

# Contents

<b>Foreword</b>	<b>xxv</b>
<b>Features of Sniffer Pro</b>	<b>1</b>
■ It decodes for more than 450 protocols.	2
■ It provides support for major LAN, WAN, and networking technologies.	2
■ It provides the ability to filter packets at both the bit and byte levels.	3
■ It provides expert analysis and diagnosis of network problems and recommends corrective actions.	5
■ Switch Expert provides the ability to poll statistics from various network switches.	7
■ Network traffic generator can operate at Gigabit speeds.	8
<b>Chapter 1 Introduction to Sniffer Pro</b>	<b>10</b>
Introduction	17
Understanding Network Analysis	20
Network Analysis Fundamentals	24
Troubleshooting Methodology	30
The OSI Model, Protocols, and Devices	31
The OSI Model and the DOD Model	34
TCP/IP	35
IPX/SPX	36
AppleTalk	36
Ethernet	36
Fast Ethernet and Gigabit Ethernet	37
Token Ring	39
Other Protocols	40
DECnet	41
SNA	45
Wireless Communication	46
Hubs and MAUs	46
What Is a Hub?	47
What Is a MAU?	49
Switches, Bridging, and NICs	40
Switches, Bridges and Bridging	40
Differences Between a Switch and a Bridge	41
Network Interface Cards	45
Routers and Gateways	46
Routing Fundamentals and Protocols	46

## Answers to Your Frequently Asked Questions

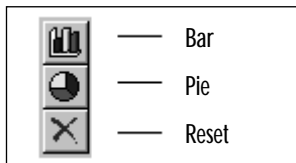
- Q:** Does NAI recommend a particular brand or model of laptop on which to run Sniffer Pro?
- A:** No. Unlike the older DOS versions of Sniffer, NAI recommends no particular brand or model of system for Sniffer Pro. Use your best judgment to buy a stable and high-performance machine.
- Q:** Can I connect 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.

Sniffer Pro Fundamentals	48
Features of Sniffer Pro	48
Other Sniffer Versions and Products	49
Other Solutions and Products	50
EtherPeek	50
Ethereal	50
Agilent Advisor	50
Management and Return on Investment	50
Charts and Reporting	51
Proactive and Reactive Network Maintenance	51
Sniffer Pro: The Exam	52
Certification Testing and the Sniffer University	52
Sniffer Certified Professional	52
SCP, SCE, and SCM	54
Other Certifications and Tracks	54
Summary	56
Solutions Fast Track	56
Frequently Asked Questions	58
<b>Chapter 2 Installing Sniffer Pro</b>	<b>61</b>
Introduction	62
Installing Sniffer Pro Step by Step	62
System Requirements for Sniffer Pro Installation	63
Minimum System Requirements for Version 4.x	63
Internet Explorer 5 with the Virtual Machine	64
Minimum System Requirements for Version 3.0	65
Installing Sniffer Pro 4.5	65
Licensing	75
Read the Readme.txt File	76
Installation of Version 3.x	77
Installing Sniffer Pro on Other Platforms and Hardware	81

Laptop Considerations	82
Apple Considerations	83
Customizing the Installation	83
Configuring Sniffer Pro for Remote Access	83
Using a Tablet PC for Portability	84
Configuring Network Interfaces and Drivers	84
The Promiscuous NIC	84
Selecting the NIC	85
NetPod	86
Replacing Drivers	88
Standard NDIS Drivers and Issues	88
Sniffer Pro Network Drivers	88
NAI Enhanced Drivers for Windows 2000	89
Removing Previously Installed PnP	
Network Drivers on Windows 98	90
Disabling Unnecessary Services on	
Ethernet Adapters Attached to Pods	91
Changing Network Speeds After	
Starting Sniffer Pro	91
Enhancing Capture Performance	92
Enhancing General System Performance	93
Notebook Resource Problems	93
Known Issues with Windows 2000	95
Installing Gigabit Ethernet, HSSI,	
and LM2000 Cards	95
Troubleshooting the Installation	97
Failed Installation	97
Drivers Not Installing	97
Installing on the Wrong Platform	98
Error Messages	98
Failing to Delete Sniffer.ini on	
an Upgrade	99
Building a Technician Tool Kit	99
Summary	101
Solutions Fast Track	101
Frequently Asked Questions	103

<b>Chapter 3 Exploring the Sniffer Pro Interface</b>	<b>105</b>
Introduction	106
Exploring the Dashboard	106
Real-Time Statistics	106
Utilization and Errors	107
Setting Thresholds	112
Configurable Dashboard Graphs	113
Understanding Menus	114
The File Menu	114
The Monitor Menu	115
The Capture Menu	123
The Display Menu	124
The Tools Menu	125
The Database Menu	125
The Window Menu	126
Help	127
Understanding the Toolbars	127
Starting, Stopping, and Viewing a Capture	129
Defining a Wizard	130
Opening and Saving a Capture	130
Printing	131
Other Icons and Functions	132
Miscellaneous Sniffer Pro Tools	132
Packet Generator and Loopback Mode	133
The Bit Error-Rate Test	135
Reporter	136
Ping	136
Trace Route	137
DNS Lookup	138
Finger	138
WhoIs	138
Address Book	139
The Expert	139
The Capture	139
False Positives	140

**The Global Statistics  
Toolbar**



The Decode Tab	140
Matrix	143
Host Table	145
Protocol Distribution	147
Statistics	148
Graphs, Charts, and Maps	148
Top Talkers	149
Heavy Protocol Distribution	149
Creating a List of Hosts on Your Network	150
Using the Address Book	150
Adding New Addresses	151
Exporting the Address Book	153
Summary	154
Solutions Fast Track	154
Frequently Asked Questions	157

## **Chapter 4 Configuring Sniffer Pro to Monitor Network Applications 159**

### **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.

Introduction	160
Basic Sniffer Pro Data Capture Operations	160
Starting and Stopping the Capture Process	161
Viewing and Dissecting the Capture	166
Monitoring with the Summary, Details, and Hex Panes	166
Sniffer Pro Analyzer Placement	177
Sniffer Pro Advanced Configuration	179
Switched Port Analyzer	180
How to Set Port Spanning	181
How to Set Port Spanning for a VLAN	181
Timestamping Procedures	183
Timestamp Columns and Timestamping	183
Viewing and Using the Expert	186
The Expert and Objects	187
Troubleshooting with the Expert System	188
The Expert Layers	188
Expert Alerts and Problems Indicators	193
False Positives and Negatives	197

Configuring Expert Options	198
Application Response Time	205
Adding Custom Protocols to ART	208
Configuring Sniffer Pro to Capture and	
Analyze NetWare Traffic	209
Sniffer Pro Traffic Capture	210
Analyzing the Summary Pane	210
Analyzing the Details Pane	211
Analyzing the Hex Pane	214
Configuring Sniffer Pro to Capture and	
Analyze Microsoft Traffic	214
Sniffer Pro Traffic Capture	215
Analyzing the Summary Pane	216
Analyzing the Details Pane	216
Analyzing the Hex Pane	224
Summary	225
Solutions Fast Track	226
Frequently Asked Questions	228

## Chapter 5 Using Sniffer Pro to Monitor the Performance of a Network 231

Introduction	232
Network Performance Issues	232
Real-Time Performance Monitoring with	
Sniffer Pro	236
Using the Dashboard in Real Time	238
The Gauge Tab	239
The Detail Tab	241
The Network Graph	243
The Detail Errors Graph	247
The Size Distribution Graph	250
Long- and Short-Term Analysis	251
Customizing Your View	251
Setting Thresholds	252
Baselining, Trending, and Change Management	256
Baselining Over Time	257
Trending Tips	257

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)

Change Management	258
Analyzing Ethernet Performance with Sniffer Pro	259
Monitoring the Performance of the Ethernet	259
Saturation Levels and Collisions	260
Ethernet Framing Problems	262
Hardware Problems	267
STP Loops and Broadcast Storms	268
Analyzing Token Ring Performance with Sniffer Pro	270
Monitoring the Performance of Token Ring	272
Setting Up Sniffer Pro to Analyze Token Ring	272
Viewing the Dashboard with Token Ring	273
Common Token Ring Performance Problems	278
Configuring Thresholds	283
Other Token Ring Performance Solutions	283
Analyzing LAN Routing Performance Issues	286
Routing Updates	287
Realigning Your Network for Better Performance	289
Summary	292
Solutions Fast Track	292
Frequently Asked Questions	296
<b>Chapter 6 Capturing Network Data for Analysis</b>	<b>299</b>
Introduction	300
Capturing Traffic	300
How to Capture Traffic	301
Taking Captures from the Menu and the Toolbar	302
Pulling Up the Capture Panel	303
Saving and Using Captures	305
Saving Captures	306
File Types	311

Retrieving and Loading Captures	311
Capturing and Analyzing Address Resolution Protocol	312
Capturing ARP Traffic	313
Analyzing the Capture	316
Capturing and Analyzing Internet Control Message Protocol	318
Capturing ICMP Traffic	318
Analyzing the Capture	320
Capturing and Analyzing Transmission Control Protocol	326
Capturing TCP Traffic	327
Analyzing the Capture	329
Capturing and Analyzing User Datagram Protocol	333
Capturing UDP Traffic	334
Analyzing the Capture	334
Summary	337
Solutions Fast Track	338
Frequently Asked Questions	341

## **Chapter 7 Analyzing Network Issues      343**

Introduction	344
Hey! Why Is the Network So Slow?	344
Using Sniffer Pro to Troubleshoot a Slow Network	345
Excessive Collisions and Collision Domains	345
Collisions on a Network Segment	347
Ethernet Specifications	348
Collision Domain	349
Repeaters	350
Ethernet Bridges	353
Ethernet Switches	353
Determining the Collision Domain	357
Half- and Full-Duplex Communication	358
Late Collisions	360

### **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.



Causes of Late Collisions	360
Broadcasts from Hubs	361
Broadcast Domains	361
What Does the Expert Say?	362
Troubleshooting the Broadcast	363
Resetting Token Ring Networks	366
Multi-MAU Configurations	367
Token Passing	368
The Active Monitor	369
The Standby Monitor	369
Ring Insertion	371
Troubleshooting the Token	373
Using Sniffer Pro to Troubleshoot a Chattering	
Network Interface Card	375
Alignment Errors	376
Fragment Errors	378
Jabber Errors	378
Using Sniffer Pro to Troubleshoot Small	
Packets (Runts)	380
Using Sniffer Pro to Troubleshoot Browsing	
Battles	381
Browser Elections	383
Troubleshoot Browsing Battles	384
Browser Communication	386
Announcement!	389
Dynamic Host Configuration Protocol Failure	390
BOOTP	390
DHCP Discover	391
DHCP Offer	393
DHCP Request	395
DHCP Ack	396
DHCP Release/Renew	397
DHCP Troubleshooting	399
Summary	401
Solutions Fast Track	402
Frequently Asked Questions	404

**Filters**

Sniffer Pro has four types of filters:

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

<b>Chapter 8 Using Filters</b>	<b>405</b>
Introduction	406
What Is Filtering, and Why Filter?	406
Using Predefined Filters	407
Filters Available to You by Default	407
Creating Filters	409
Using the Filter Dialog Box	411
Filter Dialog Box Tabs	411
Selecting Filters from the Main Menu	420
Expert-Level Filtering	420
Filtering from One Node to Another	421
MAC Address Filtering	423
IP Address Filtering	428
IPX Address Filtering	433
Troubleshooting with Filters	434
Cisco Discovery Protocol	434
Routing Information Protocol	437
Summary	439
Solutions Fast Track	439
Frequently Asked Questions	441

<b>Chapter 9 Understanding and Using Triggers and Alarms</b>	<b>445</b>
Introduction	446
Introducing Triggers	448
Configuring and Using Triggers	449
The Trigger Graphic Outline	449
The Start and Stop Trigger Screens	450
Using the Date/Time Option	451
Using the Alarm Option	452
Using the Event Filter	453
Trigger Repeat Mode	454
Configuring and Using Alarms	455
Alarm Log Display	456
The Status Column	459
The Alarm Type Column	459
The Log Time Column	460

**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.

The Severity Column	460
The Description Column	460
Configuring Alarms Notifications	460
Notification Using a Sound	460
Associating an Action with Alarm	
Severity	461
Define Severity	461
Define Actions Notification	462
Managing Alarm Actions	463
Defining an SMTP Mail Notification	464
Defining a Pager Notification	465
Defining a Beeper Notification	468
Modifying Alarm Threshold Levels	469
Expert Alarm Thresholds	469
Monitoring Alarm Thresholds	470
Application Response Time	472
Summary	474
Solutions Fast Track	476
Frequently Asked Questions	479
<b>Chapter 10 Reporting</b>	<b>481</b>
Introduction	482
Reporting Fundamentals	482
Why You Should Consider Creating a Report	484
Creating the Report Template	487
Report Contents	487
Tools of the Trade	488
Running and Exporting Reports	493
Running Reports Under the Expert	494
Running Reports Under the Matrix	497
Outline and Detail Views	497
Top N Views	498
Running Reports Under Host Table	500
Running Reports Under Protocol	
Distribution	501
Running Reports Under Global Statistics	502

**NOTE**


---

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

---

Other Exportable and Reportable Views	503
Exporting from Your Address Book	504
Exporting Data from Other Tools	504
HTML and CSV	505
Creating a Full Report: “Network Is Slow”	506
“The Network Is Slow”	507
Summary	509
Solutions Fast Track	509
Frequently Asked Questions	511

## **Chapter 11 Detecting and Performing Security Breaches with Sniffer Pro 513**

### **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.

Introduction	514
Using Sniffer Pro to Find Holes in Your Network	514
Delivery and Payload	515
Vulnerabilities in Detail	516
Code Red: The Exploit	516
Nimda: The Exploit	524
Capturing Clear-Text Passwords	527
IPv4 and Clear-Text Transfer of Information	527
Telnet	528
Telnet Echo	529
The Telnet Login Filter	530
SSH and Encryption	532
Capturing E-Mail Logins	532
Attacks: Password Capture and Replay	534
Capturing the Password, Step by Step	534
Replaying the Password	536
FTP Password Guessing	536
Simple Network Management Protocol	539
Domain Name Service Vulnerabilities	541
DNS Basics	543
Resource Records	544
DNS Recursion	545
Resolver	546
DNS Zone Transfers	551
Poisoning the DNS Cache	551

DNS Cache Poisoning: How Does It Work?	552
Cache Vulnerabilities	552
Server Message Block Vulnerabilities	555
CIFS	556
SMB and Its Flaws	556
Half the Story	556
SMB Capture	557
SMB Signing	559
Summary	560
Solutions Fast Track	561
Frequently Asked Questions	563

## Chapter 12 Troubleshooting Traffic for Network Optimization 567

Introduction	568
Fine Tuning Your Network and Performing	
Proactive Maintenance	568
Defining Key Elements of Quality	
Network Performance	569
Addressing Speed Issues	570
Addressing Reliability Issues	572
Addressing Security Issues	574
Proactive Management of Network	
Resources with Sniffer Pro	576
AntiSniff: Who's Sniffing Whom?	586
Finding Unnecessary Protocols with the	
Sniffer Pro	590
Is TCP/IP Perfect?	594
Chatty Protocols	597
AppleTalk	597
IPX/SPX	599
Optimizing LAN and WAN Traffic With	
the Sniffer Pro	601
Broadcasts in Switched LAN Internetworks	601
Spanning Tree Protocol	603
Attach Directly to a Switch for Analysis	606
Optimizing with Sniffer Pro	611

### 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

---

Using Sniffer Pro to Find WAN Latency	613
Solving Network Slowdowns with Sniffer Pro	615
More Slow Network Problems	617
Ethernet Optimization	618
Ethernet Issues and the Need for Optimization	618
Collisions and Collision Domains	618
CRC Errors	619
Bottlenecks	619
Unnecessary Broadcasts	620
NetWare Optimization and Microsoft Optimization	621
Common NetWare Optimization Needs	622
Common Microsoft Optimization Needs	624
Summary	627
Solutions Fast Track	628
Frequently Asked Questions	630
<b>Index</b>	<b>633</b>