Working with Packet Capture

In this section:

- Enabling Packet Capture
- Starting Packet Capture
  - Interface - Field Definitions
  - Protocol - Field Definitions
  - Other Options - Field Definitions
- Stopping Packet Capture
- Downloading Capture Files
- Moving Internal or ASM Capture Files
- Packet Capture Limitations

The SBC performs Packet Capture using 'tcpdump' and allows the captured file to be downloaded. The following section describes how to capture packets and download them.

Caution

Performing a Media packet capture with no host filters or against hosts terminating multiple calls can impact traffic and cause current or future calls to fail or experience other problems.

Performing a long duration capture which is outside of a maintenance window can adversely impact traffic, and should be avoided when possible.

For SBC 1000

You must insert either an ASM or external USB into the SBC 1000 in order to save packet capture files. Without this, packet capture is not allowed due to available space limitations.

For SBC 2000

Sonus recommends that you insert either an ASM or external USB into the SBC 2000 in order to save packet capture files; otherwise only a small capture session is permitted due to available space limitations on the internal flash.

Enabling Packet Capture

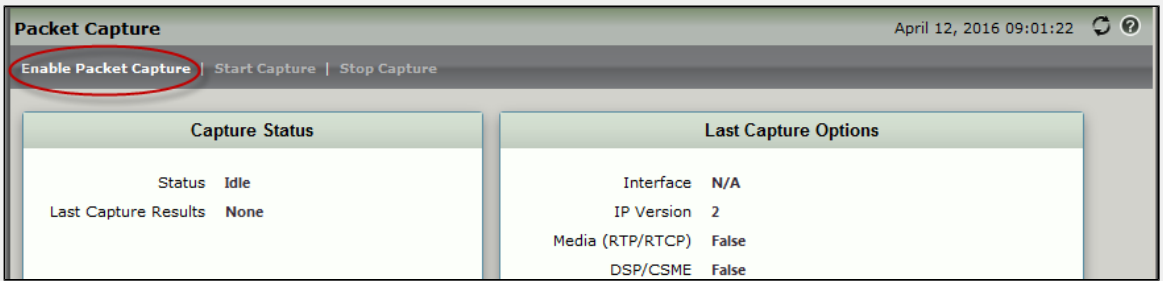
The Packet Capture feature is intended for **short** duration packet captures. For that reason, a maximum duration of 120 minutes (2 hours) is permitted.

The **Enable Packet Capture** option (available from the **Packet Capture** menu bar) enables the packet capture ability in the **SBC**.

To enable packet capture:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation bar, select **Sonus TAC Troubleshooting > Packet Capture**.
3. From the menu bar, click **Enable Packet Capture**.

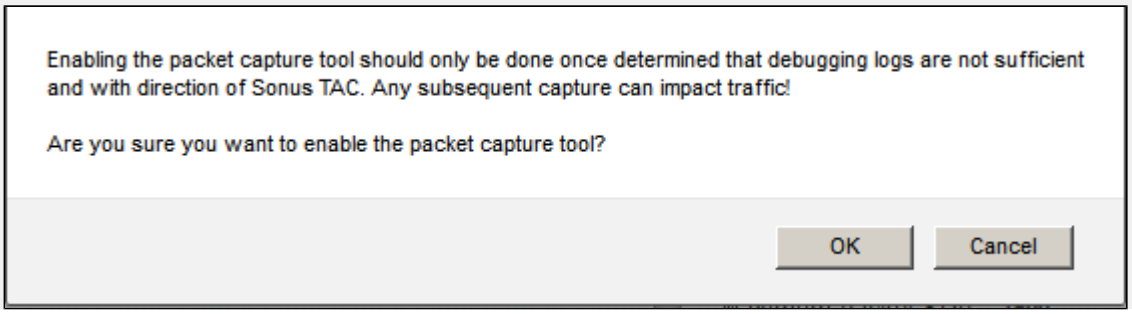
Figure 1: Enable Packet Capture



4. At the Warning note, click **OK.**

> Enable Packet Capture only under the direction of Sonus TAC.

Figure 2: Enable Packet Capture - Warning Message



Packet Capture is enabled. Refer to Start Packet Capture.

Starting Packet Capture

Packet Capture must be enabled before capturing packets. Refer to Enable Packet Capture.

To view Alarm/Event history logs for Packet Capture, access the **Diagnostics** tab and click **Logs > Alarm/Event History.**

To capture T.38 Fax, Sonus recommends enabling RTP Media and adding the Host 1 and Host 2 IP addresses of the next hop neighbor in Media SDP.

The **Start Capture** option (available from the **Packet Capture** menu bar) enables the **SBC** to capture packets.

To start capturing packets:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation bar, select **Sonus TAC Troubleshooting > Packet Capture**.
3. From the menu bar, click **Start Capture**.

Figure 3: Start Capture

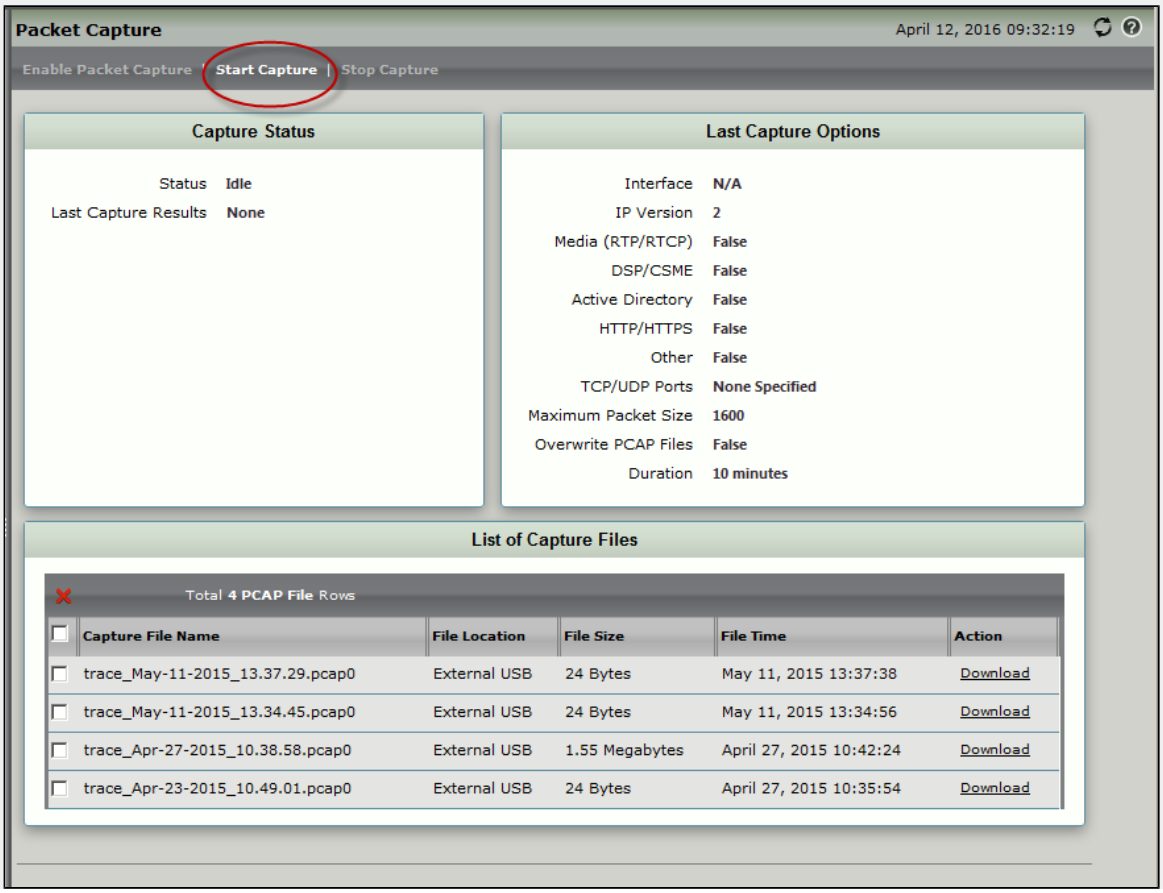
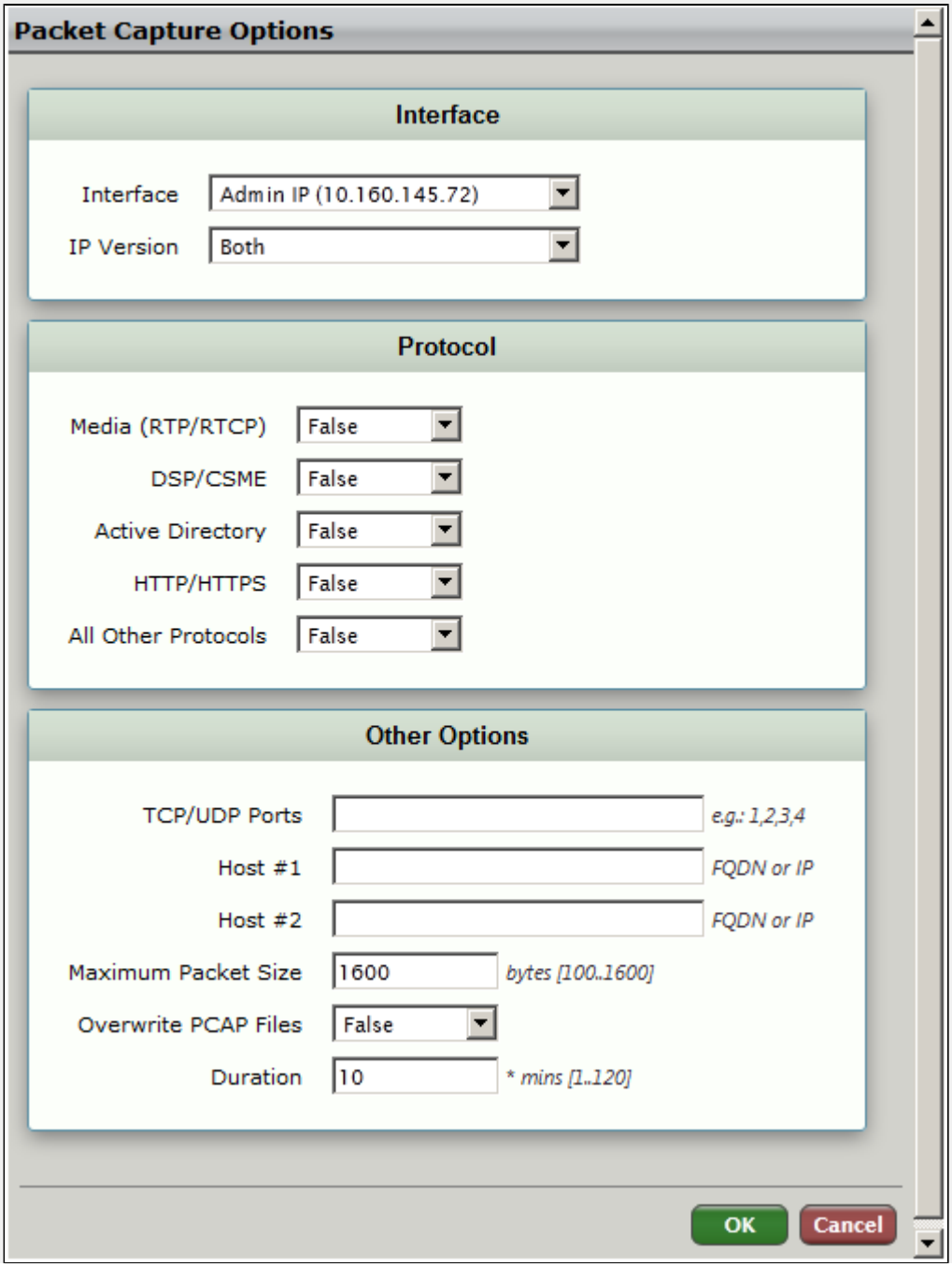


Figure 4: Packet Capture Options



4. Select the network interface (including IP Version) from which the packets will be captured.

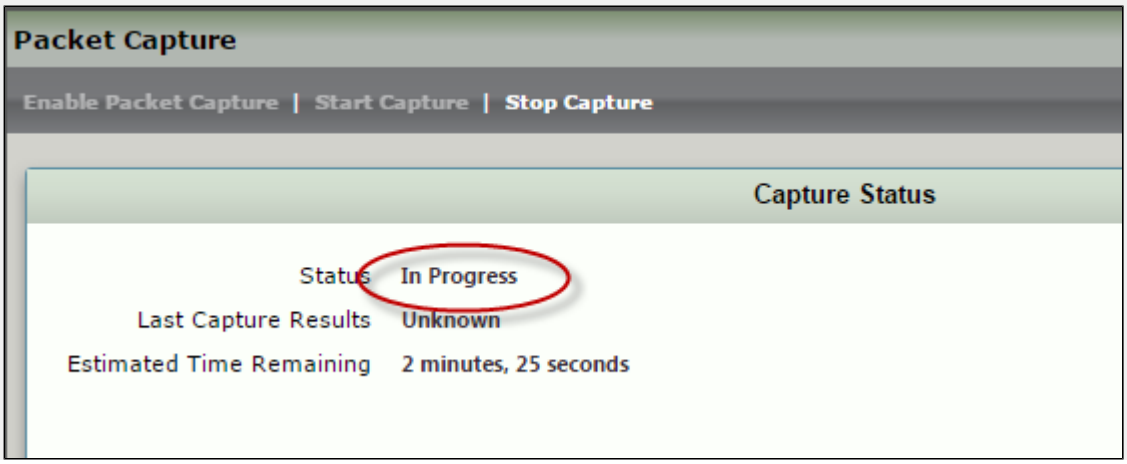
5. Select an protocol(s) from which to capture the packets.

6. Configure any relevant information for the **Other Options** sections. For details, refer to Field Definitions.

7. Click **OK**.

   The Packet Capture status turns to **In Progress**.

Figure 5: Packet Capture in Progress



Interface - Field Definitions

Interface

Specifies the network interface from which the packets will be captured.

IP Version

Specifies the IP version of the interface from which the packets will be captured. Valid selections: **IPv4**, **IPv6** or **Both**.

Protocol - Field Definitions

Media (RTP/RTCP)

This field applies to SBC 1000/2000 only.

Specifies whether or not to capture RTP/RTCP Packets.

- **Default:** False

DSP/CSME

This field applies to SBC 1000/2000 only.

Specifies whether or not to capture DSC/CSME Packets.

- **Default:** False

Active Directory

Specifies whether or not to capture LDAP Packets.

- **Default:** False

HTTP/HTTPS

Specifies whether or not to capture HTTP/HTTPS Packets.

- **Default:** False

All Other Protocols

Specifies whether or not to capture all other packet types not defined above.

- **Default:** False

Other Options - Field Definitions

TCP/UDP Ports

Specifies the port or ports used to capture packets. A maximum of four comma separated port numbers may be specified.

- **Range:** 1 - 65535

Host #1

Specifies a unique host from which to capture packets. Host is specified by IPv4 Address or FQDN.

- **Range:** 1 - 256 ASCII characters

Host #1 Direction

The following field is only visible if an address has been entered in Host #1.

Specifies the whether the captured packets are being sent to the host or received from the host, or both.

- **Default:** Transmit and Receive

Host #2

Specifies a unique host from which to capture packets. Host is specified by IPv4 Address or FQDN.

- **Range:** 1 - 256 ASCII characters

Host #2 Direction

The following field is only visible if an address has been entered in Host #2.

Specifies the whether the captured packets are being sent to the host or received from the host, or both.

- **Default:** Transmit and Receive

Maximum Packet Size

Specifies the maximum size of the individual packets to be captured.

- **Range:** 100 - 1600 Bytes
- **Default:** 1600

Overwrite

Specifies whether or not the SBC overwrites capture files in round robin fashion or not when the maximum file size has been reached.

- **Default:** False

Duration

> A maximum duration of 120 minutes (2 hours) is permitted for packet capture.

Specifies the duration of the capture in minutes. The maximum value represents 2 hours.

- **Range:** 1 - 120
- **Default:** 10

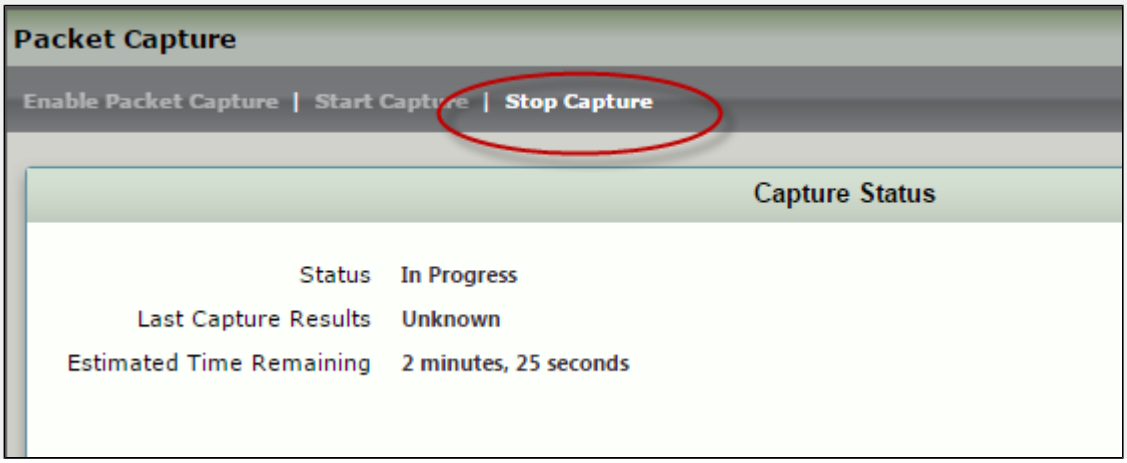
Stopping Packet Capture

The **Stop Packet** capture feature is optional; this option is used to stop the packet capture early (before the packet capture reaches the time limit set in the Duration field).

To stop capturing packets:

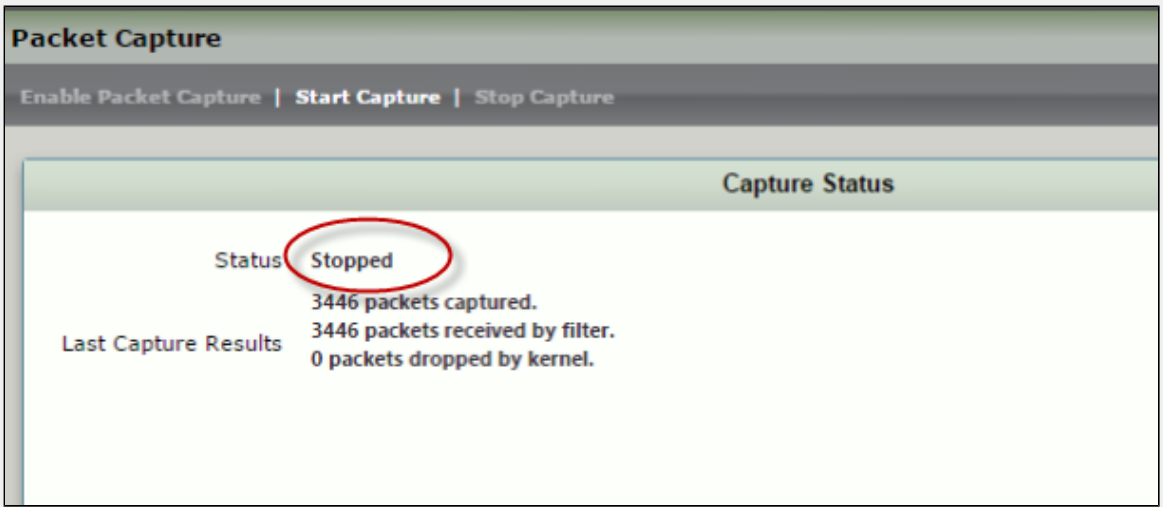
1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation bar, select **Sonus TAC Troubleshooting > Packet Capture**.
3. From the menu bar, click **Stop Capture**.

Figure 6: Stop Capture Option



The Packet Capture stops.

Figure 7: Packet Capture Stops



Downloading Capture Files

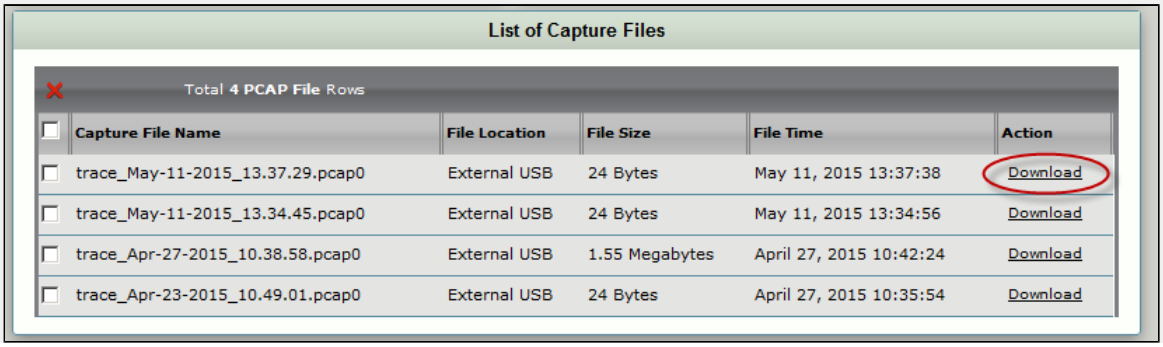
Once the packet capture has stopped, the captured file will appear in the table **List of Captured Files.**

> **To Stop Packet Capture Early**
> If you need to stop the packet capture early, from the menu bar, click **Stop Capture**.

To download captured files:

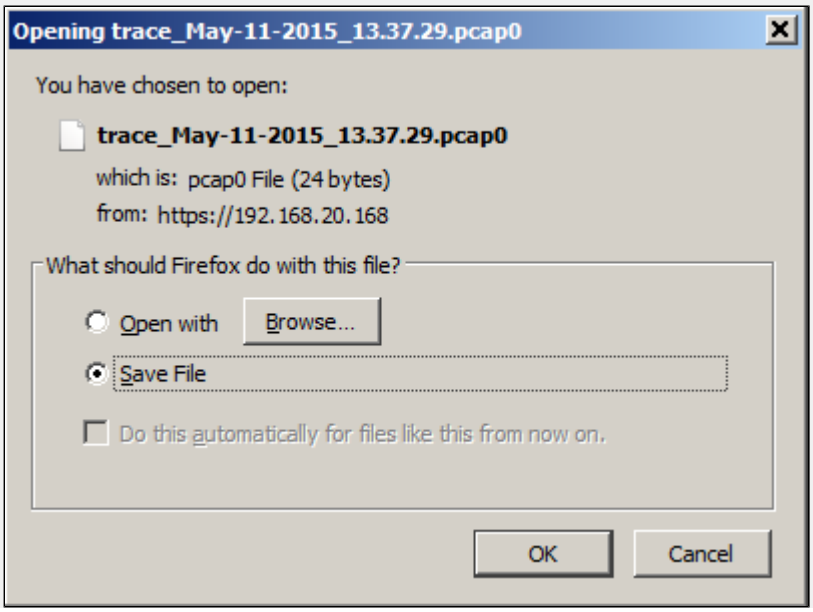
1. From the **List of Capture Files** table, next to the desired file, click **Download**.

Figure 8: Capture Files



2. Select the appropriate location to save the file. Click **OK.**

Figure 9: Save File



Note
Only one packet capture can be downloaded at a time. Depending on the size of the file and network connection, a download can take several minutes.

Moving Internal or ASM Capture Files

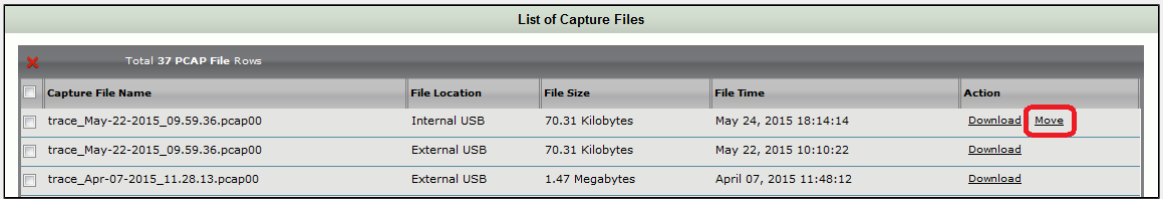
If the file location for the packet capture is Internal or an ASM, and the system has an external USB present and available, an additional option, **Move**, will appear under the Action column. The Move action relocates the packet file to the external USB, which can then be removed and taken to a PC.

The packet capture can only be saved on the internal flash for SBC 2000.

To move captured files:

1. From the **List of Capture Files** table, next to the desired file, click **Move.**

Figure 10: List of Capture Files



Packet Capture Limitations

The following lists the limitations of Packet Capture.

Size Limitations

1. An individual Packet Capture file is limited to 350 MiB in size. After the 350 MiB limit has been reached, a new file will be created to continue the packet capture.

2. A Packet Capture session size limit is dependent on whether or not
    a. 30 GiB is less than the available storage space minus (-) 30%
       Or
    b. Available storage space minus (-) 30% is less than 30 GiB

3. For SBC 1000, if there is no external USB or ASM module with a mounted hard drive, the Packet Capture will not be allowed to occur because of storage limitations.

Protocol Filters Restrictions

If Protocol Filters Active Directory, HTTP/HTTPS, or All Other Protocols are set to True, the following options will be hidden and no longer configurable:

1. Media

2. DSP/CSME

3. TCP/UDP Ports

TCP/UPD Ports Restrictions

If any TCP/UDP Ports are entered, the following options will be hidden and no longer configurable:

1. Active Directory

2. HTTP/HTTPS

3. All Other Protocols