problem identification	Continuous capture	Allows you to save data to external storage targets, potentially for larger disk capacity and higher capture throughput or to offload capture files. Continuous capture overwrites itself in memory when the buffer is full. See About Capturing to Data Storage , page 4-19.
Create targeted monitoring for problem isolation	Stop Capture and Save to File	Allows you to decide when to use trigger capture sessions. This must be setup in Setup > Alarms > Actions . See Configuring Alarm Actions , page 7-31 and Using Alarm-Triggered Captures , page 4-3.
Set up storage for data collection	Capture > Packet Capture/Decode > Data Storage	Allows you to save data for extended periods either to memory or storage. See About Capturing to Data Storage , page 4-19.
Analyze data for potential issues	Decode	See Inspecting Packet Decode Information for Suspicious Traffic .

Manually Starting a Capture

You do not have to perform any configuration and can quickly collect packet data by selecting the context menu option, **Capture**. [Figure 4-1](#) shows an example of a context menu for Top N Applications dashboard.

For details on how to use the decode window to analyze your data, see [Inspecting Packet Decode Information for Suspicious Traffic](#), page 4-28.

Figure 4-1 Quick Capture

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** Choose **Capture > Packet Capture/Decode > Sessions** and create a capture session. For detailed instructions, see [Configuring Capture Sessions, page 4-6](#).
 - Step 2** Create an alarm event from **Setup > Alarms > Actions** and click **Create** to make a new trigger capture action which uses the session from [Step 1](#).
Configure an alarm event for the type of event for which you want to capture data. For detailed instructions, see [Configuring Alarm Actions, page 7-31](#).
 - Step 3** Create a threshold which uses the alarm event action from [Step 2](#). Choose **Setup > Alarms > Thresholds** window.
To configure the threshold of parameters of interest in the associated Alarm Event, see [Defining Thresholds, page 7-34](#).
-

Scheduling Captures

You can configure multiple time-based triggered captures that start and stop automatically based on a certain time or period of time that you define. This is also referred to as continuous capture. Continuous capture overwrites itself in memory when the buffer is full. The following is an example of setting a 60 minute window to schedule capture packet data.

To set up a schedule capture:

-
- Step 1** Create a new capture from the **Capture > Packet Capture/Decode > Sessions** window.
 - Step 2** Check the Auto Capture **Enable** check box.
 - Step 3** Set the Start Date and Time and Duration (in minutes) to *60*.
 - Step 4** Select an appropriate storage type to store your capture data. For example, select capture to *memory HDD*.
 - Step 5** Select appropriate software filters.
 - Step 6** Click **Submit**.
 - Step 7** To start the capture session, return to the **Capture > Packet Capture/Decode > Sessions** menu and select the capture session you previously created and click **Start**.
-

Troubleshooting Application Slowness Using Alarms

This section describes how to use Packet Analyzer to use triggered alarms and capture files to help you determine the source of some network problems.

Before You Begin

You must already create an alarm that notifies you when there is a surge in application traffic. If you need to create an alarm, thresholds, and set up email notification, see [Setting Up Alarms and Alarm Thresholds](#), page 7-30.

To use existing alarms to help you to create and analyze captured packet files:

-
- Step 1** After receiving an email that was triggered by an alarm notification, view the alarm summary and analyze the details. For example, if your alarm triggers when your application has reached a certain threshold, choose **Monitor > Alarm Summary** to view the Top N Applications by Alarm Count dashboard.

If you use [sites](#), you could view the top sites by alarm count dashboard in order to see the alarm details and determine what threshold variable is causing the alarm to trigger.
 - Step 2** To view more details (or drill down) from this dashboard, left-click the row you are interested in and select **Application Response Time** in order to analyze the response time during the time interval of the alarm trigger. If your application is not listed in the graph, you can select the table icon to choose your application from the list of all the applications and drill down from there to analyze the response time.
 - Step 3** Adjust the Interactive filter to view specific time ranges and severity levels in order to view where the spike in response time occur. This helps to determine if the occurrence is limited to a one-time event, if it occurs more than once in a short period of time, or is an event related to a specific time of the day. For example, by changing the time range filter from 1 hour to 4 hours to 1 day, you can see the latest data trends that help you to determine what to do next. See [Filtering Traffic for Viewing on the Dashboards](#), page C-4.
 - Step 4** In the graph that displays, focus in on the time frame when the event occurs by using the slider to pinpoint the event. Look for peak or valleys; these may be critical changes that require investigation. Using the legend you can determine whether the event was caused by the network or server. See [Changing the Time Interval Using Zoom/Pan Charts](#), page C-6.

- Step 5** Select any of the metrics provided below the application average response time graph.
- a. To view if there are specific clients that have significant transaction time differences, see the Top Clients By Average Transaction Time graph in order to identify data such as Client-Server Application Transactions using an application-specific filter.
 - To view a table of response time metrics and add new metrics for additional data (such as average server response time) and use the drop down menu to select which other metric data you want to appear in the graph.
-

Application Performance Monitoring Using Capture and Decode

This task explains how to proactively monitor your application performance, then use it to help isolate and troubleshoot application latency issues experienced by your end user.

Before You Begin

Packet Analyzer assumes that your system time is synchronized. If you do not have the time synchronized between the Packet Analyzer and the standard time source outside the Packet Analyzer, then you may see either incorrect data or no data. If you suspect inaccurate timestamps, you need to set up the System Time so that Packet Analyzer data presentation is accurate. For instructions on how to set system time by choosing **Administration > System > System Time**, see [Synchronizing Your System Time](#), page 5-5.

- Step 1** Identify and monitor your business critical applications. To see Layer 7 application details, ensure you enable deep packet inspection. Choose **Setup > Classification > Applications Settings** and select the Deep Packet Inspection check box.
- For detailed instructions, see [Adding More Detail into Dashboard and Application Reports](#), page 7-54.
- Step 2** Proactively detect performance degradation using threshold violation alerts. First, define your alarm by choosing **Setup > Alarms > Actions**. Then define the thresholds for your alarm by choosing **Setup > Alarms > Thresholds**.
- For detailed instructions, see [Setting Up Alarms and Alarm Thresholds](#), page 7-30.
- Step 3** Validate a reported trouble ticket or network issue. Choose **Monitor > Overview > Response Time Summary** and use the Top N Applications by Transaction Time dashboard to identify which application may be impacted.
- You can select the table view to see more than the top default applications. You can also use the other dashboards to view server or client transaction times. See [Using Response Time Summary](#), page 3-5.
- Step 4** Analyze the application performance behavior over time using the Interactive Report filter. Determine if the behavior is transient, persistent, recurring, and so on. For details on using the Interactive Report filters, see [Filtering Traffic for Viewing on the Dashboards](#), page C-4.
- Step 5** Zoom in to view specific spikes in the performance, and drill down to isolate whether the cause of the degradation stems from your network, server or application. See [Changing the Time Interval Using Zoom/Pan Charts](#), page C-6.
- Step 6** Analyze the server response time and network performance metric in order to eliminate one of them as the cause. See [Server Response Time](#), page 3-22 and [Network Response Time](#), page 3-21.
- Step 7** Analyze server activity based on the traffic the server is placing on the network and assess the cause of increase in the server response time. See [Analyzing Host Traffic](#), page 3-11.

- Step 8** Perform packet captures in order to identify the root-cause. For details on quick captures or trigger captures, see [Capturing and Decoding Packets, page 4-1](#).
- Step 9** Perform additional actions to isolate and troubleshoot the problem including: QoS analysis and interface analysis.
-

Creating and Managing Capture Sessions

You can use capture sessions to capture, filter, and decode packet data, manage the data in a local or remote storage, and display the contents of the packets. The captured packets can be decoded and analyzed using Packet Analyzer for more efficient problem isolation.

This section contains the following topics:

- [Configuring Capture Sessions, page 4-6](#)
- [Configuring Software Filters, page 4-7](#)
- [Configuring Hardware Filters, page 4-9](#)
- [Understanding Hardware and Software Capture Sessions Filters, page 4-14](#)
- [Viewing Capture Sessions, page 4-15](#)

Configuring Capture Sessions

It is important for you to collect data over time and have various locations for which you want to analyze data, we support multiple sessions per capture location/target. You can collect data using multiple sessions per target, but only one session runs per hard disk target. Concurrent capture sessions can run if capture to buffers or different hard disk based targets. This limitation is mainly to avoid disk fragmentation and better performance. Capture decode filters can be used to view or separate different subset of packets to different files. Packet Analyzer now supports up to 25 capture sessions. If you have external storage you can save to local disk and some number of LUNs. As part of configuring a capture session, you can also create software filters, if desired (see [Creating a Software Capture Filter for a Capture Session, page 4-7](#)).

To configure a new capture session:

-
- Step 1** Choose **Capture > Packet/Capture Decode > Sessions**.
- Step 2** Click **Create** to set up a new capture. The Packet Analyzer displays the Configure Capture Session window.
- Step 3** Enter information in the Capture Settings Fields ([Table D-60](#)) as appropriate.
- 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 4** Click **Submit** to finish configuration for this session, or configure Software Filters for this session .
-

Configuring Software Filters

You can create and save specialized filters that will disregard all capture data except the information in which you are interested (see [Figure 4-5](#)). You can configure multiple software filters for each session (up to six). This allows you to narrow in on the traffic that you are interested in, and it also saves resources (either memory or disk space).

Use the following topics for help on filtering network traffic using software filters:

- [Creating a Software Capture Filter for a Capture Session, page 4-7](#)
- [Editing a Software Capture Filter, page 4-7](#)
- [Understanding Software Capture Filter Options, page 4-8](#)

Creating a Software Capture Filter for a Capture Session

You can create software capture filter for many variables. This workflow examines how to create a capture session with a software filter.

To create a software capture filter:

-
- | | |
|---------------|--|
| Step 1 | Choose Capture > Packet Capture/Decode > Sessions . |
| Step 2 | Click Create to create a new capture session.

If you already have a capture session to which you want to add a software filter, see Editing a Software Capture Filter, page 4-7 for detailed instructions. |
| Step 3 | Click Create in Software Filters section. |
| Step 4 | Enter information in each of the fields as appropriate. See Table D-66 for descriptions of the fields. |
| Step 5 | Click Submit to create the filter, or click Cancel to close the dialog box without creating a software filter. |
-

Editing a Software Capture Filter

To edit software capture filters:

-
- | | |
|---------------|---|
| Step 1 | Choose Capture > Packet Capture/Decode > Sessions . |
| Step 2 | Choose the session to edit, then click Edit .

The Software Filter dialog box displays. See Table D-66 . |
| Step 3 | Choose the Software Filters , then click Edit . |
| Step 4 | Enter information in each of the fields as appropriate. |
| Step 5 | Do one of the following: <ul style="list-style-type: none">• To apply the changes, click Submit.• To cancel the changes, click Cancel. |
-

Important Notes about Software Capture Filters

This section contains important software capture filters details that may be helpful to know.

- Multiple software filters use the “OR” logic; in other words, if a packet passes any software filter, it is captured.
- If you create a session and then start it, you cannot edit the session or analyze it without stopping it. If you edit a session containing already captured data, you get a warning stating that the session will be cleared and the data removed. If clearing the session and removing the data is acceptable, ignore the warning dialog message, then add a filter to the session and click **Submit** to enable the new filter settings.
- The application filter can be used to filter on the highest layer of the protocol parsing; that is usually a layer 4 protocol (based on port). If you want to filter on the transport protocol (for example, UDP or TCP), you will need to use the IP Protocol selector. Selecting, for example, TCP in the “IP Protocol” selector will filter on all packets using TCP.



Tip

Be careful when setting capture software filtering for encapsulation. If you set a software capture filter with encapsulation for the top three network traffic layers only, data displays only if the top three layers match the specified encapsulation type.

Understanding Software Capture Filter Options

You can define a software filter to filter based on any of the following options:

- Source host address
- Destination host address
- Network encapsulation
- VLAN or VLAN range
- TCP Flag bits
- Application
- Source port or port range
- Destination port or port range
- IP Protocol



Note

Software capture filtering is not supported on URL-based applications.

[Table D-66](#) contains descriptions of the Software Filter dialog box fields.

**Note**

The parameters described in the table above are independently evaluated by the Packet Analyzer. Therefore, the Packet Analyzer will allow you to enter parameters that are contradictory, but you will not be able to get meaningful results if they do not match.

For example, the parameters Network Encapsulation and Source/Destination Address are independently evaluated. If a filter is specified with contradicting parameters such as “Network Encapsulation=IP4” and “Source Address=an IPv6 address”, it will never match any traffic, and the result will be 0 packets captured.

Configuring Hardware Filters

You can use hardware filtering to help limit the amount of traffic allowed into the Packet Analyzer for processing. The Packet Analyzer hardware platforms that support hardware filtering include:

- Specific Packet Analyzer 2000 Series Appliance—2400

Depending on your Packet Analyzer, the hardware filter support varies.

Creating Packet Analyzer Appliance Hardware Filters

This section describes how to create Packet Analyzer appliance hardware filters.

The Hardware filters allow you to improve capture performance by eliminating extraneous traffic, since packets filtered out are excluded from capture processing.

**Note**

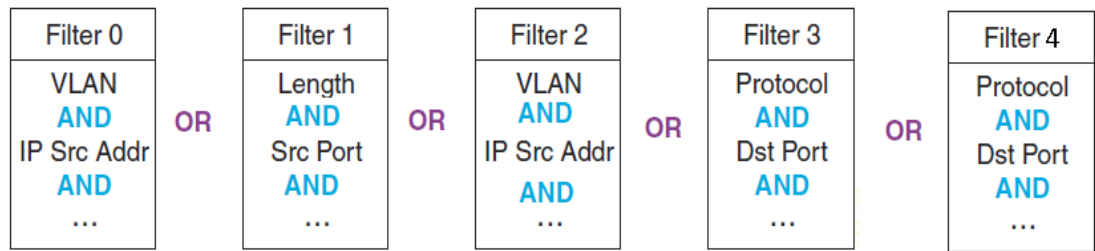
The hardware filter applies to the Packet Analyzer 2400 appliance. .

Software filters add flexibility to your filtering, but a capture session is most efficient when you use hardware filters only. The less traffic requiring software filtering, the more efficient the filtering.

For the Packet Analyzer appliances that support hardware filtering, you can set up to five hardware filters per appliance. When multiple hardware filters are created on the appliance, the logic among them are OR logic.

Hardware filters and global packet slicing affect all capture sessions, except for ERSPAN capture sessions.

All fields within a single filter are combined with AND logic. The filters are then combined with OR logic. See [Figure 4-2](#) for examples of filter logic you can use.

Figure 4-2 Hardware Filter Logic (AND/OR)

See [Configuring Supported Packet Analyzer Appliance Hardware Filters, page 4-10](#) for detailed steps.

Configuring Supported Packet Analyzer Appliance Hardware Filters

The Hardware Filters window appears at the bottom of the **Capture > Packet Capture/Decode > Sessions** window. To configure a hardware filter:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Sessions**.
 - Step 2** Click **Create**.
 - Step 3** Enter a name in the Name field.
 - Step 4** Choose any or all of the following types of filters:
 - VLAN
 - VLAN and IP
 - IP
 - IP and TCP/UDP
 - [IP and Payload Data](#)
 - [Payload Data](#)



Note

When you use the IP address fields in the hardware filters, tunneled packets will be filtered based on the outer IP address. The Packet Analyzer will further inspect matching packets to analyze the contents within the tunnel. The Packet Analyzer will always display the inner IP address in the packet list. See [Understanding the Packet Analyzer Packet Decoder, page 4-31](#) for details.

- Step 5** Data fields will then appear that correspond with the type of hardware filter you select. Fill in the desired fields.
 - Step 6** Click **Submit** to complete the configuration of the capture session.
-

IP and Payload Data

To configure an IP and Payload Data hardware filter:

-
- Step 1** Enter a Filter Name and select your options.

- Step 2** Enter a Source Address / Mask (optional).
- Step 3** Enter a Destination Address / Mask (optional).
- Step 4** Choose a Layer 4 Protocol, either TCP or UDP.
- Step 5** Enter the values for Pattern Match:
- Enter a Value of up to four bytes (eight hex characters).
 - Enter a Mask of up to four bytes (eight hex characters).
 - Enter an Offset from 1-1023. The offset is relative to the beginning of the payload (Layer 5).

**Note**

Only one payload segment (one row) is required and provided. This is to guard against overlapping payload segments. If overlapping segments have different values the filter will never match anything due to the inherent AND logic.

- Step 6** Click **Submit**.

Payload Data

To configure a Payload Data hardware filter:

- Step 1** Enter a Filter Name.
- Step 2** Choose a Layer 4 Protocol, either TCP or UDP.
- Step 3** Enter the values for Payload Data:
- Enter a Value of up to four bytes (eight hex characters).
 - Enter a Mask of up to four bytes (eight hex characters).
 - Enter an Offset from 1-1023. The offset is relative to the beginning of the payload (Layer 5).

**Note**

Only one payload segment (one row) is required and provided. This is to guard against overlapping payload segments. If overlapping segments have different values the filter will never match anything due to the inherent AND logic.

- Step 4** Click **Submit**.

Configuration Example

Figure 4-3 and Figure 4-4 shows configuration examples on how to calculate the offset value and how to set mask to use the payload feature.

Figure 4-3 Configuration Example

Creating and Managing Capture Sessions

No.	Time	Source	Destination	Protocol	Length	No.	Time	Source	Destination	Protocol	Length
1	0.000000	66::1e00:1010	66::1e00:1600	FTP	107	1	0.000000	66::1e00:1010	66::1e00:1600	FTP	107
6	0.000908	66::1e00:1010	66::1e00:1600	FTP	100	6	0.000908	66::1e00:1010	66::1e00:1600	FTP	100
11	0.001486	66::1e00:1010	66::1e00:1601	FTP	105	11	0.001486	66::1e00:1010	66::1e00:1601	FTP	105
12	0.001644	66::1e00:1010	66::1e00:1601	FTP	120	12	0.001644	66::1e00:1010	66::1e00:1601	FTP	120
13	0.001813	66::1e00:1010	66::1e00:1601	FTP	102	13	0.001813	66::1e00:1010	66::1e00:1601	FTP	102

Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)						Frame 6: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)					
Ethernet II, Src: 00:00:e9:ed:c1:e8 (00:00:e9:ed:c1:e8), Dst: 00:00:8f:8e:c8:40 (00:00:8f:8e:c8:40)						Ethernet II, Src: 00:00:e9:ed:c1:e8 (00:00:e9:ed:c1:e8), Dst: 00:00:8f:8e:c8:40 (00:00:8f:8e:c8:40)					
802.1Q Virtual LAN, PRI: 1, CFI: 0, ID: 306						802.1Q Virtual LAN, PRI: 1, CFI: 0, ID: 306					
Internet Protocol Version 6, Src: 66::1e00:1010 (66::1e00:1010), Dst: 66::1e00:1600 (66::1e00:1600)						Internet Protocol Version 6, Src: 66::1e00:1010 (66::1e00:1010), Dst: 66::1e00:1600 (66::1e00:1600)					
Transmission Control Protocol, Src Port: 38112 (38112), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 13						Transmission Control Protocol, Src Port: 38112 (38112), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 6					
File Transfer Protocol (FTP)						File Transfer Protocol (FTP)					
RETR /#4095\r\n						QUIT\r\n					

Hex Data			ASCII Data		
0000	00 00 8F 8E C8 40 00 00 E9 ED C1 E8 81 00 21 32@.....12	0000	00 00 8F 8E C8 40 00 00 E9 ED C1 E8 81 00 21 32@.....12
0010	86 DD 60 00 00 00 00 2D 06 40 00 66 00 00 00 00	..`.....@.f....	0010	86 DD 60 00 00 00 00 26 06 40 00 66 00 00 00 00	..`.....@.f....
0020	00 00 00 00 00 00 1E 00 10 10 00 66 00 00 00 00f....	0020	00 00 00 00 00 00 1E 00 10 10 00 66 00 00 00 00f....
0030	00 00 00 00 00 00 1E 00 16 00 94 E0 00 15 FE BBf....	0030	00 00 00 00 00 00 1E 00 16 00 94 E0 00 15 FE BBf....
0040	7C 21 FE F6 78 A0 80 18 0A E1 AB 42 00 00 01 01	.x.....B....	0040	7C 2E FE F6 78 F7 80 18 0A 8A 5D C9 00 00 01 01	.x.....]....
0050	08 0A 6E 18 55 84 6E 18 4A 48 52 45 54 52 20 2F	..n.U.n.JHRETR /	0050	08 0A 6E 18 55 85 6E 18 4A 48 51 55 49 54 0D 0A	..n.U.n.JHQUIT..
0060	23 34 30 39 36 0D 0A BA D7 49 1A	#4096...I.	0060	5D F2 E4 78]...x

Hardware Filter Dialog

* Name: ipv6 tcpPortPayload

Description:

Type: IP and Payload Data

Source Address / Mask: 66::1e00:1010/128

Destination Address / Mask:

Protocol: TCP

Payload Data: Offset 6 Value Ox 23343039 Mask Ox ffffffff

Offset Value Ox Mask Ox

Offset Value Ox Mask Ox

Offset Value Ox Mask Ox

Apply Cancel Reset

Hardware Filter Dialog

* Name: ipv6 tcpPortPayload

Description:

Type: Payload Data

Protocol: TCP

Payload Data: Offset 0 Value Ox 51550000 Mask Ox ffff0000

Offset Value Ox Mask Ox

Offset Value Ox Mask Ox

Offset Value Ox Mask Ox

Apply Cancel Reset

Figure 4-4 Configuration Example (Continued)

403275

No.	Time	Source	Destination	Protocol	Length
1	0.000000	66::1e00:1010	66::1e00:1600	FTP	107
6	0.000908	66::1e00:1010	66::1e00:1600	FTP	100
11	0.001486	66::1e00:1010	66::1e00:1601	FTP	105
12	0.001644	66::1e00:1010	66::1e00:1601	FTP	120
13	0.001813	66::1e00:1010	66::1e00:1601	FTP	102

.....

▶ Frame 12: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)

▶ Ethernet II, Src: 00:00:e9:ed:c1:e8 (00:00:e9:ed:c1:e8), Dst: 00:00:8f:8e:c8:41 (00:00:8f:8e:c8:41)

▶ 802.1Q Virtual LAN, PRI: 1, CFI: 0, ID: 306

▶ Internet Protocol Version 6, Src: 66::1e00:1010 (66::1e00:1010), Dst: 66::1e00:1601 (66::1e00:1601)

▶ Transmission Control Protocol, Src Port: 38116 (38116), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 26

▼ File Transfer Protocol (FTP)

▶ PASS noreply@ixiacom.com\r\n

```

0000  00 00 8F 8E C8 41 00 00 E9 ED C1 E8 81 00 21 32  ....A.....!2
0010  86 DD 60 00 00 00 00 3A 06 40 00 66 00 00 00 00  ..\.....@.f...
0020  00 00 00 00 00 00 1E 00 10 10 00 66 00 00 00 00  .....f....
0030  00 00 00 00 00 00 1E 00 16 01 94 E4 00 15 FE 96  .....
0040  81 1F FF 6D 75 DA 80 18 0B 29 C8 C0 00 00 01 01  ...mu.....)....
0050  08 0A 6E 18 55 85 6E 18 4A 49 50 41 53 53 20 6E  ..n.U.n.JIPASS n
0060  6F 72 65 70 6C 79 40 69 78 69 61 63 6F 6D 2E 63  oreply@ixiacom.c
0070  6F 6D 0D 0A 47 E1 8E D9                          om..G...

```

Hardware Filter Dialog

* Name ⓘ

Description

Type

Source Address / Mask

Destination Address / Mask

Protocol

Payload Data

Offset Value Ox Mask Ox

Offset Value Ox Mask Ox

Offset Value Ox Mask Ox

Understanding Hardware and Software Capture Sessions Filters

You can filter specific traffic data and manage that information in local or remote storage. This increases your visibility into network issues and allows you to filter out unnecessary information. You can use either hardware or software filters to target specific packet data to receive.

As shown in [Figure 4-5](#), if network packets coming into the Packet Analyzer pass through the hardware filters you have configured, the packets go on to the next step. If no hardware filters are configured, all packets pass through.



Note

Hardware filters are supported on specific Packet Analyzer platforms. See [Configuring Hardware Filters, page 4-9](#) for details.

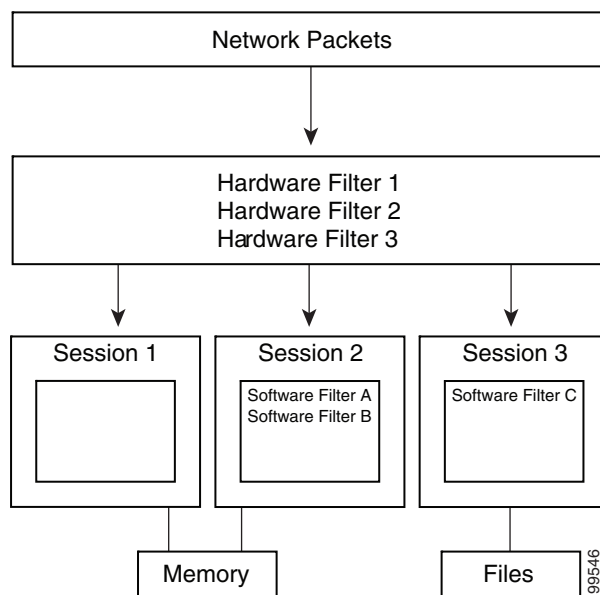
Packets must then pass at least one software filter in that particular session to be saved by that session. If no software filters are configured for a session, then all packets are captured. For more information about software filters, see [Configuring Software Filters, page 4-7](#).

For better performance for the supported Packet Analyzer platforms, hardware filters are recommended over software filters, and fewer sessions are recommended over more sessions.

You do not have to configure the items in [Figure 4-5](#) in any particular order. For example, you can set Global Capture Settings first, and then configure Capture Sessions, and then create filters; or, you can create Hardware and Software filters first, and then configure Capture Sessions, and finally apply Global Capture Settings. We recommend that you “Start” the session last; otherwise, you will start capturing before you have configured any filters and before doing any packet slicing.

Global Capture Settings and Hardware Filters can be changed at any time, even when the session is running; they will affect running capture sessions immediately. We recommend that you first stop your capture session to edit it since you may capture some unexpected packets during the filter change.

Figure 4-5 *Packet Analyzer Capture Sessions Example*



Viewing Capture Sessions

To access the basic operations for capturing, viewing and decoding packet data on the Packet Analyzer, choose **Capture > Packet Capture/Decode > Sessions**.

The Capture Sessions window shows the list of capture sessions. If none have been configured, the list will be blank. [Table D-59](#) describes the Capture Sessions fields and operations that you can perform from the Capture Sessions window.

Working with Capture Files

To decode, download, rename, convert/merge, delete, analyze, or error-scan saved packet capture files use the Files option.

This section covers the following topics:

- [Analyzing Capture Files, page 4-15](#)
- [Downloading Capture Files, page 4-16](#)
- [Deleting a Capture File, page 4-16](#)
- [Deleting Multiple Capture Files, page 4-16](#)
- [Understanding Capture Sessions, page 4-17](#)

Analyzing Capture Files

The Capture Files window (click **Analyze** button at **Capture > Packet Capture/Decode > Files**) enables you to obtain various statistics including traffic rate (bytes/second) over a capture period and lists of hosts and protocols associated with network traffic.

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.



Note

After clicking the **Drill-Down** button, the Host Statistics results table will display both source and destination hosts, if either the source or destination host of the traffic belongs to the Host/Subnet that you had specified.

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 choosing **Drill-Down**. You can also drill down on a specific **Protocol** or **Host/subnet** address.

[Table D-58](#) describes the different areas of the Capture Analysis window.

Drilling Down into Packet Error Details

You can further investigate, or drill down, into packet error details by viewing the decode packet data available on Packet Analyzer.

The Capture Errors and Warnings Information window shows warnings and errors, and packet irregularities. From here, you can launch the Packet Decode Window, where you can drill down to packet details.

To get to the Capture Errors and Warnings Information window, choose **Capture > Packet Capture/Decode > Files**. Highlight a file and click the **Errors Scan** button. The Error Scan window displays. The fields are described in [Table D-61](#). Then select the packet details by selecting a row and clicking the **Decode Packets** button.

Downloading Capture Files

You can only download one capture file at a time. To download a capture file to your computer:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Files**.
 - Step 2** Choose a capture file from the list of captures.
 - Step 3** Click **Download**.
 - 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 > Packet Capture/Decode > Files**.
 - Step 2** Check the check box to select a capture file from the list of captures, or select more than one if desired.
 - Step 3** Click **Delete**. A dialog box displays and asks “**Are you sure you want to delete file(s)?**” and displays the file name.
 - Step 4** Click **OK** to delete the file(s) or **Cancel** to allow the file(s) to remain.
-

Deleting Multiple Capture Files

To delete all capture files at once:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Files**.
 - Step 2** Check at least one check box to select a capture.
 - Step 3** Click **Delete All** to delete all captures.

A dialog box displays and asks “**Are you sure you want to delete all files?**”

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

Understanding Capture Sessions

To understand how Packet Analyzer creates capture files with saved packet data, it is important to learn about how Packet Analyzer handles capture session triggers.

This section contains the following topics:

- [Types of Capture Triggers, page 4-17](#)
- [Resolving Session Conflicts, page 4-17](#)
- [Manipulating Capture Files, page 4-18](#)

Types of Capture Triggers

Packet capture sessions can be triggered on the Packet Analyzer in several ways:

- Manually, by starting a capture using the Capture menu option or clicking the Start capture button.
- Scheduled, by specifying a start date/time and maximum duration when you create or edit a capture session.
- Alarmed, by creating an alarm with an associated trigger capture action that starts a particular capture session.

Resolving Session Conflicts

Packet Analyzer supports multiple capture sessions associated with the same capture storage location, but only one of these sessions can be running at any given time. Since there are several ways for such capture session to be started, it is possible for conflicts to arise among such capture sessions.

For example, suppose one capture session is started manually, but another capture session is scheduled to begin capturing while the first is still running. If these two sessions capture to the same storage location, there is a conflict. In this case, Packet Analyzer resolves the conflict by automatically stopping the manual session and allowing the scheduled session to begin.

In general, Packet Analyzer resolves capture session conflicts by prioritizing them in the following (descending) order:

1. High-severity alarm triggered capture
2. Low-severity alarm triggered capture
3. Scheduled capture
4. Manual capture

If a manually started capture session is saving data to the local disk and a scheduled capture is set to begin capturing to the same local disk, Packet Analyzer does not stop the manual session if the “uninterruptible” flag is set to true.

If there are existing capture sessions already running on the same storage target, this means there is a conflicting alarm trigger. An alarm trigger is created when you configure an alarm threshold to start collecting packet data. Each alarm has a severity option.

Once a capture session is completed, you can manipulate the file. See

Manipulating Capture Files

This section provides an overview of the tasks you can complete with capture files. See [Table 4-2](#).


For information about how to save capture sessions to files, see [Creating and Managing Capture Sessions](#), page 4-6.



Caution

If you have capture files with a state of **Full** and the Packet Analyzer is rebooted, the capture is triggered again and these files may be overwritten by the new capture. If you want to retain the file, save the file before you reboot.

Table 4-2 Actions You Can Complete with Capture Files

Action	Description
Decode	Display the packets in a file.
Download	Download a file to your computer in .pcap file format.
	 Note Do not add a file suffix when you provide the filename. The suffix .pcap is added automatically.
Rename	Give the file a new name. A dialog box displays and asks you to enter the new name for the selected capture file.
Merge	Merges capture files that were captured simultaneously in chronological order.
	Note Merged files cannot exceed 2,000 MB. This limit is set purposely since many tools can not handle the large size capture files.
Delete	Delete selected capture files.
Analyze	View statistical analysis of the selected capture. See Analyzing Capture Files , page 4-15.
Errors Scan	View more information about the file (Packed ID, Protocol, Severity, Group, and Description). From here you can also decode the packet. For more information see Drilling Down into Packet Error Details , page 4-15.

Utilizing Capture Data Storage

Cisco Security Packet Analyzer platforms offer external storage connectivity for extended capture durations and higher capture bandwidths. All platforms support iSCSI data storage. Some platforms may support other forms of data storage, but this document covers only iSCSI data storage.

This section covers the following topics:

- [About Capturing to Data Storage](#), page 4-19
- [Installing and Configuring Local and External Storage](#), page 4-19
- [Recovering Data Storage](#), page 4-24

Figure 4-6 External Storage Setup



About Capturing to Data Storage

To avoid filling up the local server disk on the Packet Analyzer, you can capture files to external storage. One of the benefits of using external storage is that it can provide larger capacities, higher read/write speeds, and can be moved from one Packet Analyzer to another. The capture files are decoded in the same manner as the **Capture > Packet Capture/Decode > Files** page.

Using Packet Analyzer, you can perform internal and external storage management using **Capture > Packet Capture/Decode > Data Storage**. This window lists detected storage devices, including the internal hard drive, if one is available. For details on how to install and configure local and external storage, see [Installing and Configuring Local and External Storage, page 4-19](#).

This release supports 32 external data storage targets, or Logical Unit Numbers (LUNs).

You can create multiple capture sessions per target. Only one capture per storage target (file location) is allowed at a time. Additionally you can have multiple sessions to memory.

Installing and Configuring Local and External Storage

You can use local or external storage as a repository for long term data for performance comparisons.

This topic covers:

- [Configuring the iSCSI and SAS Array, page 4-20](#)
- [Locating the Packet Analyzer IQN and SAS Address, page 4-20](#)
- [Preparing LUNs for File Storage in iSCSI and SAS, page 4-22](#)
- [Connecting to the iSCSI Array, page 4-21](#)
- [Using LUNs to Store Packets in iSCSI and SAS from a Capture Session, page 4-22](#)
- [Logging In and Out of External Storage LUNs, page 4-23](#)
- [Connecting and Disconnecting iSCSI and SAS, page 4-23](#)
- [Configuring External SAS port, page 4-23](#)

Configuring the iSCSI and SAS Array

You may decide that in addition to or instead of local storage that you want to set up an external storage drive using iSCSI and SAS. This section contains the required settings for Packet Analyzer.

Use your vendor's user documentation to ensure you have properly configured the iSCSI and SAS array. The Cisco Packet Analyzer is independent of most array settings, but some are important for accessibility and performance.

-
- Step 1** To configure the disk volumes on the array there is often a *Segment Size* setting. Larger segment sizes can improve write speeds. Configure the *Segment Size* setting to use the largest possible segment size (up to 512 KB).
- Multiple volumes can be configured on a single array.
- Step 2** Assign a Logical Unit Number (LUN) to the disk volume. This number is used for volume identification by the host.
- Step 3** Map the LUNs to iSCSI Qualified Names (IQNs) and to the SAS address on the array. The Packet Analyzer's local IQN and SAS address are listed using `remote-storage iscsi local-iqn` and `remote-storage sas local-address`. Each IQN and SAS unique identifier represent a different list of LUNs which hosts (such as the Packet Analyzer) can access.
- Packet Analyzer supports up to 32 LUNs between all protocols and multiple LUNs mapped to one IQN and SAS address.
- Step 4** Packet Analyzer also has an IQN, which represents the host side of an iSCSI session and a SAS address which represents the SAS session. You must give the Packet Analyzer's IQN SAS address access to the iSCSI and SAS array's LUNs. The arrays call this *Host Access*. Be sure to give the Packet Analyzer's IQN and SAS address read-write access. Most arrays require this for security reasons to ensure that only certain hosts can access the LUNs.
- Each Packet Analyzer has a unique IQN and SAS address, so perform this required step for each Packet Analyzer that requires access and for each target LUN that you want to access. For more details about which CLI command to use, see [Locating the Packet Analyzer IQN and SAS Address, page 4-20](#).



Caution

Only one Packet Analyzer should connect to a LUN because only one host can have write access at a time. If multiple Packet Analyzer connect to the same LUN simultaneously, there will be access conflicts and capture operations may not work properly.

-
- Step 5** Ensure the Packet Analyzer management port has IP connectivity to the iSCSI or SAS array. For details on how to complete this required task, see [Connecting to the iSCSI Array, page 4-21](#).
-

Locating the Packet Analyzer IQN and SAS Address

To find the Packet Analyzer IQN, use the `remote-storage iscsi local-iqn` CLI and for SAS address, use the `remote-storage sas local-address` command:

```
root@secpaxx# remote-storage iscsi local-iqn
Local iSCSI Qualified Name: iqn.1987-05.com.cisco:WS-SVC-NAM3-6G-K9.00:19:55:07:15:9A
```

For details on how to complete the storage array configuration, see [Connecting to the iSCSI Array, page 4-21](#).

Connecting to the iSCSI Array

After you configure the iSCSI storage arrays, ensure that the array has an IP path to the Packet Analyzer management port. The array can be connected while the Packet Analyzer is running.

Some arrays come with multiple storage controller modules. As a security feature, module ownership must often be mapped to each LUN or IQN.

The Packet Analyzer logs into the storage to start an iSCSI session using the IP address and IQN(s) of the storage array.

To connect the storage array using the user interface:

-
- Step 1** Log into the Packet Analyzer web interface. To access the Data Storage page, choose **Capture > Packet Capture/Decode > Data Storage**.
- Step 2** Click **iSCSI Login** and enter the iSCSI array IP address. Then click **Search IQN Targets**.
A list of IQNs available to the Packet Analyzer host IQN appear.
- Step 3** Depending on the outcome, perform one of the following steps:
- a. If the IQNs do not appear, check **remote-storage iscsi list** to verify the iSCSI session was properly started.

The follow example shows how to verify the iSCSI session.

```
root@secpaxx# remote-storage iscsi list
Storage ID: 16
Label:
Status: Ready
Protocol: iSCSI
Target IP: 172.20.122.81
Target IQN: iqn.2011-09:celeros.target11
Type: LUN
Model: IET VIRTUAL-DISK
LUN: 4
Capacity: 24.98GB
Available: 24.98GB
Active iSCSI Sessions:
tcp: [8] 172.20.122.81:3260,1 iqn.2011-09:celeros.target11
```

The LUN number (in the above example, *LUN 4*) helps you identify one LUN from others mapped to the same IQN. This number is unique to each IQN, meaning two LUNs from different IQNs can have the same number.

- b. If the iSCSI session was properly started, check the storage array configuration to verify that:
 - The LUNs are mapped to the target IQN, and
 - The Packet Analyzer IQN has been given Read/Write access to the LUNs.

- c. If you make any configuration changes, logout of the iSCSI session and login again. To logout, use the CLI **remote-storage iscsi logout** or use the GUI and click **iSCSI Logout**. All LUNs mapped to that target IQN will be disconnected from the Packet Analyzer.
-

Preparing LUNs for File Storage in iSCSI and SAS

Some arrays come with multiple storage controller modules, and the module ownership must often be mapped to each LUN (Logical Unit Numbers). This is a common security feature.

To see if the Packet Analyzer can access the storage array LUNs and prepare them to store files:

Step 1 Choose **Capture > Packet Capture/Decode > Data Storage**.

New LUNs which have not been used by the Packet Analyzer show a status of *Unformatted*.

- a. Skip to [Step 3](#) if your LUNs are formatted.
- b. If no LUNs appear, see [Installing and Configuring Local and External Storage, page 4-19](#) and [Configuring the iSCSI and SAS Array, page 4-20](#) for detailed instructions on how to set up your storage array.

Step 2 To prepare these LUNs for capture use, select the LUN and click **Format**. After a few minutes, the status should change to *Ready*.

Step 3 To apply optional user labels to the LUNs to help differentiate between them, select the LUN and click **Label**.

The Label dialog appears with information about the current label and the last time the LUN was formatted.

You are now ready to use the external storage for capture files.

Using LUNs to Store Packets in iSCSI and SAS from a Capture Session

To use a LUN to store packets from a capture session:

Step 1 Go to **Capture > Packet Capture/Decode > Sessions**.

Step 2 Under the Capture Sessions table, click **Create**.

Step 3 Fill in the appropriate fields for creating a session, and for Storage Type choose the **Files** option.

Step 4 Use the File Location table to select the LUN you wish to use. Each list entry includes the protocol and either the model or the user label if it is set. Note that the list will only include targets which are in the *Ready* state.

Step 5 Click **Submit** to create the session.

When a session is *STARTED*, the associated LUN state changes to *In Use*. At that point, no other session can use that LUN until the session is deleted. This prevents contention, corrupted data, and write bandwidth degradation.

Logging In and Out of External Storage LUNs

You can use iSCSI to facilitate data transfers over intranets and to manage your remote capture data storage.

Packet Analyzer provides a more streamlined workflow to log in and out of your data storage targets. You must log into iSCSI in order to save capture sessions to remote storage. If you do not log in, capture sessions are saved to either local disk or memory locations.

To log in or out of your available remote data storage LUNs:

-
- Step 1** Ensure you have configured your target iSCSI system with read/write permission to your Packet Analyzer for at least one LUN in the storage array. For details, see [About Capturing to Data Storage, page 4-19](#).
 - Step 2** Choose **Capture > Packet Capture/Decode > Data Storage** and click **iSCSI Login**.
 - Step 3** To enable auto discovery of any iSCSI Qualified Name (IQN) target, enter the target IP address of the storage location and click **Search IQN Targets**.
All available IQNs for that location display in the table.
 - Step 4** To log out, click **iSCSI Logout**. The list of IQNs to which you are currently logged into displays in a table.
 - Step 5** To view the LUNs which the system will log you out, select one of the IQNs and a popup displays the associated LUNs to select.
-

Connecting and Disconnecting iSCSI and SAS

Before physically disconnecting an external storage device, it is highly recommended to use the **Unmount** button on the **Capture > Packet Capture/Decode > Storage** window. This notifies the Packet Analyzer that the device will be disconnected, so that the Packet Analyzer can perform important cleanup procedures. After this is done, the storage target displays as *Unmounted* in the status column, and it is safe to remove the external storage device. External storage is automatically unmounted in this manner when the Packet Analyzer is powered down.



Caution

If this step is skipped, it is possible to corrupt the storage data upon physical disconnect.

If a device has been logically disconnected using the **Unmount** button, but the storage is still physically connected, it can be reactivated using the **Mount** button. It will restore the storage target's previous state. This makes it unnecessary to physically disconnect and reconnect the storage, which can be particularly useful if the storage is located far away from you.

Configuring External SAS port

All the Cisco SEC-PA-2400-K9 appliances have two SFF8644 mini-SAS HD connectors on UCSC-SAS9300-8E card (See [Figure 4-7](#)) at the rear of the chassis, which supports iSCSI managed storage arrays using x8 wide SAS ports. Use SFF-8644 (12G SAS) port to reach the SAS storage.

Connect the External SAS port to the External SAS device. Navigate to **Capture > Packet Capture/Decode > Data Storage** page to see the External SAS storage devices.

Figure 4-7 UCSC-SAS9300-8E Card

Recovering Data Storage

In the event that a previously working target displays as *Unformatted*, you can use the CLI to determine what happened by running a filesystem check on it. Use the command **remote-storage <protocol> fsck <storage ID>**, when you know the protocol. You can find the storage ID using **remote-storage <protocol> list**. The filesystem check can potentially resolve filesystem corruption or state issues. If the command succeeds, it automatically mounts the storage and displays as *Ready*.

The following shows a iSCSI recovery example:

```
root@secpa.cisco.com# remote-storage iscsi list
Storage ID: 16
  Label:
  Status: Unformatted
  Protocol: ISCSI
  Target IP: 172.20.10.81
  Target IQN: iqn.2011-09:celeros.target11
  Model: IET VIRTUAL-DISK
    LUN: 4
    Capacity: 24.98GB
    Available: 24.98GB

Storage ID: 15
  Label: target 16
  Status: In Use
  Protocol: ISCSI
  Target IP: 172.20.10.81
  Target IQN: iqn.2011-09:celeros.target16
  Model: IET VIRTUAL-DISK
    LUN: 5
    Capacity: 24.98GB
    Available: 16.47GB

Active iSCSI Sessions:
tcp: [8] 172.20.10.81:3260,1 iqn.2011-09:celeros.target11
tcp: [7] 172.20.10.81:3260,1 iqn.2011-09:celeros.target16

root@secpa.cisco.com# remote-storage iscsi fsck 16
FS check completed successfully.
root@secpa.cisco.com# remote-storage iscsi list
Storage ID: 16
  Label:
  Status: Ready
  Protocol: ISCSI
  Target IP: 172.20.10.81
```

```

Target IQN: iqn.2011-09:celeros.target11
Model: IET VIRTUAL-DISK
      LUN: 4
      Capacity: 24.98GB
      Available: 9.87GB

Storage ID: 15
      Label: target 16
      Status: In Use
      Protocol: iSCSI
      Target IP: 172.20.10.81
Target IQN: iqn.2011-09:celeros.target16
Model: IET VIRTUAL-DISK
      LUN: 5
      Capacity: 24.98GB
      Available: 16.47GB

Active iSCSI Sessions:
tcp: [8] 172.20.10.81:3260,1 iqn.2011-09:celeros.target11
tcp: [7] 172.20.10.81:3260,1 iqn.2011-09:celeros.target16

```

Working with Capture Query

Capture sessions will have files associated with them. This feature will query all the files associated with a particular capture session for packets matching some search criteria.

When you run the query, it will generate pcap files that contain packets matching the search criteria. These query files will be archived within a gzipped tar file (.tgz) so the files can be easily downloaded for offline processing.



Note

The Security Packet Analyzer has a built-in decoder for inspecting the results.

- This feature is available in Packet Analyzer 2400 models. You can only query the capture session with File as Storage Type (also known as capture to disk's session).
- Capture query will not be applicable to the captured files which have been modified. For example, in **Capture > Packet Capture/Decode > Files** page, if you change the captured file name by renaming or merging, then that capture session associated capture files can no longer be used for query.
- For a captured session in running state, there will be a captured file. The query job will skip this captured file and will not perform any search/match operation. You have to do the query only after the file writing process is complete or after the capture session is stopped manually.
- **Capture > Packet Capture/Decode > Query** page can show only the last 100 queries in the History table.

Related Topics

- [Creating a New Query](#)
- [Decoding a Query](#)
- [Downloading Query Files](#)
- [Deleting a Query](#)
- [Duplicating a Query](#)

Creating a New Query

To create a new query:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Query**.
 - Step 2** Click **New Query** to create a new query.
 - Step 3** Enter information in each of the fields as appropriate. See [Table D-67](#) for descriptions of the fields.
Click **Query** to create and add the new query to the Queue table, or click **Cancel** to close the dialog box without creating a query.
Only one query job will run at a time. If multiple query jobs are submitted, the queries will be queued and will run only after the previous job is completed or canceled manually. The job in the queue will run based on the queue order.
-

Canceling a Query

To cancel a query:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Query**.
 - Step 2** Select a query from the Queue table.
 - Step 3** Click **Cancel** to cancel the query.
The canceled query will move to the history table with a status indicating that they are canceled. The canceled query will have some files associated with it which can be decoded but it will not have a .tgz archive for download.
-

Decoding a Query

To decode a query:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Query**.
 - Step 2** Select a query from the History table.
 - Step 3** Click **Decode**.
The Decoder window appears. For table descriptions see [Table D-64](#).
For detailed steps, see [Analyzing Packets in the Packet Decoder, page 4-28](#).
-

For certain queries, **Decode** button will be disabled. This is because the query result file (.pcap and .tgz) will not be available.

Downloading Query Files

You can download all of the query files for a particular query with one click. To download the query files to your computer:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Query**.
 - Step 2** Select a query from the History table.
 - Step 3** Click **Download**.

A **Save File** dialog box opens and provides a way for you to rename and save the file at a location of your choice. The files will be grouped within a zipped tar file (.tgz).

For certain queries, **Download** button will be disabled. This is because the query result file (.pcap and .tgz) will not be available.

Deleting a Query

To delete a query and its associated files:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Query**.
 - Step 2** Select a query from the History table.
 - Step 3** Click **Delete**.
 - Step 4** Click **Yes** to delete the query or **No** to allow the query to remain.
-

Duplicating a Query

You may want to create a new query that is similar to one of your previous queries. The duplicate feature makes it easy to reuse and alter the parameters from a query in the History table.

To duplicate a query:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Query**.
 - Step 2** Select a query from the History table.
 - Step 3** Click **Duplicate**.
The New Query dialog box appears, See [Table D-67](#).
 - Step 4** Modify the required query parameters.
 - Step 5** Click **Query** to add a new query to the Queue table, or click **Close** to close the dialog box without duplicating a query.
-

Inspecting Packet Decode Information for Suspicious Traffic

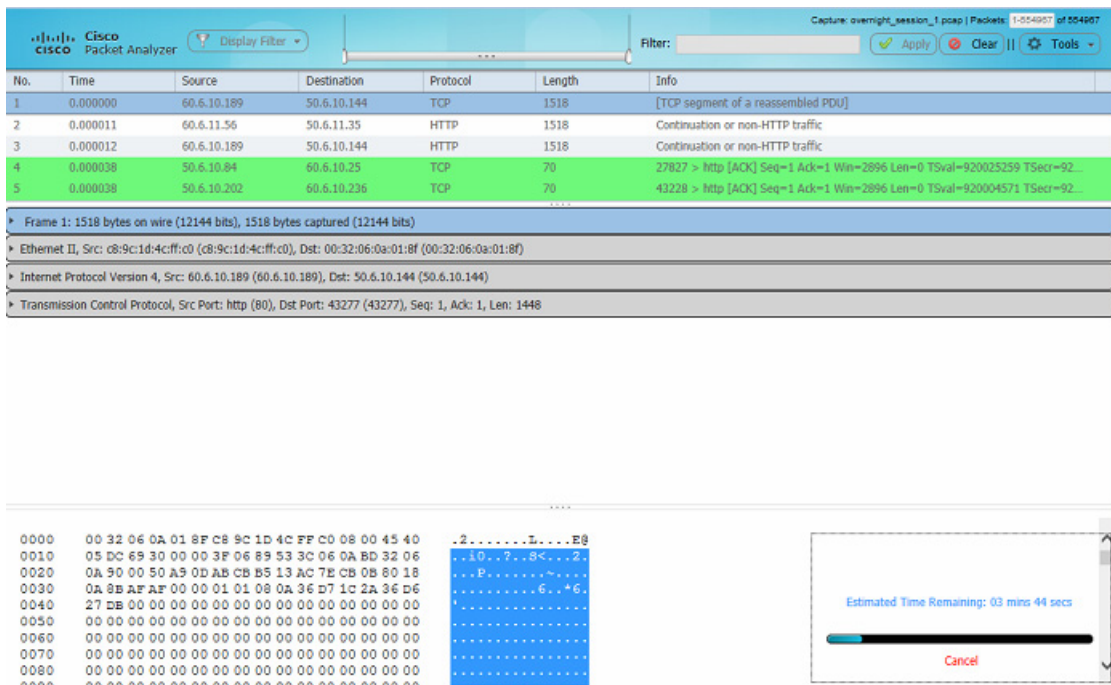
After you have captured some traffic data packets, you can use the Packet Analyzer packet decoder to view the packet contents and inspect for suspicious traffic.

This section includes the following sections:

- [Analyzing Packets in the Packet Decoder, page 4-28](#)
- [Filtering Packets Displayed in the Packet Analyzer Packet Decoder, page 4-29](#)
- [Viewing Detailed Protocol Decode Information, page 4-30](#)
- [Understanding the Packet Analyzer Packet Decoder, page 4-31](#)

Analyzing Packets in the Packet Decoder

Figure 4-8 *Packet Decoder Window*



Note

To use these decode features, you must be capturing to memory with the no rotate option selected. Otherwise, captures must be paused or stopped. For detailed descriptions about the features in this window, see [Understanding the Packet Analyzer Packet Decoder](#).

To inspect packet decode information for suspicious traffic:

- Step 1** Choose **Capture > Packet Capture/Decode > Sessions** and create a capture session. If you already have a capture session choose **Capture > Packet Capture/Decode > Files**.
- Step 2** Choose a capture session or file, and then click **Decode**. The Packet Decoder window displays. See [Figure 4-8](#). For table descriptions see [Table D-65](#).

- Step 3** To quickly filter on a key word or phrase, for example rtp to focus on voice quality, enter the word in the Filter text box (see [Figure 4-8](#)). The window refreshes displaying only data that includes the filtered information.
- Step 4** To filter packet data based on multiple filters, click **Display Filter** and enter your options in the window, then click **Apply**. This action displays only the distribution of the packets that match your filter. For detailed steps, see [Filtering Packets Displayed in the Packet Analyzer Packet Decoder, page 4-29](#).
- Step 5** To save filters for future use, click **Save Display Filters** on the Display Filter window. You can also edit or remove existing filters as needed.
- Step 6** To view the packet capture flow and focus in on a specific time interval or area of interest click on the slider in the Packet Histogram and move the left or right cursors to zoom in (see [Figure 4-8](#)). To pan this filtered data, click and hold the slider while moving it inside the histogram. This provides a visual of packet capture flow and enables you to navigate through the packet list.
- Step 7** To toggle
- between a one and two-column layout view, choose **Tools > Toggle Layout**.
 - between the Packet Histogram and the packet paging controls, choose **Tools > Show ...**
- Step 8** To disable the default colors in the packet window, choose **Tools > Disable Protocol Coloring**.
- Step 9** To review capture file information, choose **Tools > Capture Info**.
- Step 10** To save the current filtered packet info displayed on this page, choose **Tools > Save Filtered Packets**. Only visible when filters are in use. Saves to memory or to the capture file based on the options in your Capture Sessions window. See [Configuring Capture Sessions, page 4-6](#).
- Step 11** To make the font size larger or smaller for the hex data pane, hover over the top-right corner of the pane to see the enlarge option. To increase the font, select the **A+** or to decrease it select the **A-**.
- Step 12** Use the Tools menu to perform validation tasks—options have limited support. Options include:
- TCP Checksum Validation check box—filter on TCP in the decode window and use the TCP pane to verify that the checksum has been validated.
 - UDP Checksum Validations check box—filter on UDP in the decode window and use the UDP pane to verify that the checksum has been validated.
 - IP Host Name Resolution—perform global host name resolution for Packet Analyzer. Synchronizes with the Administration preferences.
- Step 13** Use **Decode As** option to temporarily force specific tcp and /or udp ports to be decoded as the specific protocols as specified by the user. This is useful for custom protocols that use user defined ports or the same ports may be used by more than one protocols
- Step 14** To view packet details including packet range displayed, data port, and number of filtered packets, see the heading in the upper right corner of the Packet Analyzer window.
-

Filtering Packets Displayed in the Packet Analyzer Packet Decoder

To filter packets based on multiple options for display in the Packet Analyzer Packet Decoder:

- Step 1** From the Packet Analyzer Packet Decoder, click **Display Filter**. The Packet Analyzer - Display Filter Window displays.

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/Host** address filters on IP address.
 - **MAC** address filters 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 traveling in both directions.
- Define a **Protocol Filter**:
 - Click **Match any (or)** to display packets that match any of the protocols or fields.or
 - Click **Match all (and)** to display packets that match all of the protocols or fields.
 - Choose a protocol from the **Protocols** list.



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

- Choose a protocol field from the Fields list, then specify the field value if applicable.

Step 3 To add more protocol filters, click the + sign.

Step 4 To delete a defined Protocol Filter, click the - sign.

Step 5 Click **OK** to apply the filter and close the window or **Apply** to apply the filter and keep the window open.

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, Packet Analyzer lists the protocol as *skinny*, not SCCP.

**Tip**

- Protocols are color coded both in the Packet Browser and the Protocol Decode pane.
- Choose 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.

Understanding the Packet Analyzer Packet Decoder

The Packet Analyzer, also known as the packet decoder, uses two levels of packet analysis: basic and full. Because preparing a large capture file for full analysis can take a long time, Packet Analyzer automatically chooses which level to use based on your filtering complexity. This allows you to browse your captured packet data more quickly without having to wait for analysis.

When you select a capture file to analyze for the first time, Packet Analyzer limits some of the more complex display filters you can use. For example, you can filter using protocol identifiers such as TCP, UDP, SDP, and SIP which allow the packet decode to display more quickly than an advanced filtering selection.

If you enter more advanced filters (such as those with and/or logic operators on the protocol field), Packet Analyzer automatically begins the full analysis of the capture file and then applies your complex filter to display the results. For example, if you filter using 'ip.src==192.168.1.1 && tcp.dstport==80', the Packet Analyzer starts the full analysis and displays it only after the results have been filtered.

Understanding the Packet Analyzer Packet Decoder Window and Browser Pane

The Packet Analyzer Packet Decoder window shows three views of a packet:

- a summary line briefly describes the packet type
- the protocol field of interest can be shown and analyzed in the portion of the window directly below the summary line
- a hexadecimal dump shows exactly what the packet looks like when it goes across the wire.

There are many unique features in the Packet Analyzer Packet Decoder decode window; for example, it can assemble all the packets in a TCP conversation and highlight the ASCII data in that conversation. You can use the expanded display filter functionality to allow you to view more focused data.

[Figure 4-8](#) is an example of the Packet Analyzer Packet Decoder window.

You can perform the following tasks in the Packet Analyzer window:

- Show Packet histogram display the number of packets over a specific time range. This provides a feel of the packet flow for the capture. You can use the histogram selector control to navigate through the packet list as well. You can apply a display filter to make the histogram show the distribution of the packets that match the applied filter. Can set time range and move across histogram. Firefox is faster than IE performance with this feature.
- Toggle to Show Packet Paging Controls displays the buffer divided into pages.
- Toggle layout changes how the three content panes in the decoder are arranged.

- Display Hex data font size by hovering over two buttons in the top right corner of the hex data content pane of the decoder. You can increase or decrease the font size of the contents.
- Display the current range of packets in the packet list by selecting the Packet range button. You can also enter the range of packets to view.
- Use the Display Filter button to display Saved Display Filters and Manage Display Filters windows.
- Alter Protocol coloring. You can map custom colors to specific protocols in this release. Default colors
- Use the Tools menu—options have limited support. Options include:
 - TCP Checksum Validation check box—filter on TCP in the decode window and use the TCP pane to verify that the checksum has been validated.
 - UDP Checksum Validations check box—filter on UDP in the decode window and use the UDP pane to verify that the checksum has been validated.
 - IP Host Name Resolution—perform global host name resolution for Packet Analyzer. Synchronizes with the Administration preferences.
- Use Decode As option to temporarily force specific tcp and /or udp ports to be decoded as the specific protocols as specified by the user.
- Display Filter input field to manually enter display filters.

Customizing Display Filters

Use custom display filters to create and save customized filters to use in the Packet Analyzer decode window to limit which packets are displayed.

Packet Analyzer supports most software display filters with the following exceptions:

- Filters using Perl Regular Expressions. For example:
`http.request.uri matches "gl=se$"`
- Filters on a protocol payload (a protocol section in a packet). For example:
`udp[8:3]==81:60:03`

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

- [Creating Custom Display Filters, page 4-32](#)
- [Editing or Deleting Custom Display Filters, page 4-35](#)

Creating Custom Display Filters

To create custom display filters:

-
- Step 1** Choose **Capture > Packet Capture/Decode > Sessions**.
The Hardware Filters box is displayed at the bottom of the page.
 - Step 2** Click **Create**. The Hardware Filters Dialog box displays. See [Table D-63](#).
 - Step 3** Enter information in each of the fields as appropriate.
 - Step 4** Do one of the following:
 - To create the filter, click **Submit**.

- To cancel filter creation, click **Cancel**.

Tips for Creating Custom Decode Filter Expressions

You can construct custom decode filter expressions using the following logical and comparison operators listed in [Table 4-3](#).

Table 4-3 Logical and Comparison Operators

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

To group subexpressions within parentheses, use the fields in [Table D-62](#) to help you add filter expressions.

Examples of Custom Decode Filter Expressions

[Table 4-4](#) provides some examples of basic Packet Analyzer display filters you can use to filter on application types.

Table 4-4 Basic Packet Analyzer Display Filters (Limited to Application Types)

Filter	Meaning
tcp	Find all TCP-based applications
udp	Find all UDP-based applications
! eth	Find all packets other than Ethernet
tcp and not vlan	Find all TCP traffic NOT running over vlan
http	Find all src/dst HTTP application packets (may be not standard port 80 if different application 'decode as' port specified; e.g. 'tcp.port==8080,http')
ftp http	Find either ftp or http packets
not tcp	Exclude all TCP packets
! tcp	Exclude all TCP packets
! (ftp http)	Exclude all FTP and HTTP packets

[Table 4-5](#) provides some examples of complex Packet Analyzer display filters.

Table 4-5 Compound Packet Analyzer Display Filters

Filter	Meaning
tcp.port eq 80	Find all src/dst HTTP packets on standard HTTP port 80
ip.addr == 192.168.1.0/24	Find all packets in Class C network (subnet)
tcp.flags.reset == 1	Find all TCP resets
tcp.window_size == 0 && tcp.flags.reset != 1	Src is instructing dst to stop sending data (TCP buffer full)
Ipv6.addr == ::1	Correct statement with IPv6 label and IPv6 address.

Table 4-6 provides some examples of protocol field hexbyte filters.

Table 4-6 Protocol Field Hexbyte Filters

Filter	Meaning
eth.src==00:3c:06:0a:02:68	Find source MAC
eth.dst==00:3c:06:0a:02:68	Find destination MAC
eth.addr==00:3c:06:0a:02:68	Find source or dest MAC
! (eth.addr==00:3c:06:0a:02:68)	Find all MAC except specific address
eth.addr contains 00:3c	Find bytes in any protocol field subrange

Table 4-7 provides some examples of protocol field hexbyte subrange filters.

Table 4-7 Protocol Field Hexbyte Subrange Filters

Filter	Meaning
eth.addr[0:2]==00:3c	Find specific subrange in MAC
eth.addr[1:3]==3c:06:0a	Find specific subrange in MAC

Table 4-8 provides some examples of hexbyte data representations syntax.

Table 4-8 Hexbyte Data Representations (Syntax)

Filter	Meaning
eth.dst == ff:ff:ff:ff:ff:ff	Hexbyte separators can be colons
eth.dst == ff-ff-ff-ff-ff-ff	Hexbyte separators can be dashes
eth.dst == ffff.ffff.ffff	Hexbyte separators can be dots (one or two bytes)

**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 or Deleting Custom Display Filters

To edit custom display filters:

-
- Step 1** From the Packet Analyzer Packet Decoder, choose **Display Filters**.
 - Step 2** To edit a filter, choose the filter to edit then click **Edit**.
 - Step 3** Change the information in each of the fields as appropriate.
 - Step 4** To delete a filter, choose the filter to delete from the Hardware Filters Data Port 1 or Data Port 2 pane, then click **Delete**.
-

