



CHAPTER 1**Overview 1-1**

- Introducing Cisco Packet Analyzer 1-1
- Overview of the Packet Analyzer Platforms 1-3
- How to Use Packet Analyzer to Analyze Your Traffic 1-4
- Before You Begin 1-4

CHAPTER 2**Getting Started 2-1**

- Before You Begin 2-1
- Quick Start 2-2
- Where to Go to Learn How to Customize Your Packet Analyzer 2-2

CHAPTER 3**Monitoring and Analyzing Traffic 3-1**

- How To Make Dashboards Work for You 3-2
 - How Do I Solve My Problem? 3-2
- Troubleshooting Application Slowness 3-3
- Using Traffic Summary 3-4
- Using Response Time Summary 3-5
- Using Site Summary 3-6
- Using Alarm Summary 3-7
 - Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment 3-8
- Analyzing Traffic 3-9
 - Analyzing Site Traffic 3-10
 - Analyzing Application Traffic 3-10
 - Analyzing Host Traffic 3-11
 - Applications Detail 3-11
 - NetFlow Interface Traffic Analysis 3-11
 - DSCP Detail 3-12
 - DSCP 3-12
 - Encapsulation 3-13
 - URL Hits 3-13
 - Viewing Collected URLs 3-13
 - Filtering a URL Collection List 3-13

Detailed Traffic Analysis Views	3-14
Sites Detailed Views	3-14
Site Conversations Detailed Views	3-14
Applications Detailed Views	3-14
Application Groups Detailed Views	3-14
Application Traffic By Hosts Detailed Views	3-15
Top Application Traffic Detailed Views	3-15
Hosts Detailed Views	3-15
Host Conversations Detailed Views	3-15
Encapsulations Detailed Views	3-15
DCSPs Detailed Views	3-16
About Analyze Traffic Charts	3-16
Optimizing WAN	3-16
Ensuring WAN Optimization	3-16
Analyzing Traffic for Optimization Using the Top Talkers Detail	3-17
Analyzing Application Performance after WAAS Optimization	3-18
Comparing Transaction Time (Client Experience)	3-18
Comparing Traffic Volume and Compression Ratio	3-18
Planning Capacity Using Average Concurrent Connections (Optimized vs. Passthru)	3-18
Optimizing Usage Using Multi-Segment Network Time (Client LAN - WAN - Server LAN)	3-18
Monitoring WAAS Traffic Across Multi-Segments	3-18
Monitoring WAAS Single-Segment Traffic	3-19
Measuring Response Time	3-19
Application Response Time	3-21
Network Response Time	3-21
Server Response Time	3-22
Client Response Time	3-22
Client-Server Response Time	3-23
Application Response Time Distribution	3-23
Network Response Time Distribution	3-23
Server Response Time Distribution	3-23
Client Response Time Distribution	3-23
Client-Server Response Time Distribution	3-24
Server Application Responses	3-24
Server Application Transactions	3-24
Server Network Responses	3-24
Client-Server Application Responses	3-25
Client-Server Application Transactions	3-25
Client-Server Network Responses	3-25

Analyzing Device Interface and Health Data	3-26
Viewing Interface Information	3-26
Viewing Health Data	3-26
Switch Health Options	3-27
Router Health Options	3-30
Analyzing Media	3-32
RTP Streams	3-33
Understanding the RTP Stream Data	3-33
Monitoring RTP Streams	3-34
Voice Call Statistics	3-35
Video Streams	3-36
Understanding the Video Stream Data	3-36
Monitoring Video Stream Data	3-38
Video Channels Statistics	3-38
Calls Table	3-39
RTP Conversation	3-40
Site MOS	3-40
Video Channels Table	3-40
Video Stream Conversations	3-41
Using the Packet Analyzer Application Programming Interface	3-42

CHAPTER 4

Capturing and Decoding Packets	4-1
How Do I Solve My Problem?	4-1
Manually Starting a Capture	4-2
Using Alarm-Triggered Captures	4-3
Scheduling Captures	4-3
Troubleshooting Application Slowness Using Alarms	4-4
Application Performance Monitoring Using Capture and Decode	4-5
Creating and Managing Capture Sessions	4-6
Configuring Capture Sessions	4-6
Configuring Software Filters	4-7
Creating a Software Capture Filter for a Capture Session	4-7
Editing a Software Capture Filter	4-7
Important Notes about Software Capture Filters	4-8
Understanding Software Capture Filter Options	4-8
Configuring Hardware Filters	4-9
Creating Packet Analyzer Appliance Hardware Filters	4-9
Understanding Hardware and Software Capture Sessions Filters	4-14
Viewing Capture Sessions	4-15

Working with Capture Files	4-15
Analyzing Capture Files	4-15
Drilling Down into Packet Error Details	4-15
Downloading Capture Files	4-16
Deleting a Capture File	4-16
Deleting Multiple Capture Files	4-16
Understanding Capture Sessions	4-17
Utilizing Capture Data Storage	4-18
About Capturing to Data Storage	4-19
Installing and Configuring Local and External Storage	4-19
Configuring the iSCSI and SAS Array	4-20
Locating the Packet Analyzer IQN and SAS Address	4-20
Connecting to the iSCSI Array	4-21
Preparing LUNs for File Storage in iSCSI and SAS	4-22
Using LUNs to Store Packets in iSCSI and SAS from a Capture Session	4-22
Logging In and Out of External Storage LUNs	4-23
Connecting and Disconnecting iSCSI and SAS	4-23
Configuring External SAS port	4-23
Recovering Data Storage	4-24
Working with Capture Query	4-25
Creating a New Query	4-26
Canceling a Query	4-26
Decoding a Query	4-26
Downloading Query Files	4-27
Deleting a Query	4-27
Duplicating a Query	4-27
Inspecting Packet Decode Information for Suspicious Traffic	4-28
Analyzing Packets in the Packet Decoder	4-28
Filtering Packets Displayed in the Packet Analyzer Packet Decoder	4-29
Viewing Detailed Protocol Decode Information	4-30
Understanding the Packet Analyzer Packet Decoder	4-31
Customizing Display Filters	4-32
Creating Custom Display Filters	4-32
Editing or Deleting Custom Display Filters	4-35
CHAPTER 5	Performing User and System Administration 5-1
Performing System Administration	5-1
Monitoring Packet Analyzer Health and Traffic Statistics	5-2
Setting Network Parameters	5-3

Setting the SNMP Agent	5-3
Working with Packet Analyzer Community Strings	5-4
Synchronizing Your System Time	5-5
Understanding Packet Analyzer System Time	5-6
Setting Up E-Mail Notifications for Alarms	5-7
Sharing Packet Analyzer Data by Enabling Web Data Publication	5-7
Setting Remote Servers to Receive Syslog Messages	5-8
Configuring Hosts to Receive SNMP Traps from Packet Analyzer	5-8
Customizing System Preferences	5-9
Importing/Exporting Configuration Details	5-9
Troubleshooting Using Diagnostics Tools	5-9
System Alerts	5-9
Audit Trail	5-10
Tech Support	5-10
Controlling User Access	5-11
Local Database	5-11
Resetting Passwords	5-12
Changing Predefined Packet Analyzer User Accounts on the Switch or Router	5-12
Creating a New User	5-12
Establishing TACACS+ Authentication and Authorization	5-14
Configuring a TACACS+ Server to Support Packet Analyzer Authentication and Authorization	5-14
Configuring a Cisco ACS Server, Version 4.2	5-15
Configuring a Cisco ACS Server, Version 5.x	5-16
Configuring a Generic TACACS+ Server	5-18
Current User Sessions	5-18
Managing System Data	5-19
Handling Backups	5-19
Shrinking Storage Requirements	5-19

CHAPTER 6

Packet Analyzer Deployment	6-1
Deploying in the Data Center	6-1
Deploying in a Campus Environment	6-1
Deploying in the Branch	6-2
General Usage Scenarios	6-2
Packet Analyzer Integrations with Monitoring and Reporting Applications	6-2
Deployment Examples	6-2
Using Packet Analyzer to Monitor VoIP Quality	6-3
Auto-Discovery Capabilities of Packet Analyzer	6-4
Creating Custom Applications	6-5

Integrating Packet Analyzer with Prime Infrastructure	6-5
Integrating Packet Analyzer with Third Party Reporting Tools	6-6
Monitoring Cisco WAAS and Measuring Its Impact	6-6
Monitoring	6-9
Using Packet Analyzer to Monitor QoS/DiffServ (DSCP)	6-10
Using Packet Analyzer for Historical Trends via Interactive Report	6-12
Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications	6-14
Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications	6-14
Troubleshooting	6-14
Using Packet Analyzer for Problem Isolation	6-15
Using Packet Analyzer for SmartGrid Visibility	6-15

CHAPTER 7

Customizing Cisco Packet Analyzer	7-1
Advanced Configuration Overview	7-2
Setting Up Traffic Configurations	7-3
Configuring Traffic to Monitor	7-3
Creating a SPAN Session for RISE Appliance	7-4
Creating a SPAN Session for Appliances and other Virtual Platforms	7-4
Editing a SPAN Session for RISE Appliance	7-5
Editing a SPAN Session for Appliances and other Virtual Platforms	7-5
Setting Up Packet Analyzer Data Sources	7-6
Forwarding SPAN Traffic	7-6
Forwarding ERSPAN Traffic	7-6
Forwarding VACL Traffic	7-14
Forwarding NetFlow Traffic	7-15
Forwarding CEF Traffic	7-22
Managing WAAS and WAN Traffic	7-23
Configuring Hardware Deduplication	7-29
Setting Up Alarms and Alarm Thresholds	7-30
Configuring Alarm Actions	7-31
Viewing Alarm Actions	7-33
Understanding Trigger Capture	7-33
Defining Thresholds	7-34
Setting Host Thresholds	7-35
Setting Conversation Thresholds	7-35
Setting Application Thresholds	7-35
Setting Response Time Thresholds	7-36

Setting DSCP Thresholds	7-36
Setting RTP Stream Thresholds	7-37
Setting Voice Signaling Thresholds	7-37
Setting NetFlow Interface Thresholds	7-38
Setting Video Stream Thresholds	7-38
Setting MDI Stream Thresholds	7-39
Editing or Deleting an Alarm Threshold	7-39
Setting Up Data Export	7-40
Configuring NetFlow Export Templates	7-40
Creating NetFlow Export Templates	7-40
Editing NetFlow Export Templates	7-40
Deleting NetFlow Export Templates	7-41
Sharing Files	7-41
Using SMB file sharing on Windows	7-41
Using SFTP file sharing on Windows	7-41
Scheduling Data Report Exports	7-42
Creating a Scheduled Report Export	7-42
Editing a Scheduled Export Job	7-43
Deleting a Scheduled Export Job	7-43
Downloading a Scheduled Report	7-44
Renaming a Scheduled Report	7-44
Deleting a Saved Reports	7-44
Accessing Device Interface and Health Details	7-45
Understanding How Platform-Specific Packet Analyzer Handle Managed Device Data	7-45
Configuring and Viewing Managed Device Information	7-45
Configuring Managed Device Information on Appliances	7-46
Configuring Managed Device Information on RISE Appliances	7-47
Viewing Managed Device Information	7-48
Configuring Network Parameters	7-48
Configuring Sites	7-49
Defining a Site	7-49
Viewing Defined Sites	7-49
Editing a Site	7-50
Configuring Sites Using Subnets	7-50
Setting Interface Speed using NetFlow Interface Capacity	7-52
Creating or Editing a NetFlow Interface	7-52
Configuring DSCP Groups	7-53
Creating a DSCP Group	7-53
Editing a DSCP Group	7-53

Deleting a DSCP Group	7-54
Configuring Application Classification	7-54
Adding More Detail into Dashboard and Application Reports	7-54
About Deeper Application Classification	7-55
About Protocol Packs and Application Classification	7-55
About Packet Analyzer Classic Deep Packet Application Classification	7-56
Creating Deeper Visibility Into Application Traffic	7-56
Creating Custom Applications	7-57
Editing Custom Application Classifications	7-57
Deleting an Application Rule	7-58
Understanding Application Traffic	7-58
Configuring Application Groups	7-60
Creating an Application Group	7-60
Editing or Deleting an Application Group	7-60
Deleting an Application Group	7-61
Filtering Encapsulations	7-61
Setting Up Packet Analyzer Monitoring	7-62
Setting Aggregation Intervals	7-62
Configuring Response Time	7-63
Setting Up Media Monitoring	7-64
Creating RTP Filters	7-65
Configuring URL Collections	7-65
Enabling a URL Collection	7-66
Changing a URL Collection	7-66
Disabling a URL Collection	7-67
Configuring WAAS Monitored Servers	7-67

APPENDIX A

Understanding Packet Analyzer Traffic Sources	A-1
Data Source Overview	A-1
Ports and Hardware Details	A-3
Understanding How the Packet Analyzer Uses SPAN	A-3
A-4	
Understanding How the Packet Analyzer Uses VACLs in Catalyst Switch	A-4
Understanding How the Packet Analyzer Uses NetFlow	A-5
Understanding NetFlow Interfaces	A-6
Understanding NetFlow Flow Records	A-6
Managing NetFlow Data Sources	A-7
Understanding How the Packet Analyzer Uses WAAS	A-7
Understanding How the Packet Analyzer uses CEF	A-8

Understanding UCSE Physical Interfaces A-8

APPENDIX B

Configuring Packet Analyzer Security B-1

Idle Timeout B-1

SSL/TLS Security B-1

Configuring a Self-Signed Certificate B-1

Configuring a CA-Signed Certificate B-2

Configuring SSL/TLS Parameters B-3

Configuring SSL/TLS Ciphersuites B-3

Configuring SSL/TLS Protocols B-3

SSH Security B-4

Configuring SSH Authorized Keys B-4

Configuring SSH Ciphers and MACs B-4

Secure File Transfers B-5

Protecting Against Man-in-the-Middle Attacks B-5

SSH Known Hosts B-5

SSL/TLS CA Certificates B-6

Software Image Upgrades B-6

APPENDIX C

Understanding Packet Analyzer Behavior Reference C-1

Menu Bar C-2

Filters C-2

Quick Filter C-2

Advanced Filter C-3

Displaying Detailed Views C-3

Accessing Context Menus C-3

Performing a Quick Capture C-4

Determining How to Use Sites to View Data C-4

Filtering Traffic for Viewing on the Dashboards C-4

Filtering Data Using Global Search C-5

Switching Chart Formats Using the Chart View / Table View C-5

Accessing Other Tasks Using Mouse-Over for Details C-6

Changing the Time Interval Using Zoom/Pan Charts C-6

Using Sort Grid to Change Sort Order C-6

Displaying Bits or Bytes or Packets in Charts C-7

Statistics C-7

Context-Sensitive Online Help C-7

Feedback C-7

APPENDIX D

GUI Field Descriptions D-1

Setup User Interface Windows	D-1
Create SPAN Session Dialog Box	D-2
Packet Analyzer Data Sources Dialog Box	D-3
Edit SPAN Session Dialog Box	D-3
SNMP Credential Options in Packet Analyzer Data Sources Window	D-4
Device System Information Dialog Box	D-5
Alarm Configuration Window	D-5
Threshold Configuration Window	D-6
Host Alarm Thresholds Window	D-6
Conversation Alarm Thresholds Window	D-7
Application Alarm Thresholds Configuration Window	D-7
Response Time Alarm Threshold Configuration Window	D-8
DSCP Alarm Threshold Configuration Window	D-8
RTP Streams Threshold Configuration Window	D-9
Voice Signaling Threshold Configuration Window	D-10
NetFlow Interface Threshold Configuration Window	D-11
Video Stream Threshold Configuration Window	D-11
Video MDI Stream Threshold Configuration Window	D-12
Router System Information Window	D-12
Switch/Managed Device System Information	D-13
NBAR Interfaces Window	D-14
Site Configuration Window	D-14
Subnet Detection Window	D-15
Sites Window	D-15
Add NetFlow Interface Window	D-15
DSCP Group Setup Dialog Box	D-16
DSCP Group Label Formats	D-16
Application Window	D-17
Applications Window	D-18
URL-Based Applications Window	D-19
Response Time Configuration Window	D-20
Media Monitor Setup Window	D-20
URL Collection Configuration Window	D-21
NetFlow Export Template Window	D-22
Add Managed Device	D-23
Monitor User Interface Windows	D-24
All Alarms Table	D-30

Applications Detail Window	D-31
Application Groups Detail Window	D-31
Application Response Time (ART) Metrics	D-31
Client Server Application Responses Window	D-33
Client-Server Application Transactions Window	D-34
Client-Server Network Responses Window	D-34
DSCP Detail Window	D-35
Host Detail Window	D-35
Interfaces Stats Table	D-36
Last 50 Alarms Table	D-37
Server Application Responses Window	D-38
Server Application Transactions Window	D-38
Server Network Responses Window	D-39
Calls Table	D-39
RTP Stream for Selected Call Report Statistics	D-40
Video Signaling Channel	D-40
Video Stream Conversations	D-41
Media Signaling Sessions	D-42
RTP Stream for Selected Media Signaling Session	D-42
RTP Conversations Table	D-43
Capture User Interface Windows	D-43
Capture Analysis Window	D-43
Capture Session Fields	D-44
Capture Setting Fields	D-44
Custom Decode Filter Dialog Box	D-47
Custom Decode Subexpressions Fields	D-48
Error Scan Window	D-49
Hardware Filter Dialog Box	D-49
Cisco Security Packet Analyzer Decode Window	D-50
Software Filter Dialog Box	D-50
Capture Query Fields	D-52
Administration User Interface Windows	D-53
System Overview	D-54
SNMP Agent	D-55
E-Mail Setting	D-55
Preferences	D-55
New User Dialog Box	D-56
User Privileges	D-57
TACACS+ Authentication and Authorization	D-57
Current User Sessions	D-58

Report Descriptions **D-58**

APPENDIX E

Troubleshooting Network and Packet Analyzer Issues **E-1**

Resolving Typical Packet Analyzer Issues **E-1**

Troubleshooting Login Issues **E-2**

Understanding Typical Error Messages **E-3**

Frequently Asked Questions about Packet Analyzer Behavior **E-3**

Troubleshooting WAAS Data Issues **E-4**

Troubleshooting Video Streams **E-5**

Using the CLI to Troubleshoot Issues **E-5**

Locating Packet Drops **E-5**

Handling an Unresponsive Packet Analyzer **E-6**

Using the CLI to Troubleshoot Performance Agent (PA) **E-6**