



Release Notes

Sniffer Basic 3.5

Updated: January 15, 2000

This release note contains new features and last minute product information for Sniffer Basic 3.5. The Sniffer Basic help files also provide essential information to help you begin using Sniffer Basic.

"Information regarding NAI products that are Year 2000 compliant and its Year 2000 standards and testing models may be obtained from NAI's website at <http://www.nai.com/y2k>. For further information, send an email message to y2k@nai.com"

Table of Contents

- Important Note
 - Supported Protocols
 - New Features
 - Installation Issues
 - Known Issues
 - Drivers and Network Performance Issues
 - Available Documentation
 - Contacting Network Associates
 - Copyright and Trademark Attributions
-

Important Note:

Sniffer Basic 3.5 functionality differs from Sniffer Pro 3.5 in the following areas:

- Limited support of protocol deocdes
 - No support for Wide Area (WAN), HSSI, ATM, FDDI, or Gigabit topologies
 - No Expert analysis
 - No Sniffer Predictor
-

Supported Protocols

IP, TCP, UDP, ARP, RARP, IARP, ICMP, IGMP, BOOTP, DHCP, RIP, EGP, OSPF, IGRP, GRP, GDP, BGP, DNS, TCP_NETB, TFTP, Telnet, FTP, SMTP, POP3, SNMP, HTTP, Gopher, DHCP, FINGER, HSRP, IMAP, Moblie IP, GRE, SHTTP, SLP, ICMPv6, RIPv6, IPv6, IPESPv6, IPDEMUX, IPX, SPX, SPX2, IPX_ECHO, IPX_ERR, IPX_BURST, NCP, NOV_NETBIOS, NOV_WDOG, NOV_BCAST, NSAP, NDIAG, IPX_RIP, NLSP, NDS, FRAG, IPX_SERIAL, IPX_PING, IPX_MOBILE, IPXVIP, IPX Security, NCP over IP - Pure IP, Netware 5.0, DRP, LAT, NSP, SCP, DAP, NICE, FOUND, CTERM, MOP DL, MOP RC, LAVC, SCS, MSCP, DSP, VCSP, XWIN, APPN, LAN_MGMT, XID, IRMA, NETB, RPL, APPN-HPR, NETBEUI, SMB/SMBO, NBP, DDP, AARP, ATP, ANBP, RTMP, ZIP, ECHO, ASP, AFP, ADSP, PAP, LAP, FRAG, TOPS, DSI, VIP, VIPC, VSPP, LOOP, ECHO, VFRP, VSARP, VARP, VICP, VSRTP, VRTP, VNRPC, VST, VMAI, VNSM, VSS, VPCB, VVNG, VECHO, VRTR, VFTP, VFS, VTALK, VASYNC, VSTDA, VSTDA Getnames, VDEFL, VDIAG, VNETB, VPRNT, VSEMP, VSNA, VAFRAG, VNP, VIDIP, VIPIP, VIPARP, VIPCMN, VSX, CLNP, ISO_TP, SESS, PRES, ASN.1, IS-IS, ES-IS, ISO_NETBIOS, ACSE, ROSE, FTAM, VTP, X.400 RTS, X.400 P1, X.400 P2, X.500, CMIP, CMOT, LDAP, CLDAP, ENET, TRING, RIF, TR_MAC, ETHER_EMBED, TR_EMBED, SNAP, LOOP, BPDU, IBMRT, IBMRT/SNA, IBMNMP, IBMRPL, NGCP, HDLC, PPP, ISODE_ASS,

PROTEON_GLUE, CISCO_GLUE, VLLC, CDP, ISL, DISL, IEEE 802.10, DRiP, VTP, SMB, NetBIOS, MSRPC, RMSNET, SMB_MAIL SLOT, SMBGLOBE, SMB_NETLOGON, NT LAN Manager, RAP, SMB_BROWSER, NAMED_PIPES, LSARPC, WINSIF, NT 5.0 SMB, SRVSVC, SNTP, NTP,

=====

New Features

The following protocol decodes were added to Sniffer Basic 3.5

- SUN NFS: RPC, NFS, PMAP, MOUNT, NIS, RPCBIND, RSTAT, SUN_ND, NLM, NSM, XDR
- Microsoft Networking Protocols: LSARPC, NETRLOGON Exchange Sum, SMB/CIFS 1.1, NMPI decode, SMB Transact, SMB NT Status, SMB Frame Corr, SMB/IPX Netbios, WinSpool RPC
- Voice Over IP: G.711, G.722, G.723, G.728, G.729, H.225, H.225, H.245
- AppleTalk: STALK, KSP

Sniffer Reporter

The Sniffer Reporter is a separate application program that lets you generate graphical reports based on RMON data that has been collected by the Sniffer Basic 3.5 database. This information is recorded and stored during a user defined time frame and intervals. The reports provide the ability to display and interpret host, matrix, protocol distribution, and global statistics (per segment) information. The Sniffer Reporter supports the 10/100 Ethernet and Token Ring topologies. This release is limited to local area networks.

For more information, please refer to the Sniffer Reporter readme file included with the Sniffer Reporter CD.

New Madge Token Ring 6.11 Driver Support

The new driver supports Token Ring Madge ISA, PCMCIA (MK2) and PCI (Up to MK3).

The default ring speed is now set to 16MB.

The Madge driver support for cardbus passed all initial tests with Sniffer Basic on Windows NT but was not fully tested in this release and therefore will not be supported.

New Xircom CBE2 card support, Revision 5

The new card does not see alignment errors. It is a known limitation of the CBE2 hardware.

New Sequencing and Reassembly for the following Protocols

This section lists the protocols that are reassembled by the protocol interpreters for Release 3.5. Other protocols will be added as they become available.

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)
- Sun NFS over IP
- User Datagram Protocol (UDP)
- IP Authentication
- Lightweight Directory Access Protocol (LDAP)
- IBM Data Link Switching Protocol (DLSW)
- Finger
- Oracle Transparent Network Substrate (TNS)
- Oracle SQL*Net
- Oracle Net8
- Sybase/Microsoft Tabular Data Stream (TDS)
- Novell Network Core Protocol (NCP)
- Novell Sequenced Packed Protocol (SPX)
- Microsoft Connection Oriented DCE RPC
- Microsoft Connectionless DCE RPC
- ISO Development Environment over TCP/IP (ISODE)

- ISO Transport Protocol (ISOTP)
- ISO Session Protocol (ISOSESS)
- ISO USPS Remote Bar Coding System Image Exchange
- DEC Network Services Protocol (NSP)
- Vines FRP
- Vines IPC
- ANS.1 H245
- ANS.1 LDAP
- AppleTalk DSI
- XWindows
- X.25
- SAP
- Identification Protocol

New Sequencing and Reassembly Module

With the advent of tunneling and other such methods, multiple layers of reassembly have become necessary. The release of Sniffer Basic 3.5 facilitates the use of a new Sequencing and Reassembly "Engine" which supports multiple layers of reassembly.

This "engine" involves the dynamic construction of a *Flow Database*[™], which contains information about clients and servers on both ends of a conversation on the network. It is through the construction of the *flow database* that the sequencing of packets from the network, and thereby ultimate reassembly, is accomplished. The flows at each layer of the protocol stack are managed separately, thus allowing for multi-layer reassembly.

Protocol Interpreter User Interface Changes

Detail Display

- Vector Table

When reassembly occurs, the Detail display of the first frame of a multi-frame PDU will contain the decode for all frames reassembled. A new feature to reassembly is the addition of a "Vector Table" as part of the Detail Display of the first frame. The Vector Table contains the following useful information about the Reassembly:

1. Vector - PDU number
2. Offset - Offset from the frame number listed
3. Length - Length of individual PDU
4. Frame - Frame number in capture buffer

- Configurable Maximum Number of Detail Display Lines

It was discovered during testing in 3.5 that the new reassembly engine is so much better than past modules that extremely large multi-frame PDUs are now being correctly reassembled (which weren't in the past). For example, one trace file used for testing contains **a reassembly of 819 fragmented frames comprising over 312Kb of data**. Such large amounts of data were never seen before in Sniffer. Consequently, when such large amounts of data are processed, some performance degradation will result.

For this reason the number of Detail Display Lines is now configurable. See Display -> Display Setup -> Maximum # of Detail Lines. The minimum number of detail display lines allowed are 200.

- Hex Data Buffer Maximum

The maximum number of bytes displayed in the hex window is 32000. This is not configurable.

=====

Known Issues

Sniffer Basic Cisco Switch Alarms and UI Enhancements

- The supported Cisco switches MUST run version 4.5.1 or higher. Cisco requires software version 4.5.1 or higher to send alarms properly. If an ATM module is installed in the switch, in the version below 4.5.1, there is a problem in the Cisco software which may cause the switch to stop responding to SNMP commands.
- When deleting alarms there is a short delay when the Sniffer is communicating with the switch. If the last alarm in the list is selected to be deleted, do not select the delete icon again. If the delete icon is selected while the Sniffer is communicating with the switch to delete the last alarm, the connection with the switch may hang.
- When an alarm on the switch is configured for Rising threshold, you may receive a Rising threshold alarm as well as a Falling threshold alarm.
- Using Cisco switches version 5.1.1 requires setting the span destination port from the switch. Once the port is set to span on the switch, Sniffer Basic will be able to span and capture to the specified port.

Drivers and Network Performance Issues

Selecting a network card which does not exist on your machine will result in an incorrect message. Attempting to install a network card which does not exist on your machine from the Sniffer Basic setting menu will bring up the "Select Setting " dialog box.

The dialog box will present two options **OK** and **Cancel** and the following message: "**Click OK to Close Sniffer and exit the application**". This is an incorrect message. If you select OK, it will bring up the "Select Setting" dialog box again to allow proper installation of the driver. It will not exit the Sniffer application. If you select Cancel, it will exit the application.

Remove previous versions of the NAI enhanced Adaptec, Xircom Cardbus and Madge PCMCIA drivers from your machine prior to installing the new enhanced drivers on Windows 98 and Windows 95 only. To manually remove the old drivers, perform the following steps:

1. Uninstall the previous version of Sniffer Basic and restart the machine.
2. In the Windows control panel, select the **Network** icon. (Remember to write down the card TCP/IP settings, such as the IP address prior to removing the driver.)
3. On the **Configuration** tab of the Network dialog box, Select **Adapter**.
4. Select the specific **Network Associates, Inc.** Adapter that you wish to upgrade, then click **Remove**.
5. Select **OK**. **Important: Do not restart the machine.**
6. You will be prompted to restart the computer, select **NO**.
7. Install Sniffer Basic 3.5 from the CD as described in the Sniffer Basic installation manual and select Yes to make NAI enhanced driver available.
8. Restart the machine.
9. Windows Plug and Play will detect and install the new driver. Configure the TCP/IP settings of the driver in the Windows Control Panel Network tab as described in the installation manual.

Changing Network Speeds

- For 10/100 Mbps Ethernet and 4/16 Mbps Token Ring network adapters, it may be necessary to restart your machine and restart Sniffer Basic to change network speeds.
- Upon installing the Madge card, you will be prompted to select the ring speed. Please select the ring speed of the hub.

Heavily Loaded Ethernet Networks

On heavily loaded 100Mbps Ethernet networks using non-NAI NDIS drivers, Sniffer Basic may experience unstable behavior (for example, your system may crash). To correct this problem, increase the receive buffer size on the network adapter by performing the following steps:

1. In the Windows control panel, select the **Network** icon.

2. Select the **Adapter** tab.
3. In the Adapter tab properties, select **Adapter Properties**.
4. Increase the **Receive Buffers** value.

Increasing the Capture Performance of the NAI Xircom 10/100 Card

Certain notebooks experience resource problems when loading the enhanced NAI driver. To enable the card to load on a wide spectrum of notebooks, the ReceiveBuffer size has been reduced. If you wish to **increase** your capture performance, change the buffer settings to the highest setting possible, which still enables the card to load:

In Windows 95/98:

1. In the Windows control panel, select the **Network** icon.
2. In the list box at the top of the **Configuration** tab, select **Network Associates, Inc. Cardbus Ethernet 10/100 Adapter**, then click **Properties**.
3. Click the **Advanced** tab.
4. In the Property list box, select **ReceiveBuffers** and increase the value to a larger number. We recommend you increase the buffer size in increments of 10 to the highest possible setting, which still enables the card to load.

In Windows NT:

1. In the Windows control panel, select the **Network** icon.
2. Click the **Adapter** tab.
3. Select **Network Associates, Inc. Cardbus Ethernet 10/100 Adapter**, then click **Properties**.
4. Increase the **Receive Buffers** value to a larger number. We recommend you increase the buffer size in increments of 10 to the highest possible setting, which still enables the card to load.

Packet Generation

- On a Token Ring network, Sniffer Basic may experience erratic behavior when you try to generate a frame using the Packet Generator if the frame is greater than the maximum size configured on the network adapter. For example, in Windows NT, the system may crash. In Windows 95, the Packet Generator may remain in "Send" mode. To correct this problem, increase the maximum frame size for this network adapter under **Settings/Control Panel/Network**.
- On a 10/100 Xircom card, Sniffer Basic may not generate traffic with a 0 delay.

Using the Adaptec 10/100 on a Dolch PAC-64

The current Adaptec driver cannot share the same interrupt (IRQ 15) with the secondary IDE controller. Even though the secondary IDE controller is turned off in the BIOS, there is still an interrupt conflict. To work-around this problem, change the IRQ 15 settings to Legacy ISA under **PCI Configuration Setup** in the BIOS.

NAI Xircom 10/100 Problems

If you are having trouble loading the Xircom card, try reducing the ReceiveBuffers setting.

NOTE: Some notebooks do not have enough resources available to load the enhanced driver. Change the Receive Buffer setting from the default setting of 80 to the minimum of 60.

In Windows 95/98:

1. In the Windows control panel, select the **Network** icon.
2. In the list box at the top of the **Configuration** tab, select **Network Associates, Inc. Cardbus Ethernet 10/100 Adapter**, then click **Properties**.
3. Click the **Advanced** tab.
4. In the Property list box, select **ReceiveBuffers** and change the value to 64.

In Windows NT:

1. In the Windows control panel, select the **Network** icon.
2. Click the **Adapter** tab.
3. Select **Network Associates, Inc. Cardbus Ethernet 10/100 Adapter**, then click **Properties**.
4. Change the **Receive Buffers** value to 60.

Try the Manual Load Version of the Xircom Driver

If you are running Windows 95 Version A, you may need to load the Xircom driver manually. Perform the following steps:

1. In the Windows control panel, select the **Network** icon.
2. On the **Configuration** tab of the Network dialog box, click **Add**.
3. Select **Adapter**, then click **Add**.
4. In the **Manufacturers** list box, select **Network Associates, Inc.**
5. In the **Network Adapters** list box, select **Network Associates, Inc. CardBus Ethernet 10/100 Adapter Manual Load**, then click **OK**.
6. On the **Resources** tab, configure the hardware settings, then click **OK**.

Xircom driver memory conflict error following an installation

Change the memory address setting if you receive the following error after installing the Xircom driver with the default settings and rebooting your machine:

Service Control Manager: "*At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details.*"

NT Event Viewer, System log: "*CBE1 : Has encountered a conflict in resources and could not load.*"

CBE1 : There is a memory conflict at address 0x000000005B80000."

If you encounter this error perform the following steps:

1. In the Windows Control Panel select **Network Adapter, Properties**.
2. Select a different Memory Address by Changing the Memory Address setting for the Xircom driver (cbe.sys) from 0x5B80000 to 0xD4000

NAI (Madge) PCMCIA Token Ring Adapter Card and Windows 95 Drivers

The Network Associates PCMCIA Token Ring adapter card does not load correctly in Windows 95 if you use the drivers supplied in Windows 95 (you will see a yellow exclamation point next to the Madge card on the **Device Manager** tab under **Control Panel\System**).

To correct this problem, either install the updated drivers from Madge Networks or install the NAI enhanced drivers as described below.

Running Madge Adapter Cards under Windows 95 A or Earlier with NAI Enhanced Drivers

The Madge adapter card does not load correctly in Windows 95 Version A or earlier if you use the NAI enhanced drivers (you will see a yellow exclamation point with error code 2 next to the Madge card on the **Device Manager** tab under **Control Panel\System**).

Windows 95 Version A and earlier does not support NDIS 4, but the NAI enhanced drivers do. To workaround this problem, you must download the Windows 95 Windows Sockets 2 update from Microsoft.

1. Go to the following URL at the Microsoft web site:
<http://www.microsoft.com/windows/downloads/default.asp>
2. Download the Windows 95 Windows Sockets 2 update to a temporary directory on your PC.
3. Double-click the file *ws2setup.exe* to extract and install the program files.

Note: Each time you add a network card after updating the system, you are prompted to save the newer files or overwrite them. Click **Yes** to save the newer files.

Using the Olicom Gocard

The Olicom Gocard 3250 Cardbus was tested and has proven to work well with the Sniffer Basic application; however, it was not modified by NAI to detect error counts.

Available Documentation

Network Associates provides each of its customers with an extensive set of documentation, consisting usually of one or more product guides saved in Adobe Acrobat Portable Document Format (.PDF), and an online help system, whose form can vary, depending the platform on which the product runs.

Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines and other aids for easy navigation and information retrieval. You can also install an Acrobat plug-in file that allows you to read .PDF documents from within your web browser. Copies of the product documentation are available on the product CD-ROM or on the Network Associates website at:

ftp://ftp.nai.com/pub/manuals/total_Network_Visibility

A free copy of Acrobat Reader is also available on the CD-ROM, or from the Adobe website at:

<http://www.adobe.com/prodindex/acrobat/readstep.html>

Most Network Associates products include a documentation set which contains one or more of the following documents. **NOTE:** Not all products will include these documents. Consult your user or administrator's guide for a complete list of available documentation.

Getting Started Guide. Introduces the product, outlines product features, and provides a brief overview. In many cases, an electronic version of this guide will also be available on the product CD-ROM or from the Network Associates FTP site.

User's Guide. A User's Guide is available on the product CD-ROM. You can also install it on your hard drive from your CD-ROM. Network Associates User's Guides document all product functions extensively, and discuss how best to use your Network Associates product to accomplish your tasks.

Specialized Guides. These can include reference guides, deployment guides, configuration guides, vulnerability guides for intrusion detection software, and other product-specific documentation.

Online Help. Online help gives you quick access to hints and tips about how to use your Network Associates product. The format of the online help system for the product will vary, depending on which platform or operating system you use.

Context-Sensitive Online Help. Right-click on buttons, lists or other elements within dialog boxes to see brief, descriptive help topics.

This Release Note. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates.

Contacting Network Associates

To order products, obtain product information, or to obtain technical support, contact the Network Associates Customer Service department at 972-308-9960, or write to the following address:

Network Associates, Inc.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203

U.S.A.

Copyright and Trademark Attributions

Copyright (c) 2000 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies.

Trademarks

ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, CNX, Compass 7, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, GroupShield, HelpDesk, Hunter, ISDN Tel/Scope, LM 1, LANGuru, LeadingHelp Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee, McAfee Associates, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetOctopus, NetRoom, NetScan, Net Shield, NetShield, NetStalker, Net Tools, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, Pop-Up, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, RouterPM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SiteMeter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, Switch PM, TeleSniffer, TIS, TMach, TMeg, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, T-POD, Trusted Mach, Trusted Mail, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker, WebWall, and ZAC 2000 are registered trademarks of Network Associates and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

License Agreement

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, CONSULT THE LICENSE.TXT, README.1ST, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.