# Troubleshooting With Multiple NAMs

In addition to aggregating data from multiple NAMs as a matter of course, Cisco Prime Assurance makes it easy to actively manage and troubleshoot network problems using multiple NAMs. In the following workflow, a network operator needs to troubleshoot a set of similar authentication violations taking place at multiple branches. Because the operator suspects that the authentication problems are due to a network attack in progress, she runs the Prime Assurance Packet Capture feature against NAMs for each branch, then cross-launches the NAM Traffic Analyzer Packet Decoder to inspect the suspicious traffic.

**Step 1** Select **Tools > Packet Capture**.

**Step 2** Click **Create** to create a new capture session definition.

**Step 3** Complete the **General** section as needed. Give the session definition a unique name and specify how you want the captured data filed.

**Step 4** If you want to restrict the captured traffic to particular source or destination IPs, VLANs, applications, or ports, click **Add** in the **Software Filters** section and create filters as needed.

**Step 5** Click **Add** in the **NAMs** section. Select all the NAMs you want to capture traffic on by clicking the check box next to each NAM. Then click **Add** to add them to the packet capture definition

**Step 6** Click **Create and Start All Sessions**. Prime Assurance saves the new session definition, then runs separate capture sessions on each of the NAMs you specified. It stores the sessions as files on the Prime Assurance server, and displays the list of packet capture files in the **Capture Files** section.

**Step 7** To store the packet-capture files locally, select the files you want and click **Download**. Specify the names you want to store the files under locally and then click **OK**.

**Step 8** To examine the contents of a packet-capture file, select the file you want to see and select **Decode**. Prime Assurance will cross-launch launch the NAM Packet Decoder and display the file information.

**Step 9** To run the packet captures again, select the session definition in the **Capture Sessions** section, then click **Start**.