Contents

Features of Sniffer Pro

- It decodes for more than 450 protocols.
- It provides support for major LAN, WAN, and networking technologies.
- It provides the ability to filter packets at both the bit and byte levels.
- It provides expert analysis and diagnosis of network problems and recommends corrective actions.
- Switch Expert provides the ability to poll statistics from various network switches.
- Network traffic generator can operate at Gigabit speeds.

Answers to Your Frequently Asked Questions

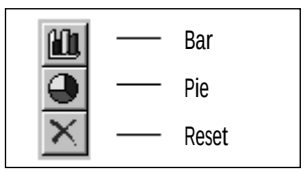
Q: Does NAI recommend a particular brand or model of laptop on which to run Sniffer Pro?

A: No. Unlike the older DOS versions of Sniffer, NAI recommends no particular brand or model of system for Sniffer Pro. Use your best judgment to buy a stable and high-performance machine.

Q: Can I connect to Sniffer Pro from a remote PC, using the Distributed Sniffer Pro console?

A: No. Sniffer Pro is standalone software and cannot be accessed using the Distributed Sniffer Pro console. To control a Sniffer Pro system remotely, you can install remote control software such as PC Anywhere, VNC, or Carbon Copy.

The Global Statistics Toolbar



WARNING

Make sure you master the art of working with timestamps so that you can troubleshoot how long a login occurs or how long it takes to transfer a file. Once you learn how to build a filter, use timestamps to isolate a client/server login to see how long it takes. You must also master this information for the SCP exam.

The Default Utilization % Dial

Taking Captures from the Menu and the Toolbar

There are a few different ways of taking captures:

- By choosing **Capture | Start** from the Main menu
- By pressing the **F10** key
- By pressing the **Start** button on the main toolbar (it looks like the Play button on your VCR)

NOTE

Remember, after 16 consecutive collisions, the frame is discarded and the collision in some cases might not be reported to the upper-layer protocols. Application timers have to expire before a retransmission attempt occurs. This stipulation can cause serious delays and program timeouts.

Filters

Sniffer Pro has four types of filters:

- Capture filters
- Display filters
- Monitor filters
- Event filters

The Alarm Type Column

The Alarm Type column indicates the type of node or the originator of the alarm as defined within the Address Book. These types can include servers, bridges, hubs, and other network devices.

NOTE

For the Sniffer Certified Professional exam, you might want to pay attention from where you can export a report.

Attacks: Password Capture and Replay

- File Transfer Protocol (FTP) is the Internet's file exchange protocol. The protocol uses client/server architecture.
- The client/server session negotiation is transmitted in clear text. The login and passwords are completely visible to any would-be hacker who has the price of a cheap sniffing program. These items can be captured and replayed with a minimum amount of effort.
- Sniffer Pro can be configured to detect invalid login or password attempts and mitigate the risk of using this clear-text protocol.

TIP

If you want to test the use of Sniffer Pro recording small packets, you can ping yourself with the following:
C:\> ping 192.168.1.1 –t –l 50
The *–t* will keep the pings continuous
The *–l* will set the length of the packets, and the *50* is setting it to 50 bytes