

# Capturing and Viewing Packets with the J-Web Interface

You can use the J-Web packet capture diagnostic tool when you need to quickly capture and analyze router control traffic on a device. Packet capture on the J-Web interface allows you to capture traffic destined for or originating from the Routing Engine. You can use J-Web packet capture to compose expressions with various matching criteria to specify the packets that you want to capture. You can either choose to decode and view the captured packets in the J-Web interface as they are captured, or save the captured packets to a file and analyze them offline using packet analyzers such as Ethereal. J-Web packet capture does not capture transient traffic.

Alternatively you can use the CLI `monitor traffic` command to capture and display packets matching a specific criteria. For details, see [Using the monitor traffic Command](#).

To capture transient traffic and entire IPv4 data packets for offline analysis, you must configure packet capture with the J-Web or CLI configuration editor. For details, see [Configuring Packet Capture](#).

This section contains the following topics:

- [Using J-Web Packet Capture](#)
- [Packet Capture Results and Output Summary](#)

## Using J-Web Packet Capture

To use J-Web packet capture:

1. Select **Troubleshoot>Packet Capture**.
2. Enter information into the Packet Capture page ([Figure 29](#)) as described in [Table 154](#).

The sample configuration in [Table 154](#) captures the next 10 TCP packets originating from the IP address 10.1.40.48 on port 23 and passing through the Gigabit Ethernet interface ge-0/0/0.

3. To save the captured packets to a file, or specify other advanced options, click the expand icon next to Advanced options, and enter information as described in [Table 154](#).
4. Click **Start**.

The captured packet headers are decoded and displayed in the Packet Capture display (see [Figure 30](#)).

[Table 155](#) summarizes the output fields of the display.

5. Do one of the following:
  - To stop capturing the packets and stay on the same page while the decoded packet headers are being displayed, click **Stop Capturing**.
  - To stop capturing packets and return to the Packet Capture page, click **OK**.

Figure 29: Packet Capture Page

Diagnose > Packet Capture

Packet Capture

The packet capture diagnostic tool allows inspection of router control traffic (not transient traffic). The summary of each decoded packet is displayed as it is captured. Captured packets are written to a PCAP file which can be downloaded.

Interface

default

Addresses

Add/Remove

Add

Direction

any

Type

host

Address

Detail level

brief

Protocols

Add/Remove

Add

Protocol

tcp

Packets

10

Ports

Add/Remove

Add

Direction

any

Port

Advanced options

Absolute TCP Sequence

Layer 2 Headers

Non-Promiscuous

Display Hex

Display ASCII and Hex

Header Expression

Packet Size

Don't Resolve Addresses

No Timestamp

Write Packet Capture File

Start

Table 154: Packet Capture Field Summary

Field	Function	Your Action
Interface	<p>Specifies the interface on which the packets are captured.</p> <p>If you select <b>default</b>, packets on the Ethernet management port 0, are captured.</p>	<p>From the list, select an interface—for example, ge-0/0/0.</p>

Detail level—Specifies the extent of details to be displayed for the packet headers. From the list, select **Detail**.

Figure 30 shows J-Web packet capture output from router1, with the level of detail set to brief. Table 155 summarizes the output in the packet capture display.

Figure 30: Packet Capture Results Page

- **Brief**—Displays the minimum packet header information. This is the default.
- **Detail**—Displays packet header information in moderate detail.
- **Extensive**—Displays the maximum packet header information.

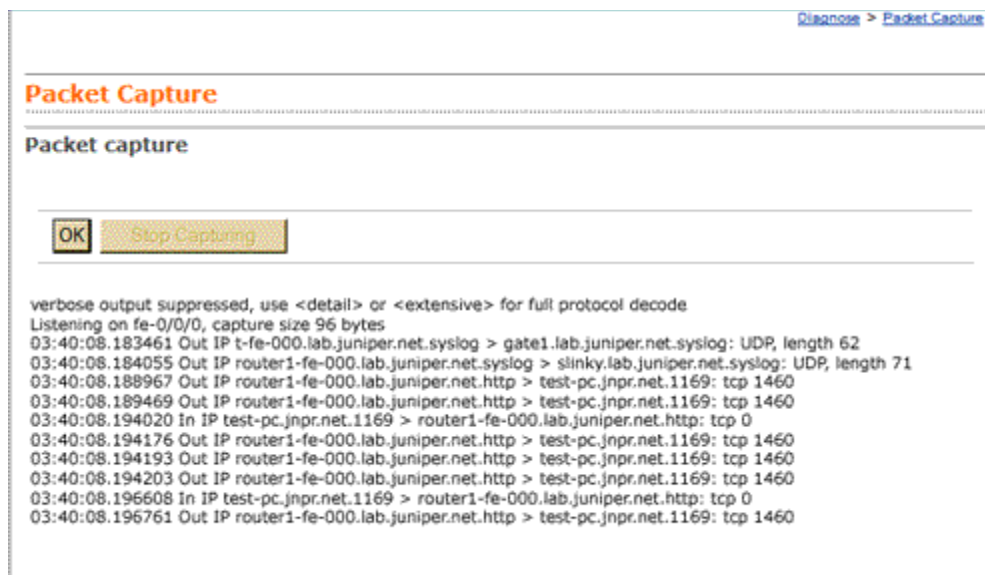


Table 155: J-Web Packet Capture Results and Output Summary

Field	Description
<i>timestamp</i>	Time when the packet was captured. The timestamp 00:45:40.823971 means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds.  <b>Note:</b> The time displayed is local time.
<i>direction</i>	Direction of the packet. Specifies whether the packet originated from the Routing Engine (Out), or was destined for the Routing Engine (In).
<i>protocol</i>	Protocol for the packet.  In the sample output, IP indicates the Layer 3 protocol.
<i>source address</i>	Hostname, if available, or IP address and the port number of the packet's origin. If the Don't Resolve Addresses check box is selected, only the IP address of the source is displayed.  <b>Note:</b> When a string is defined for the port, the packet capture output displays the string instead of the port number.
<i>destination address</i>	Hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port are displayed.  <b>Note:</b> When a string is defined for the port, the packet capture output displays the string instead of the port number.

[Contents](#) [Prev](#) [Next](#) [Index](#) [Report an Error](#)

[Site Map](#)  
[RSS Feeds](#)

[Careers](#)

[Accessibility](#)

[Feedback](#)

[Privacy & Policy](#)

[Legal Notices](#)

Copyright© 1999-2010 Juniper Networks, Inc.