Overview

This chapter contains information about the Cisco Security Packet Analyzer software and describes task overviews.

This chapter contains the following sections:

Introducing Cisco Packet Analyzer

The Cisco Security Packet Analyzer (Packet Analyzer) software is a network monitoring and analysis tool that combines flow-based and packet-based analysis into a single tool set. Packet Analyzer software provides network operations and engineering with user, command line, and application programming interfaces that you use for traffic analysis of applications, hosts, and conversations, performance-based measurements on application, server, and network latency, quality of experience metrics. as well as ways to see deeper into your network. The robust graphical user interface makes traffic monitoring and troubleshooting simple and cost-effective.

This chapter contains an overview on ways to use Packet Analyzer to monitor and analyze your network traffic. See Table 1-1 for details on high-level function areas and how they map to the user interface.

Table 1-1 Packet Analyzer Task Areas

Task Area	Menu Mapping	Function Description	Used By
Plan and Prepare	Setup menu	Create a list of your network performance goals. Set expected goals and limits for response time, expected ranges for MOS values, bandwidth usage per application, and utilization on critical WAN links. Determine on which performance issues you want to concentrate.	Network Engineers, Designers, and Architects
Monitor and Analyze	Home, Capture, Analyze and Monitor menus	View dashboards which give you a quick view of traffic performance information, and various incidents. Use interactive reports filter data when monitoring specific network traffic and troubleshooting problems. Monitor your network and perform other day-to-day operations related to proactive and reactive traffic analysis and troubleshooting. Analyze QoS policy traffic using alarms, syslogs, traps, and e-mail alerts. See Monitoring and Analyzing Traffic and Capturing and Decoding Packets.	Network Engineers, NOC Operators, and Service Operators
Administer	Administer menu	Change default system display, notification, and user settings, as well as manage database access control and view system diagnostics. See Performing User and System Administration.	Network Engineers

Table 1-1 Packet Analyzer Task Areas (continued)

Task Area	Menu Mapping	Function Description	Used By
Deploy	Setup and Admin menus	Configure devices to share data with Packet Analyzer. Configure managed devices and data sources. Perform customized setup of Packet Analyzer including sites, alarms and thresholds, scheduled exports, and so on. Monitor an extended level of your managed device's data (health and interface information). Determine which locations are ingress or egress points of a logical network boundary (aggregation layer, core, campus edge, and so on) that can offer valuable insights into the network activity within that partition. Create a baseline of current metrics including applications, bandwidth per application, top conversations and hosts, QoS values used in the network, unrecognized protocols, and current server and end-to-end response time measurements. See Customizing Cisco Packet Analyzer.	Network Engineers, Designers, and Architects
Troubleshoot	Capture, Analyze and Monitor menus	Resolve common Packet Analyzer issues including login problems and unresponsiveness, understand error messages, and troubleshoot network issues using Packet Analyzer. See Troubleshooting Network and Packet Analyzer Issues.	Network Engineers, NOC Operators, and Service Operators

Overview of the Packet Analyzer Platforms

Packet Analyzer is supported on a variety of platforms. This guide does not discuss platforms, but focuses on functions and capabilities.

For a list of Packet Analyzer models and their features and capabilities, see the data sheets in Products & Services on Cisco.com.

It is important to note that the portfolio of Packet Analyzer models differ in memory, performance, disk size, and other capabilities. Therefore, some allow for more features and capabilities (for example, the amount of memory allocated for capture).

Throughout this guide, there may be notes explaining that some features apply only to specific platforms. If there is no note, then that feature or aspect applies to all Packet Analyzer platforms.

How to Use Packet Analyzer to Analyze Your Traffic

The Cisco Packet Analyzer software helps you to address the following major areas:

- Network Layer Traffic Analysis. Packet Analyzer provides comprehensive traffic analysis to identify what applications are running over the network, how much network resources are consumed, and who is using these applications. Packet Analyzer software offers a rich set of reports with which to view traffic by Hosts, Application, or Conversations. See the discussions about Dashboards, starting with Using Traffic Summary, page 3-4.
- Application Response Time. Packet Analyzer can provide passive measurement of TCP-based applications for any given server or client, supplying a wide variety of statistics like response time, network flight time, and transaction time. See Using Response Time Summary, page 3-5.
- Voice Quality Analysis. Packet Analyzer provides application performance for real time applications like Voice and video. Packet Analyzer can compute MOS for voice and MDI for video, as well as provide RTP analysis for the media stream. See Analyzing Media, page 3-32.
- Advanced Troubleshooting. Packet Analyzer provides robust capture and decode capabilities for packet traces that can be triggered or terminated based on user-defined thresholds. See Application Performance Monitoring Using Capture and Decode, page 4-5.
- WAN Optimization insight. Packet Analyzer provides insight into WAN Optimization offerings that compress and optimize WAN Traffic for pre- and post-deployment scenarios. This is applicable for Optimized and Passthru traffic. See
- Open instrumentation. Packet Analyzer is a mediation and instrumentation product offering, and provides a robust API that can be used by partner products as well as work with customer-created applications. Contact your account representative for a copy of the *Cisco Security Packet Analyzer API Programmer's Guide*.

To understand which types of monitoring are supported by specific Packet Analyzer data sources, see Table 1-2.

Table 1-2 Data Source Monitoring Capabilities

	Monitoring Capabilities				
Data Sources	**Capture**	**Traffic**	**ART**	**RTP/Voice**	**URL**
SPAN/VACL/ERSPAN	Yes	Yes	Yes	Yes	Yes
WAAS	No	Yes	Yes	No	No
NetFlow	No	Yes	No	No	No

For information on which data sources Packet Analyzer uses to deliver this functionality, see Understanding Packet Analyzer Traffic Sources.

Before You Begin

Depending on your Packet Analyzer, ensure the following list of requirements are complete before you use Packet Analyzer. For detailed instructions, see your platform installation guide, except where noted:

- Reset your Packet Analyzer root password
- Set up a data source to send traffic to the Packet Analyzer
- Configure access to the Packet Analyzer user interface or CLI
- Synchronize your Packet Analyzer to the standard time source outside the Packet Analyzer in addition to the router or switch (depending on your platform). For detailed instructions, see Synchronizing Your System Time, page 5-5.

For optional advanced customizations, such as adding sites or configuring alarms and thresholds, see Advanced Configuration Overview, page 7-2.