Quick Card

Capturing and Analyzing Packets

Before testing

Before capturing packets, consider the following:

What is captured? All received traffic (test traffic, control plane traffic, and live traffic) that satisfies the user-specified filter criteria can be captured on all supported interfaces. All transmitted traffic (test traffic, control plane traffic, and life traffic) that satisfies the user-specified capture criteria can be captured for all supported interfaces *up to 1 Gigabit Ethernet*. When capturing transmitted traffic from a 10 Gigabit Ethernet interface, *only control plane traffic is captured*. Ethernet frames ranging from 4 to 10000 bytes long can be captured, but the 4 byte Ethernet FCS is not stored in the capture buffer.

How much can be stored in the buffer? You can specifying a buffer size ranging from 1 MB to 256 MB. You can also indicate that the instrument should stop capturing packets when the buffer is full, or overwrite the oldest packets in the buffer with new captured packets in 1 MB increments.

Why use packet slicing? You can tell the instrument to capture only the first 64 or 128 bytes of each packet, which allows you to analyze the most important data (carried in the packet headers), and to capture and store more packets in the buffer.

Configuring the test

Before capturing packets, you specify filter settings (for received packets), and capture settings. When capturing packets in Monitor or Terminate mode, you must use Port 1 for your test. If you are capturing packets in Dual Through mode, both ports can be used.

Configuring a capture for a large buffer (for example, 256 MB), with small packets (for example, 46 byte ping packets), will take a long time to fill the buffer. Configuring the capture for a small buffer with large packets will fill the buffer quickly.

Step 1 On the Main screen, use the **Test** menu to select the application for the interface you are testing.

Step 2 Select the Capture tool bar, then enable the capture feature.

Step 3 Select the **Setup** soft key, and then do the following:

a Select the **Filters** tab, and then do one of the following:

- If you launched a layer 2 application, select **Ethernet**, and then specify the settings that capture the received traffic that you want to analyze.

- If you launched a layer 3 or layer 4 application, and you want to specify *basic* filter information, select **Basic**, and then specify the **Traffic Type** and the **Address Type** carried in the received traffic you want to capture.

- If you launched a layer 3 or layer 4 application, and you want to specify *detailed* filter information, select **Basic**, and then set the filter mode to **Detailed**.

Use the **Ethernet**, **IP**, and **TCP/UDP** selections in the pane on the left to display the filter settings for your particular test, andthenspecifythesettingsthatcapturethereceivedtraffic that you want to analyze.

b Select the **Capture** tab, then specify the following settings:

Setting	Parameter
Capture buffer size (MB)	Specify a size ranging from 1 to 256 MB in a 1 MB increment. The default buffer size is 16 MB.
Capture frame slicing	If you want to capture the first 64 or 128 bytes of each frame (and ignore the rest of the frame), select 64 or 128; otherwise, select None. If you select None (the default), the entire frame is captured.
When capture buffer is filled	If you want to overwrite the oldest packets with new packets when the buffer becomes full, select **Wrap Capture**; otherwise, select **Stop Capture**.
Include frames from Traffic tab	If you want to capture transmitted frames (the traffic load which is specified on the Traffic tab), select **Yes**.

Step 4 Select the **Results** soft key to return to the Main screen.

Connecting to the circuit

Step 1 Using a fibre scope, inspect the cables and components that you intend to use to connect your instrument to the circuit. If necessary, clean them.

Step 2 Verify that your instruments are connected properly for the test.

When capturing packets, you can connect to the circuit using an end-to-end configuration or a loopback configuration.

Starting the test

Step 1 Do the following:

- If you are testing on an optical circuit, turn the laser on.
- If you are capturing transmitted or looped back traffic, select **Start Traffic**.

Step 2 Select the **Capture** toolbar, and then do the following:

a Select **Start Capture**. A message appears in the message bar indicating that the capture has started, and the action key states **Capture Started**.

b If you want to capture packets that shows how the traffic is impacted by various events, use the buttons on the **Actions**, **Errors**, and **Fault Signaling** tool bars to insert the events into the transmitted traffic stream.

Step 3 If you want to stop capturing packets before the buffer is full (for example, after the instrument has transmitted and received a certain number of frames), select the **Capture Started** action key. The action key turns grey, and a message appears in the message bar indicating that the capture is complete.

Saving or exporting captured packets

You can safe captured packets in the buffer to the internal USB drive, or export them to an external USB drive. You can save the entire buffer, or just part of the buffer. You can also optionally compress the data. Many factors contribute to the length of time it takes to save a captured file, but the key factors are the packet density and the capture size.

Step 1 On the Main screen, select **Save Capture Buffer**, then select a location, and then specify the other save settings (file name, whether to compress the file, and whether to launch Wireshare after saving.

Step 2 Select the **Save** button at the bottom of the dialog box.

A dialog box appears above the Main screen showing the percentage of the buffer that has been saved. When buffer is saved, the box closes. If you indicated that you wanted Wireshark to launch immediately after saving the buffer, the Wireshark® application appears.

Analyzing packets using Wireshark®

After saving the packets in the capture buffer (to a PCAP file), you can analyze them in detail on the instrument using the Wireshark® protocol analyzer. *Files exceeding 16 MB should not be analyzed on the instrument*; large files should be exported for analysis on another device. If you attempt to analyze a file with more than 50,000 packets, the instrument will alert you that the file should be exported for analysis.

IMPORTANT: Wireshark® Support

JDSU is distributing Wireshark® on the instrument under the GNU General Public License, version 2. It is not a JDSU product. For technical support, go to the product website at www.wireshark.org.

Step 1 On the **Capture** toolbar, select the **Wireshark** action key. The Open Capture File dialog box appears.

Step 2 Navigate to and select the file you want to analyze. The Wireshark® splash screen appears, then a small dialog box appears while the application loads the packets in the file you selected.

Step 3 After the packets are loaded, a screen similar to the one in Figure 3 appears.

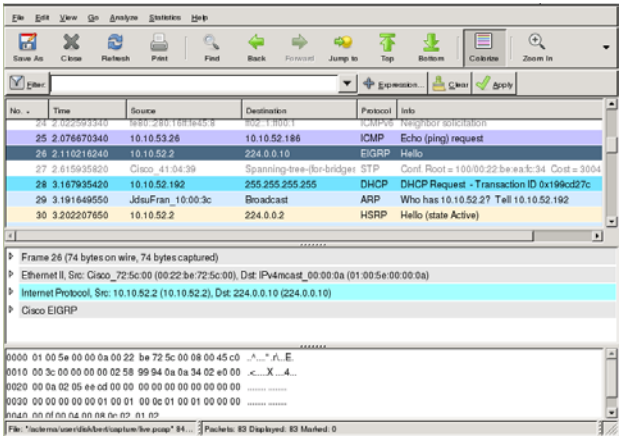

Figure 3 Sample Wireshark® screen

Step 4 Use the controls at the top of the screen to locate and evaluate the packets.

For technical support and product documentation, go to www.wireshark.org.

Analyzing packets using J-Mentor

If you want a summarized analysis of the packets, you can use the J-Mentor utility provided on your instrument. The utility is only available for analysis of packets captured on 10/100/10000 Mbps electrical, 100M optical, and 1G optical circuits. J-Mentor can only be used to analyze PCAP files with 50,000 or less packets.

Step 1 On the Capture toolbar, select the **J-Mentor** action key. The Open Capture File dialog box appears.

Step 2 Specify the link bandwidth in Mbps (this is the line rate at which you captured the traffic). Then, navigate to and select the file you want to analyze.

Step 3 If you want to observe key details for the PCAP file, select **Get PCAP Info**. This is wise if you suspect the file might exceed the 50000 packet limit for analysis on your instrument. If it does exceed the limit, a message appears instructing you to export the file for analysis.

Step 4 Select **Analyze**. The utility immediately checks for the possibility of retransmissions of packets, high bandwidth utilization, top talkers, detection of half duplex ports, and ICMP frames. After analyzing the packets, a summary screen appears indicating whether issues were found at layers 1 and 2 (the physical and Ethernet layer), layer 3 (the IP layer), or layer 4 (the TCP/UDP layer). Green indicates everything was fine at a particular layer; Red indicates that there were issues identified at that layer.

Step 5 Use the **Details** buttons to observe detailed results for each layer. For example, if you want to observe a graph of the network utilization, or a list of all IP conversations, press the **Details** button for Layer 1 / 2.

Step 6 Select **Exit** to return to the Main screen.

Related information

Use this Quick Card in conjunction with the Getting Started Manual and Testing Manual that shipped with your instrument.

Technical assistance

For the latest TAC information, go to www.jdsu.com or contact your local sales office for assistance. Contact information for regional sales headquarters is listed at the bottom of this Quick Card.

Test and Measurement Regional Sales

NORTH AMERICA	LATIN AMERICA	ASIA PACIFIC	EMEA	www.jdsu.com
TEL: 1 855 ASK JDSU FAX: +1 301 353 9216	TEL:+1 954 688 5660 FAX:+2 954 354 4668	TEL:+852 2892 0990 FAX:+852 2892 0770	TEL:+49 7121 86 2222 FAX:+49 7121 86 1222	