



TCA6000 and TCA6500 Timing Clients

Installation and Configuration Guide



Modified: 2018-01-30

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

TCA6000 and TCA6500 Timing Clients Installation and Configuration Guide
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

Revision History
January 2018—Release 3.9.0.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the TCA6000 and TCA6500 Timing Clients	xv
	Documentation Conventions	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvi
Part 1	TCA6000 and TCA6500 Timing Client Overview	
Chapter 1	TCA6000 and TCA6500 Timing Client Description	3
	TCA6000 and TCA6500 Timing Client Description	3
	TCA6000 and TCA6500 Chassis Overview	3
Part 2	Installing and Setting Up a TCA6000 or TCA6500 Timing Client	
Chapter 2	Installing and Setting Up a TCA6000 or TCA6500 Timing Client	9
	Unpacking the TCA6000 or TCA6500 Timing Client	9
	Requirements for Installing a TCA6500 Timing Client	9
	Reserving an IP Address for the TCA6000 or TCA6500 Timing Client	10
	Installing the TCA6000 or TCA6500 Timing Client	10
	Recommended Mounting Guidelines for the Antenna (TCA6500 Timing Client)	10
	Optimal GPS Antenna Mounting Conditions	11
	Minimal TCA6500 Timing Client Installation Conditions	11
	Mounting the Optional Antenna	11
	Changing the Password of Admin User Account	12
	Assigning an IP Address to the TCA6000 or TCA6500 Timing Client	14
	Visually Testing the TCA6000 or TCA6500 Timing Client	16
	Verifying the Product T1/E1 Interface Support	16
Part 3	Configuring and Upgrading the TCA6000 or TCA6500 Timing Client	
Chapter 3	Configuring a TCA6000 or TCA6500 Timing Client	19
	TCA User Accounts Overview	19
	Guidelines for User Account Management	20
	Dynamic SSL Certificate Overview	21
	Accessing the User Interface	22
	Requirements for Using the Graphical User Interface	22
	Accessing the Graphical User Interface	22
	Changing/Resetting the Login Password for Admin User	26
	Changing the IP Address	28

Setting IEEE 1588-2008 Precision Time Protocol (PTP) Parameters	31
Setting NTP Parameters	33
Enabling the NTP Support	34
Creating an NTP Association Entry	35
Modifying an Existing NTP Association Entry	37
Adding an NTP Association Entry	37
Deleting an Existing NTP Association Entry	38
Configuring the MD5 Key List	38
Configuring Alarms	39
Configuring Traps	40
Specifying SNMPv3 Contacts	41
Creating Trap Targets	42
Editing Trap Targets	42
Deleting Trap Targets	42
Creating SNMPv3 Users	43
Editing SNMPv3 Users	44
Deleting SNMPv3 Users	44
Managing TCA User Accounts	45
Creating an User Account	45
Modifying an Existing User Account	46
Deleting an Existing User Account	47
Changing the Login Password for Read/Write User	47
Configuring User Authentication through RADIUS	49
Adding a New RADIUS Authentication Server Entry	51
Deleting a RADIUS Authentication Server Entry	52
Modifying a RADIUS Authentication Server Entry Details	52
Configuring Authentication Order	52
Configuring RADIUS Accounting	53
Adding a New RADIUS Accounting Server Entry	55
Deleting a RADIUS Accounting Server Entry	55
Modifying a RADIUS Accounting Server Entry Details	56
Specifying Alarm Recipient E-Mail Address Destinations	56
Adding a User to the E-Mail List	56
Removing Users from the Alarm Event Recipient List	57
Resetting Factory Defaults	58
Stopping and Restarting the TCA6000 or TCA6500 Timing Client	58
Chapter 4 Upgrading the TCA6000 and TCA6500 Software	61
Upgrade Requirements	61
Selecting Between the Pre-Installed Software Images Using a GUI/Browser	62
Upgrading the Software Using a GUI/Browser	63
Selecting Between the Pre-Installed Software Images Using the CLI	65
Upgrading the Software Using the CLI	66
Performing Basic Configurations Using Setup Wizard through GUI	68

Part 4	Understanding the TCA6000 and TCA6500 GUI	
Chapter 5	Understanding the TCA6000 and TCA6500 Login Page	77
	Login Page Description	77
	Accessing the Login Page	77
	Understanding the Login Page	78
Chapter 6	Understanding the TCA6000 and TCA6500 Status Page	81
	Understanding System LEDs	81
	Status Page Description	81
	Accessing the Status Page	81
	Understanding the Status Page	82
	The Status Page—System Pane	83
	The Status Page—Alarm Pane	84
	The Status Page—E1 Pane	86
	The Status Page—Timing Pane	88
	The Status Page—PTP Pane	90
	The Status Page—NTP Pane	93
	The Status Page—GPS Pane (When GPS Option Is Connected)	95
	The Status Page—Resource Pane	97
Chapter 7	Understanding the TCA6000 and TCA6500 Config Page	99
	Config Page Description	99
	Accessing the Config Page	99
	Understanding the Config Page	100
	The Config Page—Network Pane	101
	The Config Page—Timing Pane	103
	The Config Page—E1 Pane	105
	The Config Page—PTP Pane	108
	TCA6000 and TCA6500 Timing Client Configurable Profiles	110
	The Config Page—NTP Pane	112
	The Config Page—Trap Pane	115
	The Config Page—SNMPv3 Pane	116
	The Config Page—Users Pane	118
	The Config Page—Profile Pane	119
	The Config Page—RADIUS Pane	121
Chapter 8	Understanding the TCA6000 and TCA6500 Admin Page	125
	Admin Page Description	125
	Accessing the Admin Page	125
	Understanding the Admin Page	125
	The Admin Page—Password Pane	126
	The Admin Page—Alarm Pane	127
	The Admin Page—Service Pane	131
	The Admin Page—Upgrade Pane	133
	The Admin Page—Config Pane	134
	The Admin Page—Remote Log Pane	137
	The Admin Page—Web-Session Pane	138

Chapter 9	Understanding the TCA6000 and TCA6500 Debug Tool Page	139
	Debug Tool Page Description	139
	Accessing the Debug Tool Page	139
	Understanding the Debug Tool Page	139
	The Debug Tool Page—Processes Pane	140
	The Debug Tool Page—Kernel Logs Pane	141
	The Debug Tool Page—Registers Pane	141
Chapter 10	Understanding the TCA6000 and TCA6500 Log Page	143
	Log Page Description	143
	Accessing the Log Page	143
	Understanding the Log Page	143
	The Log Page—EventLog Pane	144
	The Log Page—SysLog Pane	145
	The Log Page—AuthLog Pane	146
	The Log Page—Daemon Pane	147
Part 5	Troubleshooting a TCA6000 or TCA6500 Timing Client	
Chapter 11	Troubleshooting a TCA6000 or TCA6500 Timing Client	151
	Event States and Alarm Types	151
	Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log	152
Part 6	Appendixes	
Appendix A	Using Telnet with the TCA6000 and TCA6500 Timing Clients	159
	Accessing the Timing Client Using the CLI	159
	Changing the IP Address of the Timing Client using the CLI	160
	Resetting the Passwords of Both Admin User Account and Enable Mode to Factory Defaults	161
	Using the CLI to View Status and Configuration Parameters	162
	Options That You Can View in the CLI	162
	Viewing an Option in the CLI	168
	Using the CLI to Configure Timing Client Parameters	168
	Elements that You Can Configure in the CLI	168
	Using the CLI to Configure the Timing Client	179
	Accessing the Timing Client Using SSH	180
Appendix B	Using the CLI to Configure PTP and Network Interface Parameters	181
	Timing Client PTP Functions	181
	PTP Profile Types	181
	PTP Profile Configuration	183
	Default Profile Configuration Command	184
	Brilliant/Juniper Type I Profile Configuration Command	185
	Telecom Profile—Without Signaling Configuration Command	186
	Telecom Profile—With Signaling Configuration Command	187
	PTP Over Ethernet Profile Configuration Command	189

	Status Commands	189
	Sync Source Selection	190
	Configuration	190
	Status Commands	191
	Ethernet Port Network Configuration	191
	Configuration	191
	Status Commands	192
	VLAN Port Association (optional)	192
	Configuration Commands	192
	Status Commands	193
	Static Route IP (optional)	194
	Configuration Commands	194
	Status Commands	194
	Examples	194
Appendix C	Using the CLI to Configure NTP Parameters	197
	NTP Mode	197
	Enabling the NTP Support in the Timing Clients using the CLI	197
	NTP Association Configuration or Status	198
	Configuration Commands	199
	Status Commands	199
	Start, Restart, and Stop Commands—NTP	199
Appendix D	Using the CLI to Configure User Authentication and RADIUS	
	Accounting	201
	User Authentication	201
	Configuration Commands	201
	Status Commands	202
	RADIUS Accounting	202
	Configuration Commands	202
	Status Commands	203
Appendix E	Specifications	205
	Physical Dimensions	205
	Power Specifications	205
	Environmental Specifications	206
Appendix F	Agency Compliance	207
	Agency Compliance	207
Appendix G	Cable Specification	209
	Console Cable Specification	209
Appendix H	Warranty and Support	211
	Requesting Technical Support	211
	Self-Help Online Tools and Resources	211
	Returning a Hardware Component to Juniper Networks, Inc.	212

List of Figures

Part 1	TCA6000 and TCA6500 Timing Client Overview	
Chapter 1	TCA6000 and TCA6500 Timing Client Description	3
	Figure 1: TCA6000 and TCA6500 Timing Client, Front View	4
	Figure 2: TCA6000 and TCA6500 Timing Client, Rear View	5
Part 3	Configuring and Upgrading the TCA6000 or TCA6500 Timing Client	
Chapter 3	Configuring a TCA6000 or TCA6500 Timing Client	19
	Figure 3: TCA6000 or TCA6500 Timing Client Login Page	23
	Figure 4: Timing Client Status Page—System Pane	24
	Figure 5: Admin Users—Resetting the Forgotten Password	25
	Figure 6: Non-admin Users—Resetting the Forgotten Password	26
	Figure 7: Timing Client Admin Page—Password Pane	27
	Figure 8: Timing Client Config Page—Network Pane	30
	Figure 9: Timing Client Config Page—PTP Pane	31
	Figure 10: Timing Client Admin Page—Config Pane	34
	Figure 11: Timing Client Config Page—NTP Pane	36
	Figure 12: Timing Client Admin Page—Alarm Pane	40
	Figure 13: Timing Client Config Page—Trap Pane	41
	Figure 14: Timing Client Config Page—SNMPv3 User Pane	44
	Figure 15: Timing Client Config Page—Users Pane	46
	Figure 16: Timing Client Config Page—Profile Pane	48
	Figure 17: Timing Client Config Page—RADIUS Pane (Authentication)	50
	Figure 18: Timing Client Config Page—RADIUS Pane (Accounting)	54
	Figure 19: Timing Client Admin Page—Alarm Pane	57
	Figure 20: Timing Client Admin Page—Config Pane	58
	Figure 21: Timing Client Admin Page—Upgrade Pane Showing the Current Image	59
	Figure 22: Timing Client Admin Page—Upgrade Pane Showing the New Image	60
Chapter 4	Upgrading the TCA6000 and TCA6500 Software	61
	Figure 23: Timing Client Admin Page—Upgrade Pane	65
	Figure 24: Setup Wizard Page 1	68
	Figure 25: Setup Wizard Page 2	70
	Figure 26: Setup Wizard Page 3	71
	Figure 27: Setup Wizard Page 4	72
	Figure 28: Setup Wizard Page 5	74

Part 4	Understanding the TCA6000 and TCA6500 GUI	
Chapter 5	Understanding the TCA6000 and TCA6500 Login Page	77
	Figure 29: TCA6000 or TCA6500 Login Page	78
Chapter 6	Understanding the TCA6000 and TCA6500 Status Page	81
	Figure 30: Timing Client Status Page—System Pane	82
	Figure 31: Timing Client Status Page—System Pane	83
	Figure 32: Timing Client Status Page—Alarm Pane	85
	Figure 33: Timing Client Status Page—E1 Pane	86
	Figure 34: Timing Client Status Page—Timing Pane	88
	Figure 35: Timing Client Status Page—PTP Pane	90
	Figure 36: Timing Client Status Page—NTP Pane	93
	Figure 37: Timing Client Status Page—GPS Pane	95
	Figure 38: Timing Client Status Page—Resource Pane	97
Chapter 7	Understanding the TCA6000 and TCA6500 Config Page	99
	Figure 39: Timing Client Config Page—Network Pane	100
	Figure 40: Timing Client Config Page—Network Pane	101
	Figure 41: Timing Client Config Page—Timing Pane	103
	Figure 42: Timing Client Config Page—E1 Pane	105
	Figure 43: Timing Client Config Page—PTP Pane	108
	Figure 44: Timing Client Config Page—NTP Pane	112
	Figure 45: Timing Client Config Page—Trap Pane	115
	Figure 46: Timing Client Config Page—SNMPv3 Pane	116
	Figure 47: Timing Client Config Page—Users Pane	118
	Figure 48: Timing Client Config Page—Profile Pane	119
	Figure 49: Timing Client Config Page—RADIUS Pane	121
Chapter 8	Understanding the TCA6000 and TCA6500 Admin Page	125
	Figure 50: Timing Client Admin Page—Password Pane	126
	Figure 51: Timing Client Admin Page—Alarm Pane	127
	Figure 52: Timing Client Admin Page—Service Pane	131
	Figure 53: Timing Client Admin Page—Upgrade Pane	133
	Figure 54: Timing Client Admin Page—Config Pane	134
	Figure 55: Timing Client Admin Page—Remote Log Pane	137
	Figure 56: Timing Client Admin Page—Web-Session Pane	138
Chapter 9	Understanding the TCA6000 and TCA6500 Debug Tool Page	139
	Figure 57: Timing Client Debug Tool Page—Processes Pane	140
	Figure 58: Timing Client Debug Tool Page—Kernel Logs Pane	141
	Figure 59: Timing Client Debug Tool Page—Registers Pane	142
Chapter 10	Understanding the TCA6000 and TCA6500 Log Page	143
	Figure 60: Timing Client Log Page—EventLog Pane	144
	Figure 61: Timing Client Log Page—SysLog Pane	145
	Figure 62: Timing Client Log Page—AuthLog Pane	146
	Figure 63: Timing Client Log Page—Daemon Pane	147
Part 6	Appendixes	
Appendix G	Cable Specification	209

Figure 64: Console Cable Connectors	210
---	-----

List of Tables

	About the TCA6000 and TCA6500 Timing Clients	xv
	Table 1: Notice Icons	xv
Part 2	Installing and Setting Up a TCA6000 or TCA6500 Timing Client	
Chapter 2	Installing and Setting Up a TCA6000 or TCA6500 Timing Client	9
	Table 2: Antenna Mounting Requirements	10
Part 3	Configuring and Upgrading the TCA6000 or TCA6500 Timing Client	
Chapter 3	Configuring a TCA6000 or TCA6500 Timing Client	19
	Table 3: Login Classes for TCA User Accounts	20
Part 4	Understanding the TCA6000 and TCA6500 GUI	
Chapter 5	Understanding the TCA6000 and TCA6500 Login Page	77
	Table 4: Elements on the Timing Client Login Page	78
Chapter 6	Understanding the TCA6000 and TCA6500 Status Page	81
	Table 5: Elements on the Timing Client Status Page—System Pane	83
	Table 6: Elements on the Timing Client Status Page—Alarm Pane	85
	Table 7: Elements on the Timing Client Status Page—E1 Pane	86
	Table 8: Elements on the Timing Client Status Page—Timing Pane	88
	Table 9: Elements on the Timing Client Status Page—PTP Pane	90
	Table 10: Elements on the Timing Client Status Page—NTP Pane	94
	Table 11: Elements on the Timing Client Status Page—GPS Pane	96
	Table 12: Elements on the Timing Client Status Page—Resource Pane	97
Chapter 7	Understanding the TCA6000 and TCA6500 Config Page	99
	Table 13: Elements on the Timing Client Config Page—Network Pane	101
	Table 14: Elements on the Timing Client Config Page—Timing Pane	103
	Table 15: Elements on the Timing Client Config Page—E1 Pane	105
	Table 16: Elements on the Timing Client Config Page—PTP Pane	108
	Table 17: Configuration for Each Profile	111
	Table 18: Elements on the Timing Client Config Page—NTP Pane	113
	Table 19: Elements on the Timing Client Config Page—Trap Pane	115
	Table 20: Elements on the Timing Client Config Page—SNMPv3 Pane	117
	Table 21: Elements on the Timing Client Config Page—Users Pane	118
	Table 22: Elements on the Timing Client Config Page—Profile Pane	120
	Table 23: Elements on the Timing Client Config Page—RADIUS Pane	121
Chapter 8	Understanding the TCA6000 and TCA6500 Admin Page	125

	Table 24: Elements on the Timing Client Admin Page—Password Pane	126
	Table 25: Elements on the Timing Client Admin Page—Alarm Pane	127
	Table 26: Description of Alarm Names	128
	Table 27: Elements on the Timing Client Admin Page—Service Pane	131
	Table 28: Elements on the Timing Client Admin Page—Upgrade Pane	133
	Table 29: Elements on the Timing Client Admin Page—Config Pane	135
	Table 30: Elements on the Timing Client Admin Page—Remote Log Pane	137
	Table 31: Elements on the Timing Client Admin Page—Web-Session Pane	138
Chapter 9	Understanding the TCA6000 and TCA6500 Debug Tool Page	139
	Table 32: Elements on the Timing Client Debug Tool Page—Processes Pane . . .	140
	Table 33: Elements on the Timing Client Debug Tool Page—Kernel Logs Pane	141
	Table 34: Elements on the Timing Client Debug Tool Page—Registers Pane . . .	142
Chapter 10	Understanding the TCA6000 and TCA6500 Log Page	143
	Table 35: Elements on the Timing Client Log Page—EventLog Pane	144
	Table 36: Elements on the Timing Client Log Page—SysLog Pane	145
	Table 37: Elements on the Timing Client Log Page—AuthLog Pane	146
	Table 38: Elements on the Timing Client Log Page—Daemon Pane	147
Part 5	Troubleshooting a TCA6000 or TCA6500 Timing Client	
Chapter 11	Troubleshooting a TCA6000 or TCA6500 Timing Client	151
	Table 39: Event States	151
	Table 40: Alarm Types	151
	Table 41: Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log	152
Part 6	Appendixes	
Appendix A	Using Telnet with the TCA6000 and TCA6500 Timing Clients	159
	Table 42: CLI Viewing Options	162
	Table 43: Configurable Elements in the CLI	168
Appendix B	Using the CLI to Configure PTP and Network Interface Parameters	181
	Table 44: Configuration Commands	183
	Table 45: Default Routes	194
	Table 46: Network Configurations	195
Appendix C	Using the CLI to Configure NTP Parameters	197
	Table 47: NTP Configuration Commands	198
Appendix E	Specifications	205
	Table 48: Physical Dimensions	205
	Table 49: Power Specifications	205
	Table 50: Environmental Specifications	206
Appendix G	Cable Specification	209
	Table 51: Signal Flow Diagram	209







About the TCA6000 and TCA6500 Timing Clients

- [Documentation Conventions on page xv](#)
- [Requesting Technical Support on page xv](#)

Documentation Conventions

[Table 1 on page xv](#) defines the notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service

support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <http://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

TCA6000 and TCA6500 Timing Client Overview

- [TCA6000 and TCA6500 Timing Client Description on page 3](#)

CHAPTER 1

TCA6000 and TCA6500 Timing Client Description

- [TCA6000 and TCA6500 Timing Client Description on page 3](#)
- [TCA6000 and TCA6500 Chassis Overview on page 3](#)

TCA6000 and TCA6500 Timing Client Description

The TCA6000 and TCA6500 Timing Clients are carrier-class, compact network timing clients that deliver multiple outputs in a cost-efficient, flexible platform. This user manual provides installation and operational information for these Timing Clients to allow successful deployment and operation of the server.

The Timing Clients—designed as network edge timing devices—accurately distribute ITU Stratum timing over IP or MPLS networks when attached to a Stratum 1 reference source, such as the TCA8000 or TCA8500 Timing Servers. When referenced to an accurate timing source, multiple output signals are available in the following formats: T1/E1, Pulse-per-Second (PPS), Pulses per Minute (PPM), PPS2 and 10/5/1 MHz. The TCA6500 Timing Client is also designed to accept a GPS signal from a variety of manufacturers' antennas.



NOTE: The TCA6000 and TCA6500 Timing Clients ship with both T1 and E1 software images installed in the two internal non-volatile memory partitions. By default, the TCA6000 and TCA6500 Timing Clients use the E1 interface type. This manual refers to E1 configuration, alarms, and status but is also applicable to T1 except for some differences in nomenclature that are specific to each frame type. See [“Upgrading the TCA6000 and TCA6500 Software” on page 61](#) to install the software image for the appropriate interface type for the system.

TCA6000 and TCA6500 Chassis Overview

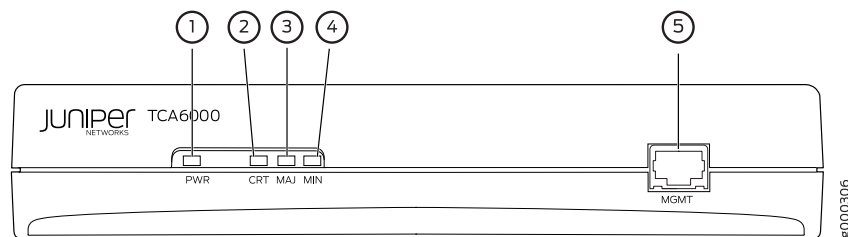
The chassis of both TCA6000 and TCA6500 Timing Clients look similar, only their internal function is different.

The front panel of the Timing Client contains the following components as shown in [Figure 1 on page 4](#):

- 1–Power LED
- 2–Critical alarm LED
- 3–Major alarm LED
- 4–Minor alarm LED
- 5–Craft port

The craft port is used to change the default IP address of the Timing Client. The LEDs display the power status and alarm status of the Timing Client.

Figure 1: TCA6000 and TCA6500 Timing Client, Front View



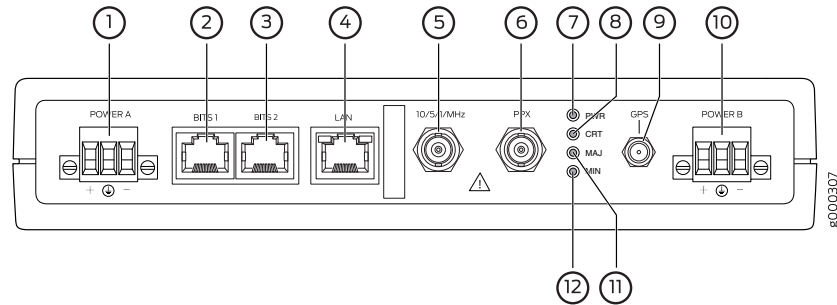
The rear panel of the Timing Client contains the following components as shown in [Figure 2 on page 5](#):

- 1–DC power terminal A
- 2–Building Integrated Timing Supply (BITS) port 1
- 3–BITS port 2
- 4–LAN port
- 5–1/5/10 MHz timing output port
- 6–PPx timing output port
- 7–Power LED
- 8–Critical alarm LED
- 9–GPS antenna port
- 10–DC power terminal B
- 11–Major alarm LED
- 12–Minor alarm LED

A pair of DC terminals each with positive, negative, and ground terminals is used to connect a DC power source to the Timing Client. The LAN port is an RJ45 connector with synch and activity LEDs, which can be used to connect the Timing Client to a PC for managing the Timing Client through an Internet browser. The GPS antenna port is used to connect the Timing Client with an appropriate GPS L1 antenna that receives a minimum GPS signal from a Timing Server. Two BITS ports are used to receive input from BITS

clock sources. Timing output ports are used to deliver 1/5/10 MHz output signal and PPx output signal. The PPx output signal can be PPS, PPM, PPS2, or Pulse-Position Hopping (PPH). The rear LEDs mirror the front LEDs and provides the power status and alarm status of the Timing Client.

Figure 2: TCA6000 and TCA6500 Timing Client, Rear View



PART 2

Installing and Setting Up a TCA6000 or TCA6500 Timing Client

- [Installing and Setting Up a TCA6000 or TCA6500 Timing Client on page 9](#)

CHAPTER 2

Installing and Setting Up a TCA6000 or TCA6500 Timing Client

This chapter describes the procedure to correctly install the Juniper Networks TCA6000 and TCA6500 Timing Clients. Installation is the same for both models, except that the TCA6500 includes an optional antenna (GPS).

- [Unpacking the TCA6000 or TCA6500 Timing Client on page 9](#)
- [Requirements for Installing a TCA6500 Timing Client on page 9](#)
- [Reserving an IP Address for the TCA6000 or TCA6500 Timing Client on page 10](#)
- [Installing the TCA6000 or TCA6500 Timing Client on page 10](#)
- [Recommended Mounting Guidelines for the Antenna \(TCA6500 Timing Client\) on page 10](#)
- [Changing the Password of Admin User Account on page 12](#)
- [Assigning an IP Address to the TCA6000 or TCA6500 Timing Client on page 14](#)
- [Visually Testing the TCA6000 or TCA6500 Timing Client on page 16](#)
- [Verifying the Product TI/EI Interface Support on page 16](#)

Unpacking the TCA6000 or TCA6500 Timing Client

The Timing Client is shipped with the following items to ensure an optimum installation:

- TCA6000 or TCA6500 Timing Client

Requirements for Installing a TCA6500 Timing Client

[Table 2 on page 10](#) lists the items needed to install the TCA6500 Timing Client.

You must use an appropriate GPS L1 antenna (1575.42 MHz) to receive a minimum GPS signal from the Timing Server. The antenna must allow a minimum signal input level of 20 dB with respect to the antenna output for the Timing Server.



NOTE: To calculate whether the external antenna, cable type, and length meets the minimum TCA GPS antenna input, use the following formula:

$$\text{TCA GPS signal input} = \text{antenna gain} - [(\text{cable length}) * (\text{cable loss} / \text{Meter or Feet})]$$

Table 2: Antenna Mounting Requirements

Customer Supplied

- GPS L1 antenna with a frequency band of 1575.42 +/-10 MHz 3 dB bandwidth.
- Antenna mount
- Mounting area clear for at least two meters of any metal or other material that could act as a shield and block the GPS signal
- 160 degree clear view of the sky
- Clamps, cable ties, and so on, to secure cable

Reserving an IP Address for the TCA6000 or TCA6500 Timing Client

The TCA6000 and TCA6500 Timing Clients support both dynamic and static IP addressing. If a static address is required, an IP address must be reserved and assigned for the Timing Client by a network administrator. The DHCP server will always assign a unique address.

Installing the TCA6000 or TCA6500 Timing Client



CAUTION:

- **Ground cable**—Make a ground cable using 8-gauge wire with the supplied ground lug. This should attach to your building's earth ground infrastructure.
- **Power**—Route power connection using 18-22 gauge wire to a 48-volt power distribution frame (fuse position) or fused breaker.

Recommended Mounting Guidelines for the Antenna (TCA6500 Timing Client)

This section describes recommendations for mounting the TCA6500 antenna at a location where the antenna will have GPS satellite visibility. A site survey is highly recommended before any installation. This will determine the best method and location for mounting the antenna. A site survey will also identify additional information such as cable lengths and required mounting materials in order to perform a secure, safe, and reliable installation.

- [Optimal GPS Antenna Mounting Conditions on page 11](#)
- [Minimal TCA6500 Timing Client Installation Conditions on page 11](#)
- [Mounting the Optional Antenna on page 11](#)

Optimal GPS Antenna Mounting Conditions

Ideally, the GPS antenna should be mounted where a 160° clear view of the sky (a 10° angle from horizontal) is available to enable a connection to visible GPS satellites. The ideal mounting location is a roof, tower or an antenna mast, high above any obstruction or any device that may cause signal interference. We recommend a location that has the following characteristics:

- Clear view of the sky in all directions—at least 270°
- Away from high-power transmitters and radar antennas
- At least 3 meters away and at least 1 meter below the highest point of a lightning rod
- Convenient path for running the outdoor coax cable from the GPS antenna to the network

Minimal TCA6500 Timing Client Installation Conditions

The TCA6500 Timing Client can still maintain accurate time when an antenna is mounted in a location that has limited visibility of GPS satellites; however, it is recommended that any obstructions should be minimized. Limitations to satellite visibility for an antenna include overhanging foliage or tall structures. Such structures can block the GPS signal from the antenna and cause gaps in the GPS satellite signal reception. In locations where satellite visibility is limited, consider the following:

- Position the GPS antenna on the side of the structure with good south-facing visibility where more satellites are visible. For example, if you are in the northern hemisphere, place the unit on the southern side of the structure unless that view is restricted or blocked. If that view is restricted or blocked, place the unit on the east or west side of the structure. Avoid the polar side where there are fewer visible satellites.
- Configure the Timing Client to use PTP peer devices on the network as an alternative time source (Sync_Source_Selection).
- Ensure that the GMT time zone parameter is set while you configure the Timing Client.

Mounting the Optional Antenna

Route the coax from the building's ingress to the Timing Client installation site and connect to the GPS server.



WARNING:

- Locate the GPS antenna away from power lines, lighting systems, HVACs, and power circuits.
- When installing the GPS antenna, do not touch power lines or other sources of “live” power.
- Have a qualified technician and or certified electrician perform the installation.

- Observe all local and regulatory standards and ordinances.
- Grounding the unit (metal mast or ground cable to the unit's base) is required for the lightning protection to work properly.

Changing the Password of Admin User Account

Juniper Networks assigns a default user account (admin/admin) with login class as Admin to a TCA6000 or TCA6500 Timing Client for logging in to the Timing Client. You can create and manage Read-Only or Read/Write user accounts in the TCA6000 or TCA6500 Timing Client by logging in as **admin**. For more information about TCA user account management, see [“Managing TCA User Accounts” on page 45](#) and [“TCA User Accounts Overview” on page 19](#).



BEST PRACTICE: Before installing the Timing Client on an active network, change the default password (admin) of the Admin user to maintain secure access to the Timing Client.



NOTE: You can reset passwords of the Admin user and the enable mode to factory defaults through the CLI, GUI, or by resetting the Timing Client. For more information about resetting of passwords, see [“Changing/Resetting the Login Password for Admin User” on page 26](#) and [“Resetting the Passwords of Both Admin User Account and Enable Mode to Factory Defaults” on page 161](#).

To change the password of the Admin user, one of the following methods may be used:

- Configuration through the craft port on the front panel:
 1. Login as **admin**.
 - a. `>admin<cr>`
 - b. `>password: admin<cr>`
 2. Enable privileged commands.
 - a. `>enable<cr>`
 - b. `>password: enable<cr>`
 3. Execute the following command to change the Admin user password:

```
# config password
Please input old password: admin<cr>
Please input new password: admin123<cr>
```

Please re-type new password: admin123<cr>

- Configuration from the management interface through the Ethernet port on the back panel:
 1. Connect a standard Ethernet cable between the Timing Client, Lan1, and the network port of the PC.
 2. Launch an Internet browser on your PC.
 3. In the **URL** field, type the following default IP address:
http://192.168.0.75
The Timing Client login page appears.
 4. In the **Login** field, enter the following:
admin (Case sensitive—use all “lower” case)
 5. In the **password** field, enter the following:
admin (Case sensitive—use all “lower” case)
 6. Click the **Login** button.
 7. Click the **Admin** tab and locate the **Password** tab across the top tabs of the Admin page.
 8. In the **Hostname** field, enter the name assigned to the Timing Client.
 9. In the **Old Password** field, enter the current password of the Admin user.
 10. In the **New Password** field, enter the new password to replace the old password.
 11. In the **Retype New Password** field, reenter the new password.
 12. Click the **Apply** button to save hostname and password changes to the memory.



NOTE: All the examples in this guide use the default password (admin) for the Admin user.

Assigning an IP Address to the TCA6000 or TCA6500 Timing Client

Juniper Networks assigns a default IP address to a TCA6000 or TCA6500 Timing Client to allow access to the user interface. The default IP address must be changed before installing the Timing Client on an active network. To change the IP address, one of the following methods may be used:

- Configuration through the craft port on the front panel:

1. Log in as **admin**.
 - a. `>admin<cr>`
 - b. `>password: admin<cr>`
2. Enable privileged commands.
 - a. `>enable<cr>`
 - b. `>password: enable`
3. `# config eth0 ip [ip-address] [mask] [gateway]`

- Configuration from the management interface through the Ethernet port on the back panel:

To change the IP address through the Ethernet port:

1. Connect a standard Ethernet cable between the Timing Client, LAN1, and the network port of the PC.
2. Apply power to the Timing Client; the unit can be previously powered.
3. Launch an Internet browser on your PC.
4. In the **URL** field, type the following default IP address:
LAN1—`http://192.168.0.75`
The Timing Client login page appears.
5. In the **Login** field, enter the following:
admin (Case sensitive—use all “lower” case)
6. In the **password** field, enter the following:
admin (Case sensitive—use all “lower” case)

7. Click the **Login** button.
8. Click the **Config** tab if it not already displayed (default).
9. Select the **LAN1** button.
10. Locate Mode in the Network section, select the **Static** or **DHCP** button that will be used to assign the Timing Client an IP address, and perform one of the following:
 - a. Select the **Static** button and enter the following information in the fields above the Mode selection:
 - In the **IP Address** field, enter the IP address to be assigned to the Timing Client.
 - In the **Mask** field, enter the subnet mask to be assigned to the Timing Client.
 - In the **Gateway** field, enter the IP address of the gateway to be assigned to the Timing Client.
 - In the **Primary DNS** field, enter the IP address of the primary DNS to be assigned to the Timing Client.



NOTE: Leave blank, if not required.

- b. In the **Secondary DNS** field, enter the IP address of the secondary DNS to be assigned to the Timing Client.



NOTE: Leave blank, if not required.

Apply, save.

- b. If the **DHCP** button is selected, the DHCP server will automatically provide the Timing Client with IP address information.

Apply, save.

Connect to the network.

- c. Contact a network administrator to enable appropriate settings for the following:
 - Speed (100Mbps, recommended)
 - Duplex (Full-duplex, recommended)
 - Auto negotiation (Disabled, recommended)

Visually Testing the TCA6000 or TCA6500 Timing Client

1. Connect the Timing Client and computer to the local network segment and launch the web browser.



NOTE: The title banner displays TCA6000 as a generic model number for all TCA6000/TCA6500 models. The unique model number for the system configuration is displayed in the Status page.

2. Open the Timing Client webpage by using the new IP address (from above), enter login/password.
3. Click the **Status** button and observe the System page. The following information should be present:
 - Model
 - Board S/N
 - System S/N
 - Software version
 - Hardware version
 - FPGA version
 - Temperature
 - MAC address—LAN1
4. Click the GPS page, and observe the following information:
 - Receiver status = Good
 - Antenna status = Good
 - Satellite status = Acquired

Verifying the Product T1/E1 Interface Support

The TCA6000 and TCA6500 Timing Clients ship with both T1 and E1 software images installed in the two internal non-volatile memory partitions. By default, the TCA6000 and TCA6500 Timing Clients use the E1 interface type. To select the T1 interface type, see [“Upgrading the TCA6000 and TCA6500 Software” on page 61](#).

PART 3

Configuring and Upgrading the TCA6000 or TCA6500 Timing Client

- [Configuring a TCA6000 or TCA6500 Timing Client on page 19](#)
- [Upgrading the TCA6000 and TCA6500 Software on page 61](#)

CHAPTER 3

Configuring a TCA6000 or TCA6500 Timing Client

This chapter describes the procedure to configure the Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are described in this chapter:

- [TCA User Accounts Overview on page 19](#)
- [Dynamic SSL Certificate Overview on page 21](#)
- [Accessing the User Interface on page 22](#)
- [Requirements for Using the Graphical User Interface on page 22](#)
- [Accessing the Graphical User Interface on page 22](#)
- [Changing/Resetting the Login Password for Admin User on page 26](#)
- [Changing the IP Address on page 28](#)
- [Setting IEEE 1588-2008 Precision Time Protocol \(PTP\) Parameters on page 31](#)
- [Setting NTP Parameters on page 33](#)
- [Configuring Alarms on page 39](#)
- [Configuring Traps on page 40](#)
- [Creating SNMPv3 Users on page 43](#)
- [Editing SNMPv3 Users on page 44](#)
- [Deleting SNMPv3 Users on page 44](#)
- [Managing TCA User Accounts on page 45](#)
- [Changing the Login Password for Read/Write User on page 47](#)
- [Configuring User Authentication through RADIUS on page 49](#)
- [Configuring RADIUS Accounting on page 53](#)
- [Specifying Alarm Recipient E-Mail Address Destinations on page 56](#)
- [Resetting Factory Defaults on page 58](#)
- [Stopping and Restarting the TCA6000 or TCA6500 Timing Client on page 58](#)

TCA User Accounts Overview

Juniper Networks assigns a default user account (admin/admin) with login class as Admin to a TCA6000 or TCA6500 Timing Client for logging in to the Timing Client. The

user logging in to the Timing Client using the Admin user account can configure the Timing Client and create, delete or modify user accounts with login class as Read-Only or Read/Write.

The TCA software supports three predefined login classes to define the access privileges for the user accounts in your Timing Client. [Table 3 on page 20](#) defines the login classes predefined in the TCA software.

Table 3: Login Classes for TCA User Accounts

Login Class	Access Privilege	Description
Admin	Create, Delete, or Modify	User can: <ul style="list-style-type: none"> • Configure all Timing Client features or parameters through CLI or WEB. • View all Timing Client configuration or log details through CLI or WEB.
Read/Write	Modify	User can: <ul style="list-style-type: none"> • Configure Timing Client features or parameters through CLI or WEB except Admin user functionalities such as creation, deletion, and modifying of user accounts. • View Timing Client configuration or log details through CLI or WEB except the following Admin user functionalities: <ul style="list-style-type: none"> • Viewing command history of other user accounts. • Viewing information about user accounts.
Read-Only	Show view	User can: <ul style="list-style-type: none"> • View Timing Client configuration or log details through CLI or WEB except the following Admin user functionalities: <ul style="list-style-type: none"> • Viewing command history of other user accounts. • Viewing information about user accounts.

The TCA software creates a separate log file for each user account to store the commands executed by the corresponding user. The software stores the session ID and timestamp in the log file to identify the various sessions for that particular user. The software deletes the log file created for the user account, when the Admin user deletes any Read-Only or Read/Write user account.



NOTE: The software can store only a maximum of 150 commands in a log file.

Guidelines for User Account Management

Keep in mind the following considerations when you (Admin) configure user accounts:

- The software supports only five user accounts.
- You cannot delete the default Admin user account assigned by Juniper Networks.
- You cannot create another Admin user account.

- The username should be 4 to 12 characters long. The characters can only include alphanumeric and underscore. No other special characters are allowed.
- The username should be unique.
- The password should be 4 to 12 characters long. The characters can include alphanumeric and special characters (that is, !@#\$_).

Dynamic SSL Certificate Overview

The TCA 6000 or 6500 Timing Client enables you to access the GUI through Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) based on the web mode configured by the Admin user. The Admin user can configure the Timing Client to use the customized key and certificate instead of the default key and certificate, when the GUI is accessed through HTTPS. By default, the Timing Client uses the default key and certificate when the GUI is accessed through HTTPS.

The Admin user can download the customized key and certificate files of **.pem** format in the Timing Client through CLI or GUI. The downloaded key file is stored as an **ssl_key.pem** file in the **etc/config** path. The downloaded certificate file is stored as an **ssl_cert.pem** file in the **etc/config** path. The Admin user can generate the customized files by using OpenSSL or FIPS 140-2 capable OpenSSL as trusted certification authority. For complete information and source of OpenSSL utility, see <http://www.openssl.org/>.

When you access the GUI through HTTPS, the Timing Client checks for the **ssl_key.pem** and **ssl_cert.pem** files in the **etc/config** path. If any one of the files is not available, the Timing Client uses the default key and certificate. If the files are available, the Timing Client checks the BEGIN header and the END footer in both the files. If the header and footer are valid in both the files, the Timing Client compares the key file with the certificate file. On successful match, the Timing Client loads the GUI and generates a syslog.

The Timing Client does not load the GUI but generates a syslog during the following scenarios:

- Mismatch identified between the key and certificate files.
- Invalid header or footer identified in one of the files.
- Validity of any file got expired.

The Admin user must keep the following conditions in mind when uploading the customized files:

- After uploading both the files, you must reboot the Timing Client for the changes to take effect.
- The Timing Client uses the default key and certificate if both or any one of the customized files is unavailable.
- You cannot modify the downloaded files but you can replace them with another ones.
- You should use only Secure Hash Algorithm (SHA-1) and RSA (1024 bits) cryptographic algorithms while generating the customized key and certificate files.

Accessing the User Interface

You can configure the TCA6000 or TCA6500 Timing Client using one of the following methods:

- Graphical user interface (GUI)
- Telnet
- Secured shell (SSH)

This chapter describes how to access the GUI. Accessing the Timing Client using Telnet and SSH is described in [“Using Telnet with the TCA6000 and TCA6500 Timing Clients” on page 159](#).

Requirements for Using the Graphical User Interface

To use the TCA6000 or TCA6500 GUI, log in to the embedded Web server with an Internet browser. The following browsers and versions are supported:

- Internet Explorer version 11.x or later
- Firefox version 1.5.0.7 or later (Firefox 3.0 is currently not supported)

The Web GUI is optimized to work and appear better in a 1280*1024 display resolution.

Accessing the Graphical User Interface

To access the GUI:

1. Open an Internet browser.
2. In the **address** or **URL** field enter the IP address assigned to the Timing Client to be accessed, using the following command:

`http://ip_address`

The Login page appears. See [Figure 3 on page 23](#).

Figure 3: TCA6000 or TCA6500 Timing Client Login Page

JUNIPER
NETWORKS

TCA6000 Timing Client

Username
Password

Forgot password?
Enter username and click [here](#)

● Sync Local Time : Mon Jan 2 09:28:23 2017
● Alarms Hostname : TCA6500-2
 PTP mode : Slave
 Clock Identity : f8:c0:01:ff:fe:08:80:a0
 Current Sync Source : Internal
 Hardware Clock Status : FREERUN
 Alarm Status : Critical
 Model : TCA6500-DC
 Location : anywhere
 Software Version : TCA6K-3.7.0-PTP-E1
 Up Time : 3 Hrs 6 min 1 sec

Network Status		
Port	Address	Link State
LAN1	10.85.33.21/255.255.255.0	up/100/Full

MAC: f8:c0:01:08:80:a0

- In the **Username** field enter the username to be used to log in to the server.



NOTE: The default username assigned by the Juniper Networks is admin. You cannot change the default username. You can create new user accounts from the config page by logging in as Admin user.

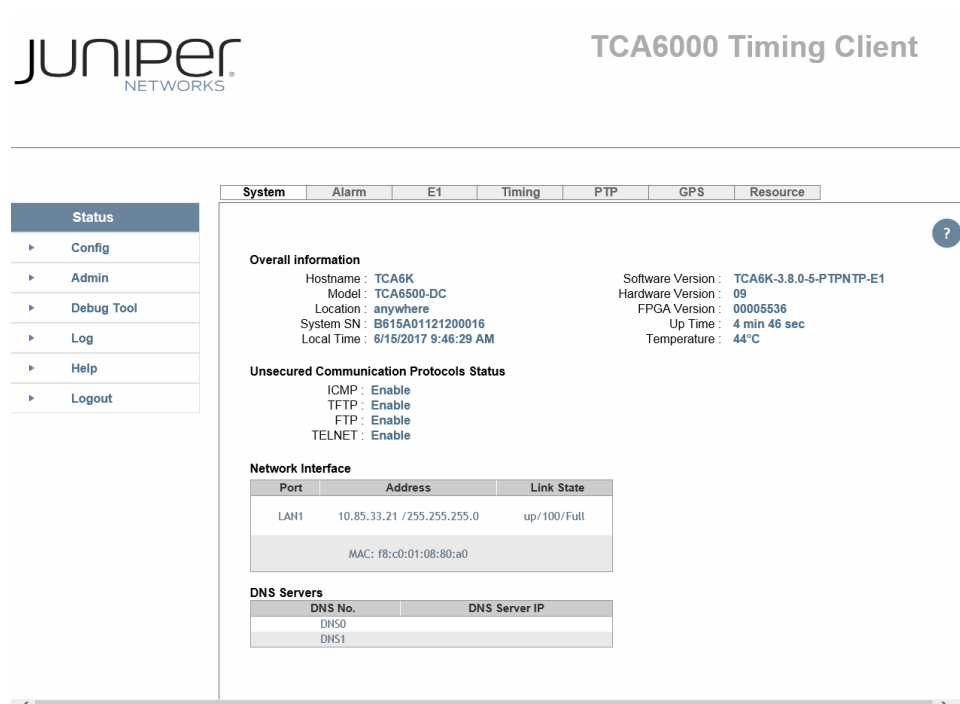
- In the **Password** field enter the password required to log in to the server.



NOTE: The default password assigned by the Juniper Networks is admin. You can change the login password of the Admin user from the admin page.

- Click the **Login** button. The Status page appears. See [Figure 4 on page 24](#).

Figure 4: Timing Client Status Page—System Pane



JUNIPER
NETWORKS

TCA6000 Timing Client

Status

- Config
- Admin
- Debug Tool
- Log
- Help
- Logout

System Alarm E1 Timing PTP GPS Resource

Overall information

Hostname : TCA6K
Model : TCA6500-DC
Location : anywhere
System SN : B615A01121200016
Local Time : 6/15/2017 9:46:29 AM
Software Version : TCA6K-3.8.0-5-PTPNTTP-E1
Hardware Version : 09
FPGA Version : 00005536
Up Time : 4 min 46 sec
Temperature : 44°C

Unsecured Communication Protocols Status

ICMP : Enable
TFTP : Enable
FTP : Enable
TELNET : Enable

Network Interface

Port	Address	Link State
LAN1	10.85.33.21 / 255.255.255.0	up/100/Full

MAC: f8:c0:01:08:80:a0

DNS Servers

DNS No.	DNS Server IP
DNS0	
DNS1	

The Timing Client GUI will automatically time out after the timeout period configured using the **config web-timeout** command. The login and password will have to be reentered to gain access to the unit.

- If you have forgotten the password, enter the username and click the **Forgot Password** link.

For Admin user accounts, you will be prompted to contact JTAC with the MAC address to get the master password. See [Figure 5 on page 25](#).

Figure 5: Admin Users—Resetting the Forgotten Password

JUNIPER
NETWORKS

TCA6000 Timing Client

Username
Password

Forgot password?
Enter username and click [here](#)

Please Contact JTAC with your device MAC Address(f8:c0:01:08:80:a0) to get the master password.


Technical Support Phone Line : +1-888-314-JTAC or +1-888-314-5822
Customer Care Contact : www.juniper.net/cm
Website : www.juniper.net

Upon logging in with the master password, the Admin user has to set a new password.

For non-admin user accounts, you will be prompted to enter the username and e-mail ID. Upon successful authentication, you will get the new password in your e-mail. See

[Figure 6 on page 26](#).

Figure 6: Non-admin Users—Resetting the Forgotten Password



TCA6000 Timing Client

Please enter your configured email id

Username

Email-Id

Submit

Go to [login page](#)

● Sync

● Alarms

Local Time : Tue Jan 10 11:53:26 2017

Hostname : TCA6K

PTP mode : Slave

Clock Identity : f8:c0:01:ff:fe:08:80:a0

Current Sync Source : Internal

Hardware Clock Status : FREERUN

Alarm Status : No Alarm

Model : TCA6500-DC

Location : anywhere

Software Version : TCA6K-3.7.0-PTP-T1

Up Time : 5 Hrs 17 min 41 sec

Network Status

Port	Address	Link State
LAN1	10.85.33.21 / 255.255.255.0	up/100/Full

MAC: f8:c0:01:08:80:a0

Changing/Resetting the Login Password for Admin User

We recommend that the TCA6000 or TCA6500 Timing Client login password of the Admin user be changed from the manufacturer set default to maintain secure access to the server.

To change the login password of the Admin user:

1. Click the **Admin** tab.

The Admin page appears. See [Figure 7 on page 27](#).



NOTE: The Admin tab is visible only to the Admin user.

Figure 7: Timing Client Admin Page—Password Pane

2. In the **Hostname** field of the System Name & Password section, enter the hostname to be assigned to the Timing Client.
3. In the **Old Password** field, enter the current password of the Admin user.
4. In the **New Password** field, enter the new password.



NOTE: Passwords are case sensitive and accept alphanumeric characters. Passwords must contain a minimum of four characters.

5. In the **Retype New Password** field, retype the assigned (new) password.
6. Click the **Apply** button.

To reset passwords of the Admin user and the enable mode to factory defaults:

1. Click the **Admin** tab.

The Admin page appears. See [Figure 7 on page 27](#).



NOTE: The Admin tab is visible only to the Admin user.

2. Select the **Default Password** check box.
3. Click the **Apply** button to reset passwords of the Admin user and the enable mode to factory defaults.



NOTE: If you have forgotten the password of the Admin user, you can reset the password to factory default by resetting the Timing Client. For more information about resetting the password by resetting the Timing Client, see [“Resetting the Passwords of Both Admin User Account and Enable Mode to Factory Defaults” on page 161](#).

Changing the IP Address

The TCA6000 and TCA6500 Timing Clients are configured to use the manufacturer's default static IP address assigned to the Ethernet port. The user interface is used to manually change the IP address of the Ethernet port and configure or change VLAN settings for the Ethernet port.



NOTE: You cannot configure Ethernet and VLAN port addresses to be in the same subnet (that is, all logical and physical interfaces should be configured to be in different subnets).

To change the address information for Ethernet port:

1. Click the **Config** tab. The Config page appears. See [Figure 8 on page 30](#).
2. In the **Mode** field, click the **Static** button to activate the address fields.
3. In the **IP Address** field, enter the IP address to be assigned to the Timing Client.



NOTE: After the IP address change, click **Apply**. Access the Timing Client using the new IP address to view and configure the current settings.

4. In the **Mask** field, enter the subnet mask to be assigned to the Timing Client.

5. In the **Gateway** field, enter the IP address of the gateway that will be registered by the Timing Client.
6. In the **Primary DNS** field, enter the IP address of the Primary DNS that will be registered by the Timing Client.



NOTE: Leave blank, if not required.

7. In the **Secondary DNS** field, enter the IP address of the Secondary DNS that will be registered by the Timing Client.



NOTE: Leave blank, if not required.

8. To determine whether an IP address is currently assigned, enter the IP address in the **Ping** field and click **Go**. If the ping goes through, then the IP address is already taken. Otherwise, it is not assigned, and can be used by the Timing Client.

9. Click the **Apply** button to save and implement the changes.

To configure or change VLAN settings for the Ethernet port:


1. Click the **Config** tab. The Config page appears. See [Figure 8 on page 30](#).
2. In the **Mode** field, select the **Static** option button to activate the VLAN address fields.
3. In the **Static Route** field, select an option button to add a static route that defines a gateway IP address for reaching the destination network or delete the static route.
4. In the **VLAN** field, select a VLAN (VLAN1 or VLAN2) for which settings should be configured.
5. In the **IP Address** field, enter the IP address for the selected VLAN.
6. In the **Mask** field, enter the subnet mask assigned to the selected VLAN.
7. In the **Id** field, enter a unique identifier in the range 2 through 4095 that is used to identify the VLAN encapsulation packet.



NOTE: If the ID you have entered is already being used by any other VLAN, a warning message is displayed.

8. In the **Priority** field, enter a priority value for the VLAN header to be used for differential services transporting the packet.
9. In the **Enable** field, select the **Yes** option button to enable VLAN encapsulation for IP packets, or select the **No** option button to disable VLAN encapsulation for IP packets.
10. Click **Apply** to save and implement the changes.

Figure 8: Timing Client Config Page—Network Pane



JUNIPER
NETWORKS

TCA6000 Timing Client

- Status
- Config
- Admin
- Debug Tool
- Log
- Help
- Logout

Network
Timing
E1
PTP
Trap
SNMPv3
Users
RADIUS

Network

LAN : ☒ LAN1

IP Address :

Mask :

Gateway :

Primary DNS :

Secondary DNS :

Domain :

Mode : ☒ Static ☐ DHCP

Speed : Mbps

Duplex :

Auto Negotiation :

Ping :

Static Route

	Network	Mask	Gateway	Interface
<input type="radio"/>	10.85.33.0	255.255.255.0	0.0.0.0	eth0
<input type="radio"/>	0.0.0.0	0.0.0.0	10.85.33.1	eth0

VLAN

VLAN : ☒ VLAN1 ☐ VLAN2

IP Address :

Mask :

Id :

Priority :

Mode : ☒ Static ☐ DHCP

Enable : ☐ Yes ☒ No

Setting IEEE 1588-2008 Precision Time Protocol (PTP) Parameters

The IEEE 1588-2008 Precision Time Protocol (PTP) section on the Config page identifies the parameters that can be set for the TCA6000 or TCA6500 Timing Client to provide synchronization using the Precision Time Protocol. To configure the Timing Client to provide PTP time synchronization:

1. Click the **Config** tab. The Config page appears.

Locate the **PTP** tab across the top of the Config page. See [Figure 9 on page 31](#).

Figure 9: Timing Client Config Page—PTP Pane

The screenshot displays the Juniper Networks TCA6000 Timing Client configuration interface. On the left is a navigation menu with options: Status, Config (selected), Admin, Debug Tool, Log, Help, and Logout. The main content area has tabs for Network, Timing, E1, PTP (selected), Trap, SNMPv3, Users, and RADIUS. The PTP configuration section includes the following fields:

- Telecom Profile: Disabled
- Priority 1: 0
- Priority 2: 1
- Domain Number: 12
- Two Step: No
- Delay Req Mode: Multicast
- Log Mean Delay Req Interval: 32 packet/sec
- Log Mean Announce Interval: 1 packet/2sec
- Log Mean Sync Interval: 32 packet/sec
- Announce Receipt Timeout: 5 Second
- DSCP: 46

An 'Apply' button is located below these fields. Below the PTP section is the 'Acceptable Master List' table:

	IP address
<input type="radio"/>	10.85.33.23

'Delete' and 'Add' buttons are positioned at the bottom of the table.



NOTE: You can view this pane only if the PTP support is enabled in the Timing Client.

The PTP pane on the configuration page allows the setting of parameters which are part of a distributed synchronous network using Precision Time Protocol (PTP).

To configure the Timing Client to provide PTP time synchronization, configure the fields in the PTP pane:

1. The **Domain Number** field specifies the domain number which the TCA6000 or TCA6500 Timing Client has been assigned to. Enter a value within the range 0 through 255 to set the domain number associated with the network broadcast domain the unit will join. This number needs to be same domain number of at least one TCA6000 or TCA6500 Timing Server that is reachable through the network.
2. In the **Delay Req Mode** field, two options are available.



NOTE: The associated TCA6000 or TCA6500 Timing Server needs to be configured to the same profile selected.

Unicast (Default)—A one-to-one connection between a server and a client. This uses unicast messaging in both downstream and upstream direction with respect to the Timing Server.

Multicast—A one-to-many relationship between a server and a client. This uses multicast messaging for the downstream and unicast for the upstream direction with respect to the Timing Server. This is referred to a Juniper Type 1 profile in the Timing Server configuration.

3. From the Log Mean Delay Request Interval list, select a delay request interval rate from the options: **32 packets/sec** and **64 packets/sec**.



NOTE: It is recommended to select **64 packets/sec**.

4. From the Announce Receipt Timeout list, select a timeout period for the announce event messages.
5. In the **DSCP** field, enter the Differential Service (DiffServ) value for the IP packet.
6. Click the **Apply** button to save the PTP parameter changes.

To configure the unicast related parameters:

1. From the Delay Req Mode list, select **unicast**.
2. From the Sync list, select a sync message rate from the options: **1 packet/sec**, **2 packet/sec**, **4 packet/sec**, **8 packet/sec**, **16 packet/sec**, **32 packet/sec**, and **64 packet/sec**.



NOTE: It is recommended to select **64 packet/sec**.

3. From the Delay list, select a delay response message rate from the options: **1 packet/64sec, 1 packet/32sec, 1 packet/16sec, 1 packet/8sec, 1 packet/4sec, 1 packet/2sec, 1 packet/sec, 2 packet/sec, 4 packet/sec, 8 packet/sec, 16 packet/sec, 32 packet/sec, 64 packet/sec, and 128 packet/sec.**



NOTE: It is recommended to select **64 packet/sec.**

4. From the Announce list, select an announce message rate from the options: **1 packet/1 sec, 1 packet/2 sec, 1 packet/4 sec, 1 packet/8 sec, 2 packet/1 sec, 4 packet/1 sec, and 8 packet/1 sec.**
5. In the **Duration** field, enter the Timing Client expiration duration for sending signaling messages without receiving acknowledgements from the Grandmaster.
6. In the **Signaling** field, select an option button to enable or disable the sending of signaling messages to the Grandmaster.
7. Click the **Apply** button to save the unicast configuration.

To add the acceptable Grandmasters for the Timing Client:

1. In the **IP Address** field, enter the IP address of the acceptable Grandmaster for the Timing Client.
2. Click the **Add** button to add the acceptable Grandmaster entry in the **Acceptable Master List** window.

To delete the acceptable Grandmaster entry:

1. Select the Grandmaster entry that you want to delete from the **Acceptable Master List** window.
2. Click the **Delete** button to delete the entry.

Setting NTP Parameters

The TCA6000 and TCA6500 Timing Clients support using the NTP to synchronize time. You can define the NTP association details and the MD5 key list to configure NTP.

- [Enabling the NTP Support on page 34](#)
- [Creating an NTP Association Entry on page 35](#)
- [Modifying an Existing NTP Association Entry on page 37](#)
- [Adding an NTP Association Entry on page 37](#)

- [Deleting an Existing NTP Association Entry on page 38](#)
- [Configuring the MD5 Key List on page 38](#)

Enabling the NTP Support

The **Config** pane on the **Admin** page enables you to configure the protocol (NTP or PTP) to be used for time synchronization. By default, the PTP support is enabled in the Timing Client.

To enable the NTP support in the Timing Client:

1. Log in to the Timing Client as Admin user.
2. Click the **Admin** tab.
3. Locate the **Config** tab across the top tabs of the **Admin** page. See [Figure 10 on page 34](#).

Figure 10: Timing Client Admin Page—Config Pane

The screenshot displays the Juniper TCA6000 Timing Client Admin Page, specifically the Config pane. The page has a top navigation bar with tabs: Password, Alarm, Service, Upgrade, Config (selected), Remote-Log, and Web-Session. A left sidebar contains a menu with Status, Config, Admin (selected), Debug Tool, Log, Help, and Logout. The main content area is titled 'Configuration Operation' and includes several sections:

- Configuration Operation:** Includes 'Reset to manufacture configuration' with a 'Reset' button and 'Backup configuration' with a 'Backup' button.
- Restore configuration:** Includes a 'Browse...' button and a 'Restore' button.
- Restore SSL Key:** Includes a 'Browse...' button and a 'Restore' button.
- Restore SSL Certificate:** Includes a 'Browse...' button and a 'Restore' button.
- Unsecured communication Protocols Configuration:** Includes 'Protocol' (set to ICMP) and 'State' (set to Disable), with an 'Apply' button.
- Protocol Support Config:** Includes 'PTP/NTP Config' with radio buttons for PTP (selected) and NTP, and an 'Apply' button.
- Log Management Configuration:** Includes 'File Size Threshold' (set to 1024 KB), 'TFTP Server' (empty field), 'Email Notification' (checkbox), and 'TFTP Notification' (checkbox), with an 'Apply' button.

A status bar at the top right indicates 'Web Session times out in :54m 54s'.

4. In the **PTP/NTP Config** field, select the **NTP** option button.
5. Click the **Apply** button.

A dialog box stating “System reboot is required to make changes effective. Do you want to reboot?” is displayed.

6. Click **Yes** to reboot the Timing Client with the NTP support.



NOTE:

- If you reject the rebooting of the Timing Client, the protocol change is not saved and the Timing Client continues to use the PTP.
- After rebooting, you cannot use the PTP commands and panes for configuring PTP functionalities. To configure PTP functionalities by using the PTP panes and CLI commands, you must enable the PTP support and reboot the Timing Client.

Creating an NTP Association Entry

To create a new NTP association entry:



NOTE: You can add only a maximum of 20 NTP association entries. Each NTP association entry should have a unique IPv4 address configured.

1. Log in to the Timing Client as Admin or Read/Write user.
2. Click the **Config** tab.
3. Locate the **NTP** tab across the top tabs of the **Config** page. See [Figure 11 on page 36](#).

Figure 11: Timing Client Config Page—NTP Pane

JUNIPER NETWORKS TCA6000 Timing Client

Network Timing T1 **NTP** Trap SNMPv3 Users RADIUS

▶ Status
Config
 ▶ Admin
 ▶ Debug Tool
 ▶ Log
 ▶ Help
 ▶ Logout

Current NTP Association

Role	Prefer	IP Address	Poll Min	Poll Max	Key	Burst	Version

Edit Delete Add

Mode: Unicast Address:
 Prefer: ☐ Burst: NA
 Version: 4 Time to live: 64
 Min Poll Interval: 4 Max Poll Interval: 4
 Key: Key 1 Save

MD5 Security Keys

Current Active Keys

```
# ntpkey_MDSkey_CERN.3362878469
# Wed Jul 26 04:54:29 2006
1 MDS "h33VcP27u3p # MDS key
2 MDS iQhM5F.hXjL[ # MDS key
3 MDS 0'W8aE_jPWaib # MDS key
4 MDS qvGof a4,d-8:Utz # MDS key
5 MDS "N*k)Nu,1(ND # MDS key
6 MDS -u0-Sch0UN5r # MDS key
7 MDS [s-(qVMefmlp)? # MDS key
8 MDS qN@uEj atKq# # MDS key
9 MDS 8sp7? 4D5y_JRIG # MDS key
10 MDS +-Z(Pv3L-Do7N, # MDS key
11 MDS L-ZF5c9MjY-GKR # MDS key
12 MDS 7a"yVFraA8-ov # MDS key
13 MDS @Gikv"ubKpGshS # MDS key
14 MDS W03-a@nZCaf+~ # MDS key
15 MD" P"C num0.atcE # MDS key
16 MDS D_C"v0eA,"yAH # MDS key
```

Save As Clear

Current New Keys

Generate Reload Save As

Upload Key

Browse... Upload



NOTE: You can view this pane only if the NTP support is enabled in the Timing Client.

- From the **Mode** list, select the NTP operation mode for the association entry. The Timing Client supports only the Unicast mode.
- In the **Address** field, enter the IPv4 address for the association entry.
- Select the **Prefer** check box if you want to set this NTP association entry as the preferred server for synchronization among others.

7. From the **Burst** list, select the burst of packets to be sent to the server at each polling interval.
8. From the **Version** list, select the version to be used for the outgoing NTP packets.
9. In the **Time to live** field, enter the number of hops for the NTP packets. This field appears dimmed if you have selected the **Unicast** mode.
10. From the **Min Poll Interval** list, select the minimum polling interval for NTP messages.
11. From the **Max Poll Interval** list, select the maximum polling interval for NTP messages.
12. From the **Key** list, select the key identifier used for encryption.
13. Click the **Save** button to create a new NTP association entry.

Modifying an Existing NTP Association Entry

To modify an existing NTP association entry:

1. Log in to the Timing Client as Admin or Read/Write user.
2. Click the **Config** tab.
3. Locate the **NTP** tab across the top tabs of the **Config** page. See [Figure 11 on page 36](#).
4. In the **Current NTP Association** window, select the association entry to be modified.
5. Click the **Edit** button to modify an existing entry.
6. Modify the applicable parameters for the selected association entry.
7. Click the **Save** button to save the changes.

Adding an NTP Association Entry

To add a new NTP association entry:

1. Log in to the Timing Client as Admin or Read/Write user.
2. Click the **Config** tab.
3. Locate the **NTP** tab across the top tabs of the **Config** page. See [Figure 11 on page 36](#).

4. Click the **Add** button to add a new NTP association entry.
5. Click the **Save** button to save the changes.

Deleting an Existing NTP Association Entry

To delete an existing NTP association entry:

1. Log in to the Timing Client as Admin or Read/Write user.
2. Click the **Config** tab.
3. Locate the **NTP** tab across the top tabs of the **Config** page. See [Figure 11 on page 36](#).
4. In the **Current NTP Association** window, select the association entry to be deleted.
5. Click the **Delete** button to delete the selected association entry.

Configuring the MD5 Key List

To configure the MD5 key list:

1. Log in to the Timing Client as Admin or Read/Write user.
2. Click the **Config** tab.
3. Locate the **NTP** tab across the top tabs of the **Config** page. See [Figure 11 on page 36](#).



NOTE: You can view this pane only if the NTP support is enabled in the Timing Client.

4. Configure the MD key list:
 - Click the **Generate** button to generate MD5 key list by using the system command **ntp-keygen**.
 - or
 - Click the **Browse** button to locate a file containing new MD5 keys and click the **Upload** button to upload the new keys.

Configuring Alarms

How the TCA6000 or TCA6500 Timing Client handles alarms during normal operation can be specified. To configure the alarms:

1. Click the **Admin** tab. The Admin page appears.
2. Click the **Alarm Profile** tab. See [Figure 12 on page 40](#).
3. For each alarm, the following parameters can be configured:
 - a. Select the **Clear Now** check box to clear an alarm immediately. This only applies to non-transient (box gray filled) and not transient alarms.
 - b. Select the **Auto Clear** check box to clear an alarm automatically after it has been active for the **Auto Clear Expiration** period of 1-24 hours. This only applies to non-transient (box gray filled) and not transient alarms.
 - c. In the **Severity** field, select the flag to accompany this alarm. Select:

Critical—Indicates the highest level alarm and is severely affecting traffic. This needs immediate attention. The following alarms are directly related to this level:

TE1_LOS, TE1_LOF, FREQ_FREERUN, LINK_DOWN

Major—Indicates this alarm needs immediate attention. The following alarms are recommended for this level:

PTP_SERVER_UNREACHABLE, LOSS_OF_POWER_FEED, FREQ_HOLD OVER

Minor—Indicates this alarm needs attention but is not urgent. The following alarms are recommended for this level:


SYS_CONFIG_CHANGE, TE1_AIS, TE1_RAI, PTP_SERVER_CHANGE, FREQ_REF_INPUT_CHANGE, FREQ_INPUT_QUALITY_CHANGE, LINK_DOWN, TIMING_OSC_DAC

None—Indicates this alarm is for information only. The following alarms are recommended for this level:

SYS_AUTHENTICATION, OVEN_TEMP_DEVIATION_HIGH, OVEN_TEMP_DEVIATION_LOW, LINK_UP, TIMEPROBE_DISABLE, FREQ_ACQUIRING
 - d. Select the **Send Trap** check box. The Timing Client will send the alarm to the Trap destinations identified on the Config page.

- e. Select the **Write Log** check box. The Timing Client will send the alarm to the local log file.
- f. Select the **Send to Email** check box. The Timing Client will send an e-mail message about this alarm to the users identified in the Alarm E-mail Recipients section of the **Alarm** tab.

Figure 12: Timing Client Admin Page—Alarm Pane



TCA6000 Timing Client

- ▶ Status
- ▶ Config
- Admin
- ▶ Debug Tool
- ▶ Log
- ▶ Help
- ▶ Logout

Password Alarm Service Upgrade Config Remote-Log Web-Session

Web Session times out in :54m 50s ?

Profile

Name	State	Clear Now	Auto Clear	Severity	Send Trap	Write Log	Send Email
FREQ_INPUT_QUALITY_CHANGE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LINK_DOWN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LINK_UP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TIMEPROBE_DISABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FREQ_ACQUIRING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOG_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTP_CM_DISABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTP_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BOA_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ALARM_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOG_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CLI_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTP_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BOA_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ALARM_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOG_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CLI_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply

Auto Clear Expiration

Timer (hour) Apply

Alarm Email Recipients

SMTP:

User1:

User3:

User5:

From:

User2:

User4:

Apply

Configuring Traps

The TCA6000 and TCA6500 Timing Clients can be configured to send event information to trap destinations on a network.


- [Specifying SNMPv3 Contacts on page 41](#)
- [Creating Trap Targets on page 42](#)
- [Editing Trap Targets on page 42](#)
- [Deleting Trap Targets on page 42](#)

Specifying SNMPv3 Contacts

The TCA6000 and TCA6500 Timing Clients can be configured to send alarm information to SNMP community files. To configure the Timing Client to send information to community files:

1. Click the **Config** tab. The Config page appears.
2. Locate the **Trap** tab at the top right of the screen. See [Figure 13 on page 41](#).
3. In the **sysLocation** field, enter the location where the Timing Client is located.
4. In the **sysName** field, enter the name to be used to identify the Timing Client.
5. In the **sysContact** field, enter the X-address of the manager to be used by the Timing Client.
6. In the **ReadOnlyComm** field, enter the string that you want the Timing Client to use to access the local SNMP read community.
7. In the **RWriteComm** field, enter the string to be used by the Timing Client to access the local SNMP read community.
8. Click **Apply** to save changes to memory.

Figure 13: Timing Client Config Page—Trap Pane



JUNIPER
NETWORKS

TCA6000 Timing Client

- ▶ Status
- Config
- ▶ Admin
- ▶ Debug Tool
- ▶ Log
- ▶ Help
- ▶ Logout

Network

Timing

T1

PTP

Trap

SNMPv3

Users

RADIUS

SNMP

sysLocation :

sysContact :

ReadWriteCommunityString:

sysName :

ReadOnlyCommunityString:

Trap

	Destination	Port
<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add"/>		

Address :

Port :

Creating Trap Targets

To create a Trap destination, perform the following from the Trap pane, as shown in [Figure 13 on page 41](#).

1. Click the **Config** tab.
2. Locate the **Trap** tab across the top of the **Config** screen.
3. Click the **Add** button.
4. In the **Address** field, enter the IP address where the Timing Client sends event information.
5. In the **Port** field, enter the port number through which the Timing Client sends event information. The default port number is 161.
6. Click the **Save** button to save changes to memory.

Editing Trap Targets

To edit a Trap destination:

1. Click the **Config** tab.
2. Locate the **Trap** tab across the top tabs of the **Config** screen.
3. Click the Trap address entry to be modified.
4. Click the **Edit** button to make any changes to the entry from the **Trap** window and from memory.
5. Click the **Save** button to save changes to memory.

Deleting Trap Targets

To delete a Trap destination:

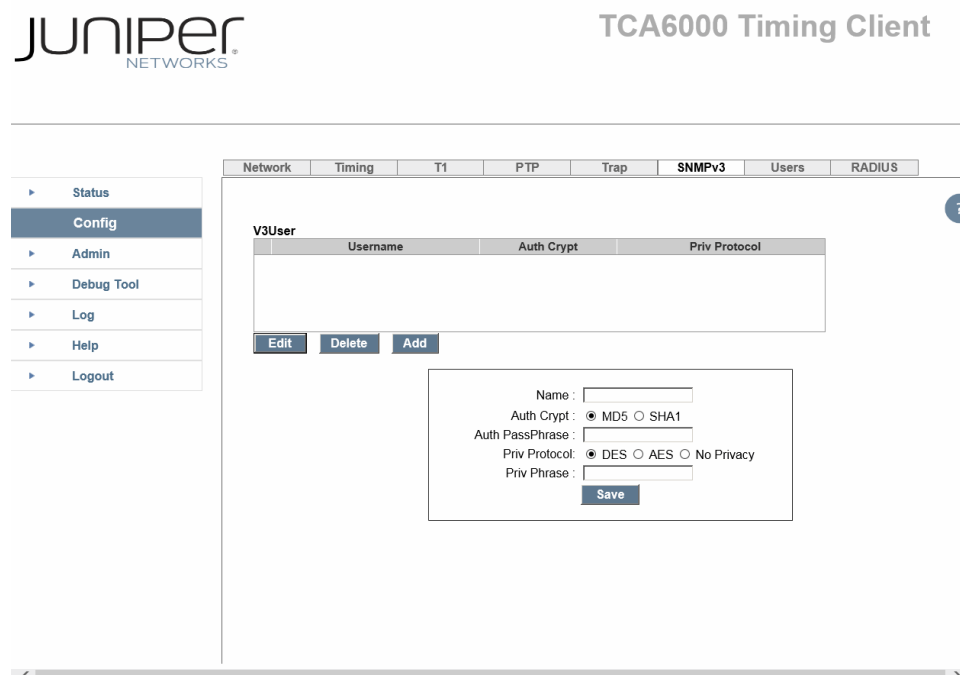
1. Click the **Config** tab.
2. Locate the **Trap** tab across the top tabs of the **Config** screen.
3. Click the Trap address to be deleted.
4. Click the **Delete** button to remove the entry from the **Trap** window and from memory.

Creating SNMPv3 Users

The TCA6000 and TCA6500 Timing Clients support security measures in SNMPv3. To create SNMPv3 users:

1. Click the **Config** tab. The Config page appears.
2. Click the **SNMPv3** tab. See [Figure 14 on page 44](#).
3. Click the **Add** button.
4. In the **Name** field, enter the username that will be used to log in to SNMPv3 log files.
5. In the **Auth Phrase** field, enter the authentication phrase to be used.
6. In the **Auth Crypt** area, select the encryption method to be used.
7. In the **Pri Phrase** field, enter the private phrase to be used.
8. In the **Pri Protocol** field, select the privilege level to be used. Select:
 - DES: The user must use the authentication phrase to log in.
 - AES: The user is not required to use the authentication phrase to log in.
 - No Privacy: The user is required to use the authentication phrase and the private phrase to log in.
9. Click the **Save** button to save the user information in the V3User window and to save changes to memory.

Figure 14: Timing Client Config Page—SNMPv3 User Pane



Editing SNMPv3 Users

To edit SNMPv3 users:

1. Click the **Config** tab. The Config page appears.
2. Click the **SNMPv3** tab. See [Figure 14 on page 44](#).
3. Click the V3User entry to be modified.
4. Click the **Edit** button to modify the user information of any entry from the window.
5. Click the **Save** button to save the changes to memory.

Deleting SNMPv3 Users

To delete SNMPv3 users:

1. Click the **Config** tab. The Config page appears.
2. Click the **SNMPv3** tab. See [Figure 14 on page 44](#).

3. Click the V3User entry to be deleted.
4. Click the **Delete** button to remove the entry.

Managing TCA User Accounts

The TCA6000 and TCA6500 Timing Clients support multiple user accounts to be created and managed by the Admin user. Juniper Networks assigns a default user account (admin/admin) with login class as Admin to a TCA6000 or TCA6500 Timing Client for logging in to the Timing Client. This Admin user account allows the administrator to create and manage multiple user accounts with login class as Read-Only and Read/Write.

The TCA user accounts can be managed by:

- [Creating an User Account on page 45](#)
- [Modifying an Existing User Account on page 46](#)
- [Deleting an Existing User Account on page 47](#)

Creating an User Account

To create a new user account:



NOTE: You can create only a maximum of five user accounts.

1. Log in to the Timing Client as Admin user.
2. Click the **Config** tab.
3. Locate the **Users** tab across the top tabs of the **Config** page. See [Figure 15 on page 46](#).

Figure 15: Timing Client Config Page—Users Pane

The screenshot shows the Juniper TCA6000 Timing Client configuration interface. The 'Users' pane is active, displaying a table with columns for Username, Email-Id, and Class. Below the table are buttons for Edit, Delete, and Add. A form for adding a new user is visible, with fields for Username, Password, Email-Id, and Class (Read-Only or Read/Write), and a Save button.

4. Click the **Add** button.
5. In the **Username** field, enter the username for the new user account.
6. In the **Password** field, enter the password for the new user account.
7. In the **Email-Id** field, enter the e-mail address for the new user account.
8. In the **Class** field, select an option button to set the login class for the new user account as Read-Only or Read/Write.
9. Click the **Save** button to create a new user account.

Modifying an Existing User Account

To modify an existing user account:



NOTE: You cannot modify the username.

1. Log in to the Timing Client as Admin user.
2. Click the **Config** tab.

3. Locate the **Users** tab across the top tabs of the **Config** page. See [Figure 15 on page 46](#).
4. In the **Users** window, select the user account to be modified.
5. Click the **Edit** button to populate the details of the selected user account in the **Username**, **Password**, **Email-Id**, and **Class** fields.
6. Modify the password or class for the selected user account.

**NOTE:**

- If you change the password, all the active sessions for the corresponding user are not logged out. The user must use the new password for new sessions.
- If you change the class, all active sessions for the corresponding user are logged out.

7. Click the **Save** button to save the changes done.

Deleting an Existing User Account

To delete an existing user account:

1. Log in to the Timing Client as Admin user.
2. Click the **Config** tab.
3. Locate the **Users** tab across the top tabs of the **Config** page. See [Figure 15 on page 46](#).
4. In the **Users** window, select the user account to be deleted.
5. Click the **Delete** button to delete the selected user account.



NOTE: All active sessions for the deleted user are logged out.

Changing the Login Password for Read/Write User

The TCA6000 and TCA6500 timing clients allow Read/Write users to change their password configured and shared by the TCA Admin user.

To change your (Read/Write user) password:

1. Log in to the Timing Client as Read/Write user.
2. Click the **Config** tab.
3. Locate the **Profile** tab across the top tabs of the **Config** page. See [Figure 16 on page 48](#).

Figure 16: Timing Client Config Page—Profile Pane

The screenshot shows the Juniper Networks TCA6000 Timing Client web interface. On the left is a sidebar with navigation links: Status, Config (highlighted), Debug Tool, Log, Help, and Logout. The main area has a top navigation bar with tabs: Network, Timing, E1, NTP, Trap, SNMPv3, Profile (selected), and RADIUS. Below the tabs, the 'Change Password' section contains three input fields: 'Old Password', 'New Password', and 'Retype New Password'. A 'Save' button is located below the 'Retype New Password' field. A circular help icon (?) is in the top right corner of the form area.

4. In the **Old Password** field, enter your current password.
5. In the **New Password** field, enter the new password to replace the old password.
6. In the **Retype New Password** field, reenter the new password.
7. Click **Save** button to change your password and save the changes.



NOTE: The new password will be effective from next login onwards. The current session is not affected.

Configuring User Authentication through RADIUS

The TCA6000 and TCA6500 Timing Clients support RADIUS server authentication, local authentication, or both based on the configured authentication order to authenticate the user logging in to the Timing Client.

When you configure the authentication order as RADIUS server authentication followed by the local authentication, the Timing Client passes the information about the logging user to the configured RADIUS servers for authentication. If any one of the RADIUS server successfully authenticates the user, then the Timing Client allows the user to log in. If all the configured RADIUS servers fail to authenticate the user or configured RADIUS servers are not available, then the Timing Client performs the local authentication and allows the user to log in after successful local authentication. The Timing Client blocks the logging user if both RADIUS and local authentication fails.

When you configure the authentication order as local authentication followed by the RADIUS server authentication, the Timing Client performs the local authentication to grant access to the logging user. If the local authentication fails to authenticate the user, then the Timing Client passes the information about the logging user to the configured RADIUS servers for authentication. If any one of the RADIUS server successfully authenticates the user, then the Timing Client allows the user to log in. If all configured RADIUS servers fail to authenticate the user, then the Timing Client denies access to the logging user.

When you configure the authentication order as RADIUS server authentication only, the Timing Client passes the information about the logging user to the configured RADIUS servers for authentication. If any one of the RADIUS server successfully authenticates the user, then the Timing Client allows the user to log in. If all configured RADIUS servers fail to authenticate the user, then the Timing Client denies access to the logging user. If all configured RADIUS servers are not available, then the Timing Client performs local authentication and allows the user to log in after successful local authentication.

When you configure the authentication order as local authentication only, the Timing Client performs the local authentication to grant or deny access to the user logging in to the Timing Client.



NOTE:

- The selection of RADIUS authentication server to authenticate user is based on the order in the RADIUS authentication server list.
- The user authentication process is implemented only for the Access Request, Access Reject, and Access Accept messages.
- The user authentication process is not supported for shell users.

The user authentication process protects the Timing Client from being accessed by unauthorized persons. The usage of RADIUS authentication servers provides the following advantages:

- Management of multiple user credentials on remote machine for detailed logging.
- Centralized user information and authentication process at one server.
- No loss of user information due to Timing Client damage.

To configure user authentication process:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 17 on page 50](#).

Figure 17: Timing Client Config Page—RADIUS Pane (Authentication)

JUNIPER NETWORKS TCA6000 Timing Client

Network Timing E1 PTP Trap SNMPv3 Users **RADIUS**

▶ Status
Config
 ▶ Admin
 ▶ Debug Tool
 ▶ Log
 ▶ Help
 ▶ Logout

RADIUS Authentication Servers

Server IP	Port	Retries	Timeout	Secret Word

Edit Delete Add

Authentication Order

☒ radius
☐ local

Apply

RADIUS Accounting Servers

Server IP	Port	Retries	Timeout	Secret Word

Edit Delete Add

RADIUS Accounting Level

☐ 1: For login accounting only
☐ 2: For interactive and login accounting
☒ 3: For configuration, interactive and login accounting

RADIUS Accounting Status

☒ Enable ☐ Disable

Apply

3. Configure the RADIUS authentication server details.
4. Click the **Save** button to save the authentication server configuration.

5. Select the authentication order.
6. Click the **Apply** button to apply the configured authentication order.

The following sections describe RADIUS authentication server configuration and authentication order configuration:

- [Adding a New RADIUS Authentication Server Entry on page 51](#)
- [Deleting a RADIUS Authentication Server Entry on page 52](#)
- [Modifying a RADIUS Authentication Server Entry Details on page 52](#)
- [Configuring Authentication Order on page 52](#)

Adding a New RADIUS Authentication Server Entry

To add a new RADIUS authentication server entry to the authentication server list:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 17 on page 50](#).
3. In the **Server IP** field, enter the IP address of the RADIUS authentication server to be used for user authentication.
4. In the **Port** field, enter the port through which the specified RADIUS authentication server is contacted for user authentication.
5. In the **Retry** field, enter the number of attempts should be made for contacting the specified RADIUS authentication server.
6. In the **Timeout** field, enter the time in seconds till which the Timing Client waits for a response from the specified RADIUS authentication server.
7. In the **Secret Word** field, enter the password shared with the specified RADIUS authentication server.
8. Click the **Save** button to add the RADIUS authentication server entry in the **RADIUS Authentication Servers** window and memory.

Deleting a RADIUS Authentication Server Entry

To delete a RADIUS authentication server entry from the authentication server list:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 17 on page 50](#).
3. In the **RADIUS Authentication Servers** window, click the RADIUS authentication server entry to be deleted.
4. Click the **Delete** button to remove the entry from the RADIUS Authentication Server window and memory.

Modifying a RADIUS Authentication Server Entry Details

To modify the details of a RADIUS authentication server entry existing in the authentication server list:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 17 on page 50](#).
3. In the **RADIUS Authentication Servers** window, select the RADIUS authentication server entry to be modified.
4. Click the **Edit** button to populate the values of the selected RADIUS authentication server entry in the **Server IP**, **Port**, **Retry**, **Timeout**, and **Secret Word** fields.
5. Modify the populated values.
6. Click the **Save** button to save the changes done in the selected RADIUS authentication server entry.

Configuring Authentication Order

To configure the authentication order:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 17 on page 50](#).
3. In the first drop box, select the type of authentication to be performed initially. Select:

- radius: To authenticate the user using the configured RADIUS authentication servers.
 - local: To authenticate the user using local settings.
4. In the second drop box, select the type of authentication to be performed on failure or unavailability of initial authentication. Select:
- radius: To authenticate the user using the configured RADIUS authentication servers.
 - local: To authenticate the user using local settings.
5. Click the **Apply** button to save the authentication order.

Configuring RADIUS Accounting

The TCA6000 and TCA6500 Timing Clients support RADIUS accounting for the user logged in to the Timing Client. Once the user is logged in to the Timing Client, the Timing Client passes the accounting information to the configured RADIUS accounting servers. The Timing Client stops the accounting process when the user session is closed either voluntarily or involuntarily. The Timing Client waits for acknowledgment from the accounting servers for each accounting packet.

When the RADIUS accounting is enabled, the Timing Client tries to log the accounting information in any one of the configured RADIUS accounting server based on the configured timeout period and number of retries. When the logging of accounting information fails for all configured accounting server, the Timing Client raises an `ACCOUNTING_SERVER_UNAVAILABLE` alarm.

When the RADIUS accounting server is unavailable, the accounting information (latest 15 commands) is buffered. The Timing Client sends the buffered information to the RADIUS accounting server after the server becomes available.

The accounting process supports login accounting, interactive commands accounting, and configuration commands accounting.



NOTE:

- The selection of RADIUS accounting server to log the accounting information is based on the order in the RADIUS accounting server list.
- The accounting process is implemented only for the Accounting Request and Accounting Response messages.
- The RADIUS accounting is not supported for shell users.
- The accounting process does not support immediate accounting and accounting of web configurations.

The usage of RADIUS accounting servers provides the following advantages:

- Centralized usage history of all users on one server.
- No loss of usage history of users due to Timing Client damage.

To configure RADIUS accounting:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 18 on page 54](#).

Figure 18: Timing Client Config Page—RADIUS Pane (Accounting)

JUNIPER
NETWORKS

TCA6000 Timing Client

Network Timing E1 PTP Trap SNMPv3 Users **RADIUS**

▶ Status
Config
 ▶ Admin
 ▶ Debug Tool
 ▶ Log
 ▶ Help
 ▶ Logout

RADIUS Authentication Servers

Server IP	Port	Retries	Timeout	Secret Word

Edit Delete Add

Authentication Order

☒ radius
☐ local

Apply

RADIUS Accounting Servers

Server IP	Port	Retries	Timeout	Secret Word

Edit Delete Add

RADIUS Accounting Level

☐ 1: For login accounting only
☐ 2: For interactive and login accounting
☒ 3: For configuration, interactive and login accounting

RADIUS Accounting Status

☒ Enable ☐ Disable

Apply

3. In the **RADIUS Accounting Status** field, select the **Enable** option to enable RADIUS accounting.
4. Click the **Apply** button to apply RADIUS accounting status configuration.
5. Configure the RADIUS accounting server details.
6. Click the **Save** button to save the accounting server configuration.

7. In the **RADIUS Accounting Level** field, select the type of accounting information to be logged in the RADIUS accounting server.
8. Click the **Apply** button to apply the configured RADIUS accounting level.

The following section describe RADIUS accounting server configuration:

- [Adding a New RADIUS Accounting Server Entry on page 55](#)
- [Deleting a RADIUS Accounting Server Entry on page 55](#)
- [Modifying a RADIUS Accounting Server Entry Details on page 56](#)

Adding a New RADIUS Accounting Server Entry

To add a new RADIUS accounting server entry to the accounting server list:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 18 on page 54](#).
3. In the **Server IP** field, enter the IP address of the RADIUS accounting server to be used for accounting.
4. In the **Port** field, enter the port through which the specified RADIUS accounting server is contacted for accounting.
5. In the **Retry** field, enter the number of attempts should be made for contacting the specified RADIUS accounting server.
6. In the **Timeout** field, enter the time in seconds till which the Timing Client waits for a response from the specified RADIUS accounting server.
7. In the **Secret Word** field, enter the password shared with the specified RADIUS accounting server.
8. Click the **Save** button to add the RADIUS accounting server entry in the RADIUS Accounting Servers window and memory.

Deleting a RADIUS Accounting Server Entry

To delete a RADIUS accounting server entry from the accounting server list:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 18 on page 54](#).

3. In the **RADIUS Accounting Servers** window, click the RADIUS accounting server entry to be deleted.
4. Click the **Delete** button to remove the entry from the RADIUS Accounting Servers window and memory.

Modifying a RADIUS Accounting Server Entry Details

To modify the details of a RADIUS accounting server entry existing in the accounting server list:

1. Click the **Config** tab.
2. Locate the **RADIUS** tab across the top tabs of the **Config** page. See [Figure 18 on page 54](#).
3. In the **RADIUS Accounting Servers** window, select the RADIUS accounting server entry to be modified.
4. Click the **Edit** button to populate the values of the selected RADIUS accounting server entry in the **Server IP**, **Port**, **Retry**, **Timeout**, and **Secret Word** fields.
5. Modify the populated values.
6. Click the **Save** button to save the changes done in the selected RADIUS accounting server entry.

Specifying Alarm Recipient E-Mail Address Destinations

- [Adding a User to the E-Mail List on page 56](#)
- [Removing Users from the Alarm Event Recipient List on page 57](#)


Adding a User to the E-Mail List

The TCA6000 and TCA6500 Timing Clients can be configured to send e-mail alarm event messages directly to selected users. To add a user to the list of e-mail recipients:

1. Click the **Admin** tab.
2. Locate the **Alarm** tab across the top tabs of the Admin page. See [Figure 19 on page 57](#).
3. In the Alarm Email Recipients section:
 - a. In the **SMTP** field, enter the IP Address of the e-mail server the Timing Client will register to send e-mail messages.

- b. In the **User x** field, enter the IP address or domain name of the user the Timing Client will send alarm event information to.
 - c. In the **From** field, enter the IP address or domain name of the from address the Timing Client will register to send e-mail messages.
4. Click the **Apply** button to save your changes to memory.

Figure 19: Timing Client Admin Page—Alarm Pane



TCA6000 Timing Client

- ▶ Status
- ▶ Config
- Admin**
- ▶ Debug Tool
- ▶ Log
- ▶ Log
- ▶ Help
- ▶ Logout

Password Alarm Service Upgrade Config Remote-Log Web-Session

Web Session times out in :54m 50s ?

Profile	Name	State	Clear Now	Auto Clear	Severity	Send Trap	Write Log	Send Email
	FREQ_INPUT_QUALITY_CHANGE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	LINK_DOWN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	LINK_UP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	TIMEPROBE_DISABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	FREQ_ACQUIRING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	LOG_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	PTP_CM_DISABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	PTP_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	BOA_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	SNMP_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	ALARM_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	LOG_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CLI_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	PTP_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	BOA_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	SNMP_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	ALARM_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	LOG_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CLI_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply

Auto Clear Expiration
 Timer (hour)
Apply

Alarm Email Recipients

SMTP:
 User1:
 User3:
 User5:

From:
 User2:
 User4:

Apply

Removing Users from the Alarm Event Recipient List

To remove a user from the list of recipients who receive alarm events:

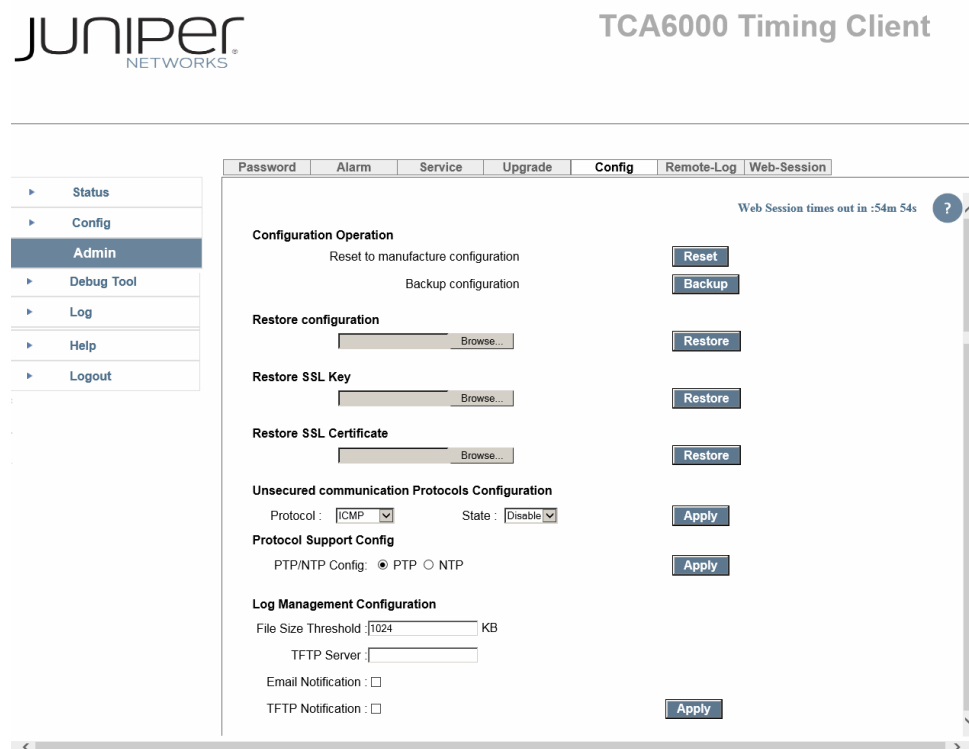
1. Click the **Admin > Alarm** tabs.
2. In the **Alarm Email Recipient** section, locate the **User** field that contain the address of the recipient(s) to be removed.
3. Highlight all addresses, and press the **Delete** key.
4. Click the **Apply** button to save changes to memory.

Resetting Factory Defaults

The TCA6000 and TCA6500 parameters can be reset to the manufacturer's default parameters at any time. To reset the unit to the manufacturer's default parameters:

1. Click the **Admin > Config** tabs. See [Figure 20 on page 58](#).
2. Locate the Configuration Operation section on the left-hand side of the page.
3. Click the **Reset** button next to the text "Reset to manufacture configuration" to reset the parameters to their default configuration.

Figure 20: Timing Client Admin Page—Config Pane



Stopping and Restarting the TCA6000 or TCA6500 Timing Client

The TCA6000 and TCA6500 Timing Clients can be rebooted, or a clean power down can be performed by halting all the processes running on the Timing Client. To reboot or halt the Timing Client:

1. Click the **Admin** tab.
2. Select the **Upgrade** tab at the top of the screen.

3. Click the **Reboot** or **Halt** button.
4. Click **Apply** to reboot or halt the Timing Client.

The Timing Clients provide carrier-class upgrade capability. Two flash partitions are allocated to store software images. All upgrade or downgrade images are placed in volatile RAM first, and written to the inactive flash partition. Depending on the image chosen to run on the Timing Client, the active or non-active images can be selected by selecting the image using the drop-down arrow. Once the unit has been rebooted, the new selected image will be running.

Figure 21: Timing Client Admin Page—Upgrade Pane Showing the Current Image

JUNIPER
NETWORKS

TCA6000 Timing Client

► Status
► Config
Admin
► Debug Tool
► Log
► Help
► Logout

Password Alarm Service **Upgrade** Config Remote-Log Web-Session

Web Session times out in : 23m 32s ?

Upgrade:
☐ TFTP ☐ FTP ☒ SCP
 Server:
 File Name:
 Username:
 Password:

Halt and Reboot System
☐ Halt ☒ Reboot
 Software Image: TCA6K-3.9.0_RC10-PTPNT-T1(Active) ▼

Figure 22: Timing Client Admin Page—Upgrade Pane Showing the New Image

JUNIPER
NETWORKS

TCA6000 Timing Client

► Status
► Config
Admin
► Debug Tool
► Log
► Help
► Logout

Password Alarm Service **Upgrade** Config Remote Log

Upgrade:
☐ TFTP ☐ FTP ☐ SCP
Server:
File Name:
Username:
Password:

Halt and Reboot System
☐ Halt ☒ Reboot
Software Image:

CHAPTER 4

Upgrading the TCA6000 and TCA6500 Software

This chapter describes the processes for upgrading software on Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are discussed:

- [Upgrade Requirements on page 61](#)
- [Selecting Between the Pre-Installed Software Images Using a GUI/Browser on page 62](#)
- [Upgrading the Software Using a GUI/Browser on page 63](#)
- [Selecting Between the Pre-Installed Software Images Using the CLI on page 65](#)
- [Upgrading the Software Using the CLI on page 66](#)
- [Performing Basic Configurations Using Setup Wizard through GUI on page 68](#)

Upgrade Requirements

The TCA6000 and TCA6500 Timing Clients are shipped with software pre-installed and ready to be configured when the Timing Client is powered on. To upgrade the software you must connect to the Timing Client using the GUI or a Telnet connection.

Upgrades affect service and cause the Timing Client to reboot. The Timing Client must reboot to load the new software version. All timing outputs are interrupted during this period (approximately 1-3 minutes). After the new version is loaded, frequency and time lock can take up to 50 minutes to resume normal status (LOCKED) for PTP or NTP features.

Gather the following information before upgrading the Timing Client:

- Admin password
- Name of the TFTP, FTP, or SCP server
- IP address of the TFTP, FTP, or SCP server
- Username and password of the FTP or SCP server
- Filename of the software upgrade or downgrade image

Selecting Between the Pre-Installed Software Images Using a GUI/Browser

The TCA6000 and TCA6500 Timing Clients ship with both T1 and E1 software images installed in the two internal non-volatile memory partitions. By default, the TCA6000 and TCA6500 Timing Clients use the E1 interface type. You can view the software images from the Timing Client Admin web interface page (see [Figure 22 on page 60](#)). The active software image is displayed as **(Active)** in the Halt and Reboot System drop-down menu.

To select an alternate software image using the Web-based GUI:

1. Verify that the Timing Client is powered on.
2. Enter the IP address of the Timing Client into a web browser.
For example, **https://10.1.0.42**.
3. Log in to the Timing Client as **admin**.
Login: admin
Password: admin
4. Select the **Admin** tab from the menu on the left.
5. Select the required interface from the drop-down menu.
6. Select the **Reboot** option.
7. Click **Apply** to reboot the Timing Client.
8. Select **Yes** when prompted with the dialog box stating “Do you confirm a system reboot system?” The Timing Client reboots and loads the selected software image.



.....

NOTE: If the appropriate software image interface is not shown in either software image partitions, upgrade the in-active partition with the appropriate software image, and then perform the reboot as described in [“Upgrading the Software Using a GUI/Browser” on page 63](#).

.....

Upgrading the Software Using a GUI/Browser

To upgrade the TCA6000 and TCA6500 Timing Client using the Web-based GUI:

1. Verify that the Timing Client is powered on.



NOTE: Ensure that you have cleared the browser cache history.

2. Enter the IP address of the Timing Client into a web browser.

For example, **https://10.1.0.42**.

3. Log in to the Timing Client as **admin**.

Login: admin

Password: admin

4. Select the **Admin** tab from the menu on the left.

5. Select the network protocol to be used for transferring the software upgrade or downgrade image.

- Select **TFTP** to download the software image from the server supporting TFTP.
- Select **FTP** to download the software image from the server supporting FTP.
- Select **SCP** to download the software image from the server supporting SCP.

6. In the **server** field, enter the IP address of the server that contains the software upgrade or downgrade image.

For example, **10.1.0.52**.

7. In the **file name** field:

- Enter the name of the software image file supplied by Juniper Customer Support if the image is to be downloaded from the TFTP or FTP server.

For example, **TCA6K-3.4.0-1-PTP-E1**.

- Enter the name of the Juniper supplied software image file with the file path if the image is to be downloaded from the SCP server.

For example, **/build/tca/images/TCA6K-3.4.0-1-PTP-E1**.



NOTE: Two flash partitions are allocated to store software images. These can be used to store the same images or two different images should you wish to revert to a previous version.

All upgrade or downgrade images are written in volatile RAM first, and are loaded to the inactive flash partition. You can select active or non-active images to run on the Timing Client by selecting the image using the drop-down arrow. After the unit has been rebooted, the new—selected—image will be running on the appliance.

8. In the **user name** field, enter a valid server username.



NOTE: The **user name** field is applicable only if the image is to be downloaded from the SCP or FTP server.

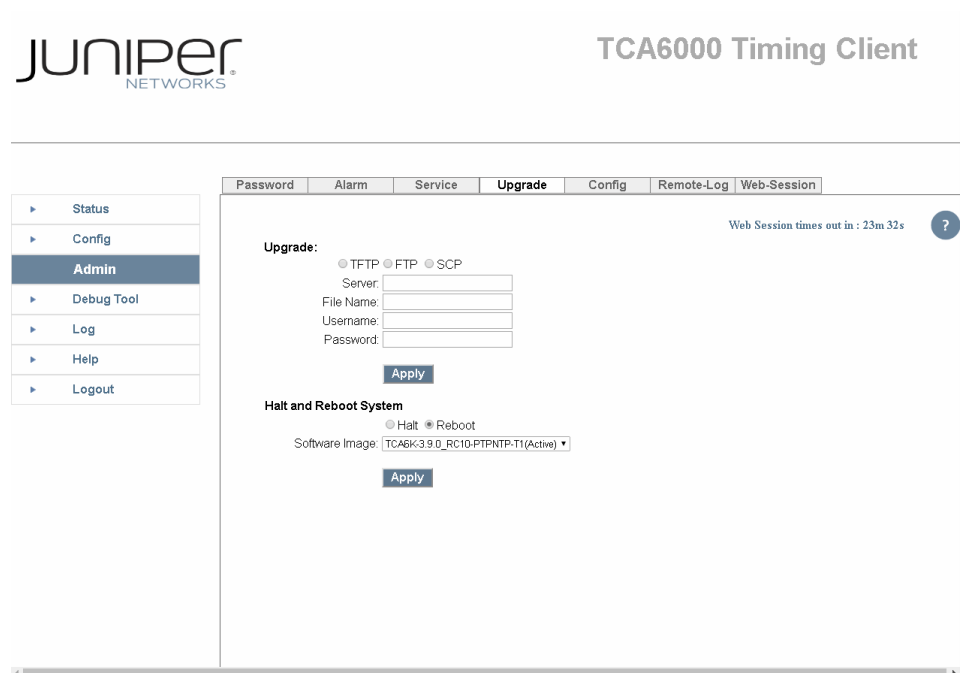
9. In the **password** field, enter the password of the server username.



NOTE: The **password** field is applicable only if the image is to be downloaded from the SCP or FTP server.

10. Select the **Apply** button. The browser status (bottom of webpage) shows the download progress. After the image file is completely downloaded (typically 5-7 minutes), a dialog box appears with the message, “Upgrade successful. The new software image will take effect after the system reboots!”
11. Select **OK** to acknowledge the upgrade message.
12. Select the **Reboot** option.
13. Click **Apply** to reboot the Timing Client.
14. Select **Yes** when prompted with the dialog box stating “Do you confirm a system reboot system?” The Timing Client reboots and loads the new software image.

Figure 23: Timing Client Admin Page—Upgrade Pane



Rebooting the Timing Client will invoke an upgrade if it completes successfully. If the upgrade fails in a detectable manner, the upgrade or downgrade image is discarded, and the Timing Client boots from the previous image. If the upgrade failed in a manner detectable only during the booting sequence, the hardware recovery cycle interrupts the process and the system reverts back to the previous image; the upgrade or downgrade image is discarded.

Selecting Between the Pre-Installed Software Images Using the CLI

The TCA6000 and TCA6500 Timing Clients ship with both T1 and E1 software images installed in the two internal non-volatile memory partitions. By default, the TCA6000 and TCA6500 Timing Clients use the E1 interface type. Use the **show partition** command to display the active and backup software images. The CLI displays the current software image as **Active**.

To select an alternate software image using the CLI:

1. Verify that the TCA6000 and TCA6500 Timing Client is powered on.
2. Connect to the Timing Client over a telnet application.

```
>telnet 10.1.0.42
```

3. Enter the login and password.

```
>login: admin
Password: admin
```

4. Issue the **en** command, and then enter **enable** as the password.

```
>en
Password: enable
```

5. Issue the **show partition** command to verify that the software image appears in Partition 1.

```
# show partition
Partition 1: cern-2.1.2-2-PTP-E1 (Active)
Partition 2: cern-2.1.2-2-PTP-T1
```

6. To initiate the reboot, issue the **reboot *partition-number*** command where *partition-number* is the number of the partition you want to load. Type **Y** to confirm.

```
# reboot 2
Are you sure you want> to reboot? y/n
>Y
The appliance will reboot resulting in a "no service" condition.
```



NOTE: If the appropriate software image interface is not shown in either software image partitions, upgrade the in-active partition with the appropriate software image, and then perform the reboot as described in [“Upgrading the Software Using the CLI” on page 66](#)

Upgrading the Software Using the CLI

To upgrade the software using the CLI:

1. Verify that the TCA6000 and TCA6500 Timing Client is powered on.
2. Connect to the Timing Client over a telnet application.

```
>telnet 10.1.0.42
```

3. Enter the login and password.

```
>login: admin
Password: admin
```

4. Issue the **en** command, and then enter **enable** as the password.

```
>en
Password: enable
```

5. Issue the corresponding CLI command to load the software into the partition, then confirm the upgrade.

- Issue the **tftp *tftp-ip-address filename*** command if you want to download the software image from the TFTP server.

```
# tftp 10.0.122.10 TCA6K-3.4.0-1-PTP-E1
Are you sure you want to upgrade? y/n

>Y
Please wait during file transfer...
upgrade successful!
The new software will take effective after the reboot
```

- Issue the **ftp ftpserverip filename username password** command if you want to download the software image from the FTP server.

```
# ftp 10.0.122.10 TCA6K-3.4.0-1-PTP-E1 user_1 user123
Are you sure you want to upgrade? y/n

>Y
Please wait during file transfer...
upgrade successful!
The new software will take effective after the reboot
```

- Issue the **scp username scpserverip filename** command if you want to download the software image from the SCP server.

```
# scp user_1 10.209.164.21 /build/tca/images/TCA6K-3.4.0-1-PTP-E1
Password: *****
Are you sure you want to upgrade? y/n

>Y
Please wait during file transfer...
upgrade successful!
The new software will take effective after the reboot
```

6. Issue the **show partition** command to verify that the software image appears in Partition 1.

```
# show partition
Partition 1: TCA6K-3.4.0-1-PTP-E1
Partition 2: TCA6k-3.3.0-3-PTP-T1(Active)
```

7. Issue the **reboot 1** command to initiate the reboot, and then type **Y** to confirm.

```
# reboot 1
Are you sure you want> to reboot? y/n

>Y
The appliance will reboot resulting in a "no service" condition.
```

Rebooting the Timing Client will invoke an upgrade if it completes successfully. If the upgrade fails in a detectable manner, the upgrade or downgrade image is discarded, and the Timing Client boots from the previous image. If the upgrade failed in a manner detectable only during the booting sequence, the hardware recovery cycle interrupts the process and the system reverts back to the previous image; the upgrade or downgrade image is discarded.

Performing Basic Configurations Using Setup Wizard through GUI

The setup wizard enables you to configure basic settings that are required for TCA6000 and TCA6500 Timing Clients to operate. The Setup Wizard pages appear when you log in to the Timing Client through GUI for the first time after the upgrade or reset.

To perform basic configurations using the setup wizard through GUI:

1. Log in to the Timing Client as **admin**. The **Setup Wizard Page 1** (Figure 24 on page 68) appears.

Figure 24: Setup Wizard Page 1

The screenshot shows the 'Welcome To Setup Wizard' page for the TCA6000 Timing Client. The Juniper Networks logo is in the top left. The page is divided into two main sections. On the left, a sidebar indicates 'Setup Wizard : General Configuration Page 1 of 5'. The main content area has a 'Host Information' section with input fields for 'Hostname' (containing 'TCA6K') and 'Domain Name' (containing 'localhost'). Below this is a 'RADIUS Authentication Servers' section with a table header: 'Server IP', 'Port', 'Retries', 'Timeout', and 'Secret Word'. There are 'Add', 'Edit', and 'Delete' buttons below the table. The 'Users' section has a table header: 'Username', 'Email-id', and 'Class', with 'Add' and 'Edit' buttons below it. A 'Next' button is located at the bottom right of the main content area.

2. In the **Hostname** field, enter the hostname to be assigned to the Timing Client.
3. In the **Domain** field, enter the domain name of the LAN.
4. Click **Add** under **RADIUS Authentication Servers** section to add a new RADIUS authentication server entry. You can edit or delete an existing entry by using **Edit** and **Delete** buttons.
5. In the **Server IP** field, enter the IP address of the RADIUS authentication server to be used for user authentication.
6. In the **Port** field, enter the port through which the specified RADIUS authentication server is contacted for user authentication.

7. In the **Retry** field, enter the number of attempts that should be made for contacting the specified RADIUS authentication server.
8. In the **Timeout** field, enter the time in seconds till which the Timing Client waits for a response from the specified RADIUS authentication server.
9. In the **Secret Word** field, enter the password shared with the specified RADIUS authentication server.
10. Click **Add** under the **Users** section to add a new user account. You can edit an existing entry by using the **Edit** button.
11. In the **Username** field under the **User Configuration** section, enter the username for the new user account.
12. In the **Password** field, enter the password for the new user account.
13. In the **Email-Id** field, enter the e-mail address for the new user account.



NOTE: In case of software upgrade to 3.9.0 from 3.7.0 or earlier releases, you need to configure e-mail IDs for all the existing non-admin users.

14. In the **Class** field, select an option button to set the login class for the new user account as Read-Only or Read/Write.
15. Click **Next**. The **Setup Wizard Page 2** ([Figure 25 on page 70](#)) appears.

Figure 25: Setup Wizard Page 2

JUNIPER
NETWORKS

TCA6000 Timing Client

Welcome To Setup Wizard

Setup Wizard :
Timing Configuration
Page 2 of 5

PPS Squelch
PPS Squelch : ☐ Yes ☒ No

Time Zone
Time Zone : GMT 0:00

Antenna Cable Delay Compensation
Value : 1 ns

Offset Compensation
Value : 10.000000 ns

Sync Source Priority
Priority 1 : ptp
Priority 2 : internal

Previous Next

16. In the **PPS Squelch** field, select an option button to turn on or off the PPS squelch.

17. In the **Time Zone** field, select the local time zone.

18. In the **Antenna Cable Delay Compensation** field, enter a delay compensation value to compensate for varying cable lengths. This value ranges from -100000 through 100000 nanoseconds.



NOTE: You are advised to enter:

- A negative delay compensation value to compensate the positive delay introduced by the cable.
- A positive delay compensation value to advance the PPS output delay relative to the absolute value.

19. In the **Offset Compensation** field, enter the time period (in nanoseconds) to be adjusted for DST. The default value is 0 nanoseconds (that is, the DST is turned off).

20. In the **Sync Source Priority** field, configure the priority of various synchronization reference sources. Available options are N/A, PTP, or Internal. The sync source list is arranged in orders of priority, with 1 being the highest order.

21. Click **Next**. The **Setup Wizard Page 3** (Figure 26 on page 71) appears.

Figure 26: Setup Wizard Page 3

The screenshot shows the Juniper TCA6000 Timing Client Setup Wizard Page 3. The page is titled "Welcome To Setup Wizard" and features the Juniper Networks logo. On the left, a sidebar indicates the current step: "Setup Wizard : Web & Protocol Configuration Page 3 of 5". The main content area is divided into three sections:

- WEB**: Contains radio buttons for "Standard HTTP only" (selected), "Standard and Secured HTTP", and "Secured HTTP only". Below these is a "Session Timeout" field set to "55" minutes.
- Unsecured communication Protocols Configuration**: Contains a "Protocol" section with checkboxes for "ICMP", "TFTP", "FTP", and "TELNET", all of which are checked.
- Protocol Support Config**: Contains a "PTP/NTP Config" section with radio buttons for "PTP" (selected) and "NTP".

At the bottom of the main content area, there are "Previous" and "Next" buttons.

22. In the **WEB** section, select either standard or secure HTTP, or both to configure the web mode.

23. In the **Session Timeout** field, enter the Web timeout period in minutes.

24. Select the unsecured transfer or communication protocol to be enabled from the **Protocol** list. The available options are: ICMP, TFTP, FTP, and TELNET.

25. In the **PTP/NTP Config** field, select an option button to enable the PTP or NTP protocol support in the Timing Client.

26. Click **Next**. The Setup Wizard Page 4 (Figure 27 on page 72) appears.

Figure 27: Setup Wizard Page 4

JUNIPER
NETWORKS

TCA6000 Timing Client

Welcome To Setup Wizard

Log Management

Max File Size threshold : 1024 KB

Email notification : ☐

TFTP notification : ☐

Resource Monitoring

Number of days to monitor processes : 10

Email Notification : ☐

Server Configuration

SMTP (Mail) Server :

TFTP Server :

Previous Next

Setup Wizard :
Services Parameter Configuration
Page 4 of 5

27. In the **Max File Size Threshold** field, enter a threshold value for the log files stored in system. The threshold value ranges from 100 through 1024 kilobytes.
28. Select the **Email Notification** check box under the **Log Management** section to enable sending the log file to the configured mail server when the log file size exceeds the configured threshold.
29. Select the **TFTP Notification** check box to enable sending the log file to the configured TFTP server when the log file size exceeds the configured threshold.
30. In the **Number of Days to Monitor Processes** field, enter the number of days the memory and CPU utilizations must be monitored. This value ranges from 2 through 10 days.
31. Select the **Email Notification** check box under the **Resource Monitoring** section to send an e-mail notification when the CPU or memory usage size exceeds the configured threshold.
32. In the **SMTP (Mail) Server** field, enter the IP address of the mail server to which the Timing Client will send e-mail.



NOTE: This field is available only if the **Email Notification** check box under the **Log Management** section is selected. Also, the SMTP server information is visible in the **Overall Information** page (Figure 28 on page 74) only if the **Email Notification** check box is selected.


33. In the **TFTP Server** field, enter the IP address of the TFTP server to which the Timing Client will send logs.



NOTE: This field is available only if the **TFTP Notification** check box under the **Log Management** section is selected. Also, the TFTP server information is visible in the **Overall Information** page (Figure 28 on page 74) only if the **TFTP Notification** check box is selected.

34. Click **Next**. The **Setup Wizard Page 5** (Figure 28 on page 74) appears.

Figure 28: Setup Wizard Page 5



TCA6000 Timing Client

Welcome To Setup Wizard

Setup Wizard :
Overall Information
Page 5 of 5

Host Information

Hostname : **TCA6K**
Domain Name : **localhost**

RADIUS Authentication Servers

Server IP	Port	Retries	Timeout	Secret Word

User Details

Username	Email-Id	Class
test	rviji@juniper.net	Read-Write

Timing Configuration

PPS Squelch : **OFF**
Time Zone : **GMT -1:00**
Offset Compensation : **0.000000**
Antenna Cable Delay Compensation : **10000**
Sync Source Priority : **ptp, internal**

Web Status

Web Mode : **Standard HTTP only**
Web Timeout : **30 Minute(s)**

Unsecured Communication Protocols Status

ICMP : **Enable**
TFTP : **Enable**
FTP : **Enable**
TELNET : **Enable**

Protocol Support

Protocol Support Config : **PTP**

Log Management Configuration

Email Notification : **No**
TFTP Notification : **No**
Max Log File Threshold : **1024 Kilobyte(s)**

Resource Monitoring Configuration

Number of Days to monitor processes : **10**
Email Notification : **No**

Server Configuration

SMTP (Mail) Server :

Previous
Finish

The **Overall Configuration Information** page appears and lists the summary of overall settings configured through the setup wizard.

35. Click **Finish**.

A dialog box stating "Your system require reboot to configure protocol-support" is displayed, if you have changed the protocol support. Click **OK** to reboot.

If you have changed the web-mode, then a dialogue box stating "Web-server restart is required to apply new web-mode. Do you want to apply setting" is displayed. Click **Yes** to apply the settings. After confirmation, another dialogue box stating "Web server is going to restart" is displayed. Click **OK** to reboot.

36. A dialog box stating "Do you want to finish Setup-Wizard" is displayed. Click **OK** to finish.

PART 4

Understanding the TCA6000 and TCA6500 GUI

- [Understanding the TCA6000 and TCA6500 Login Page on page 77](#)
- [Understanding the TCA6000 and TCA6500 Status Page on page 81](#)
- [Understanding the TCA6000 and TCA6500 Config Page on page 99](#)
- [Understanding the TCA6000 and TCA6500 Admin Page on page 125](#)
- [Understanding the TCA6000 and TCA6500 Debug Tool Page on page 139](#)
- [Understanding the TCA6000 and TCA6500 Log Page on page 143](#)

CHAPTER 5

Understanding the TCA6000 and TCA6500 Login Page

This chapter describes the Login page for the Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are discussed:

- [Login Page Description on page 77](#)
- [Accessing the Login Page on page 77](#)
- [Understanding the Login Page on page 78](#)

Login Page Description

The Login page appears when the TCA6000 or TCA6500 Timing Client is accessed. The Login page provides information about the Timing Client configuration and other relevant details.

Accessing the Login Page

To access the TCA6000 or TCA6500 Timing Client Login page:

1. Open an Internet browser on a computer.
2. In the **address** field, enter the IP address that has been assigned to the Timing Client, and select Go.

The Login page appears. See [Figure 29 on page 78](#).

Figure 29: TCA6000 or TCA6500 Login Page

JUNIPER
NETWORKS

TCA6000 Timing Client

Username
Password

Forgot password?
Enter username and click [here](#)

● Sync
● Alarms

Local Time : Mon Jan 2 09:28:23 2017
 Hostname : TCA6500-2
 PTP mode : Slave
 Clock Identity : f8:c0:01:ff:fe:08:80:a0
 Current Sync Source : Internal
 Hardware Clock Status : FREERUN
 Alarm Status : Critical
 Model : TCA6500-DC
 Location : anywhere
 Software Version : TCA6K-3.7.0-PTP-E1
 Up Time : 3 Hrs 6 min 1 sec

Network Status		
Port	Address	Link State
LAN1	10.85.33.21/255.255.255.0	up/100/Full

MAC: f8:c0:01:08:80:a0

Understanding the Login Page

Table 4 on page 78 describes the elements that appear in the Login page of the TCA6000 and TCA6500 Timing Clients.



NOTE: After the Login page opens, select the Refresh button in the browser to update the page.

Table 4: Elements on the Timing Client Login Page

Element	Description
Username	Enter the name to be used as a login to the Timing Client.
Password	Enter the user password.
Login button	Click to access the Timing Client pages.
Forgot password	<p>Admin users will be prompted to contact JTAC with the MAC address to get the master password. Upon logging in with the master password, the Admin user has to set a new password.</p> <p>For non-admin users, click to get the new password in your e-mail by authenticating with your username and e-mail ID.</p>

Table 4: Elements on the Timing Client Login Page (*continued*)

Element	Description
Alarms	<p>Indicates whether there are active alarms present on the Timing Client.</p> <ul style="list-style-type: none"> Green—Indicates that there are no active alarms on the Timing Client. Red—Indicates that there is one or more active alarms on the Timing Client.
Local Time	<p>The time kept by the Timing Client clock.</p> <p>NOTE: Click the Refresh button in the browser to update the time.</p>
Hostname	The name assigned to the Timing Client.
PTP Mode	Mode the system is operating. That is, Slave.
Clock Identity	PTP identification. Indicates the local clock identity in 64 bits UUID.
Current Sync Source	Indicates the current sync source type.
Hardware Clock Status	<p>Indicates the synchronization status of the hardware clock.</p> <ul style="list-style-type: none"> Acquiring—Indicates in process to lock to a provisioned reference Lock—Indicates locked to a provisional reference Freerun—Indicates no reference is available Holdover—Indicates in holdover state after all references are disqualified
GPS Receiver (Optional) Status	<p>Indicates the GPS receiver status of the TCA6500 clock. States are as follows:</p> <ul style="list-style-type: none"> No GPS Time. Good—GPS receiver is tracking minimum of three satellites for position solution. No Usable Satellites. Survey-in Progress—GPS board is in self-survey mode and waiting to complete 100%. Do not move unit. Position is Questionable—Saved stored position does not track to the GPS location while tracking present moment. Almanac not Complete—GPS constellation information not completely downloaded. Upon initial power-on, can take up to 12.5 minutes.
Number of Satellites	Indicates the number of GPS satellites the TCA6500 Timing Client has located. All satellites may not be visible.
Alarm Status	Indicates whether there are active alarms in effect.

Table 4: Elements on the Timing Client Login Page (*continued*)

Element	Description
Model	Specifies the Juniper Networks TCA6000 or TCA6500 Timing Server model.
Location	Displays the location of the Timing Client.
Software Version	Indicates the software version of the Timing Client.
Up Time	Indicate the uptime since the most recent power up.
Network Status Window	This window provides network connection information of the Timing Client.
Port	Indicates the port the Timing Client is using.
Address	Lists the IP address assigned to the Timing Client. Lists the MAC address assigned to the Timing Client by the manufacturer.
State	Displays the status of the connection—up or down.

CHAPTER 6

Understanding the TCA6000 and TCA6500 Status Page

This chapter describes the information provided on the TCA6000 or TCA6500 Status page. The following topics are addressed:

- [Understanding System LEDs on page 81](#)
- [Status Page Description on page 81](#)
- [Accessing the Status Page on page 81](#)
- [Understanding the Status Page on page 82](#)

Understanding System LEDs

The TCA6000 and TCA6500 Timing Clients have the following LEDs:

- Power (PWR)—Indicates that the Timing Client is receiving power.
- Critical (CRT)—Indicates that the Timing Client has generated a CRITICAL alarm.
- Major (MAJ)—Indicates that the Timing Client has generated a MAJOR alarm.
- Minor (MIN)—Indicates that the Timing Client has generated a MINOR alarm.
- The network Ethernet port—LAN—Has integrated Sync and Activity LEDs embedded in the RJ45 connector.

Status Page Description

The Status page provides operational and connectivity information for a TCA6000 or TCA6500.

Accessing the Status Page

To access the Status page:

1. Log in to a TCA6000 or TCA6500 Timing Client.
2. Click the **Status** tab. The Status page appears. See [Figure 30 on page 82](#).



NOTE: After the Status page opens, click the Refresh button in the browser to update the page.

Figure 30: Timing Client Status Page—System Pane

Understanding the Status Page

- The Status Page—System Pane on page 83
- The Status Page—Alarm Pane on page 84
- The Status Page—E1 Pane on page 86
- The Status Page—Timing Pane on page 88
- The Status Page—PTP Pane on page 90
- The Status Page—NTP Pane on page 93
- The Status Page—GPS Pane (When GPS Option Is Connected) on page 95
- The Status Page—Resource Pane on page 97

The Status Page—System Pane

Figure 31: Timing Client Status Page—System Pane

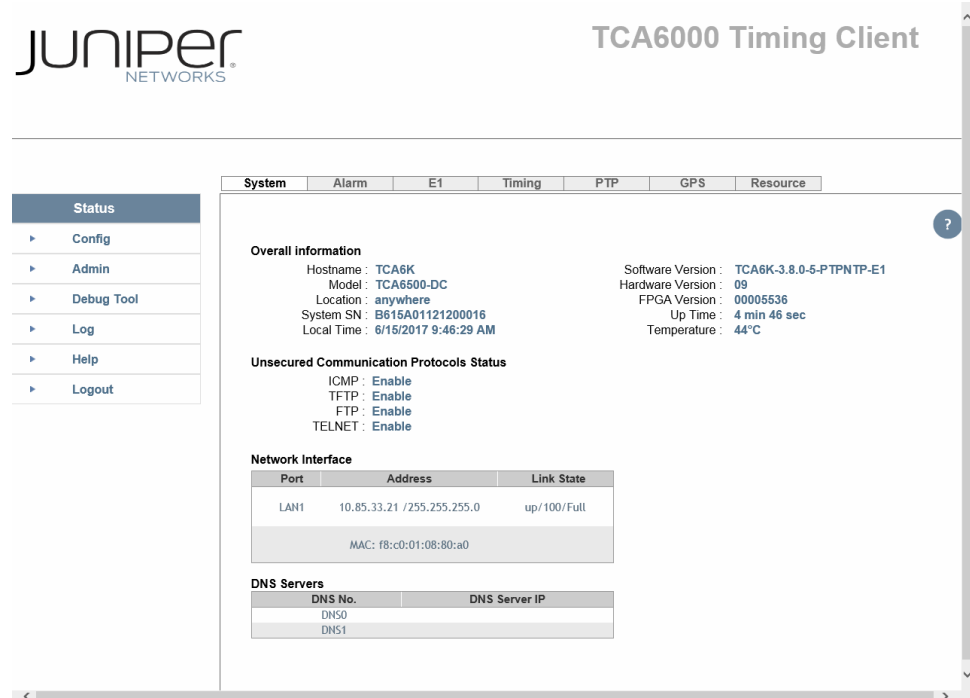


Table 5 on page 83 describes the elements that appear on the Status page—System Pane of the TCA6000 and TCA6500 Timing Clients.

Table 5: Elements on the Timing Client Status Page—System Pane

Element	Description
Overall Information Section	This section provides general information about the Timing Client.
Hostname	The name assigned to the Timing Client. You can use the admin page to assign a name to the server.
Model	The model name of your Timing Client.
Location	Indicates the physical location where the Timing Client is installed.
System SN	The serial number of the Timing Client.
Local Time	The time set on the clock of the Timing Client.
Software Version	The version of software installed on the Timing Client.
Hardware Version	The version of the Timing Client hardware.
FPGA Version	The version of FPGA installed on the Timing Client.

Table 5: Elements on the Timing Client Status Page—System Pane (*continued*)

Element	Description
Up Time	Displays how long the Timing Client has been running since the last power up.
Temperature	Shows the temperature of the Timing Client.
Unsecured Communication Protocols Status Section	This section displays the status of unsecured transfer or communication protocols.
Protocols	Indicates the names of unsecured transfer or communication protocols such as Internet Control Message Protocol (ICMP), Trivial File Transfer Protocol (TFTP), FTP, and Telnet protocol.
Status	Indicates whether the specific unsecured transfer or communication protocol is enabled or disabled.
Network Interface Section	This section provides information about the Timing Client network connections.
Port	Indicates the Timing Client port which the address and state information corresponds to.
Address	The IP address and MAC address used by the Timing Client port.
State	The connectivity state of the port with the network.
DNS Servers Window	This window lists the DNS servers the Timing Client is accessing.

The Status Page—Alarm Pane

The Alarm pane provides valuable information about the health of the system. The Alarm pane provides the necessary information to identify and analyze issues that may be caused as a result of a system problem or an issue external to the system.

Figure 32: Timing Client Status Page—Alarm Pane

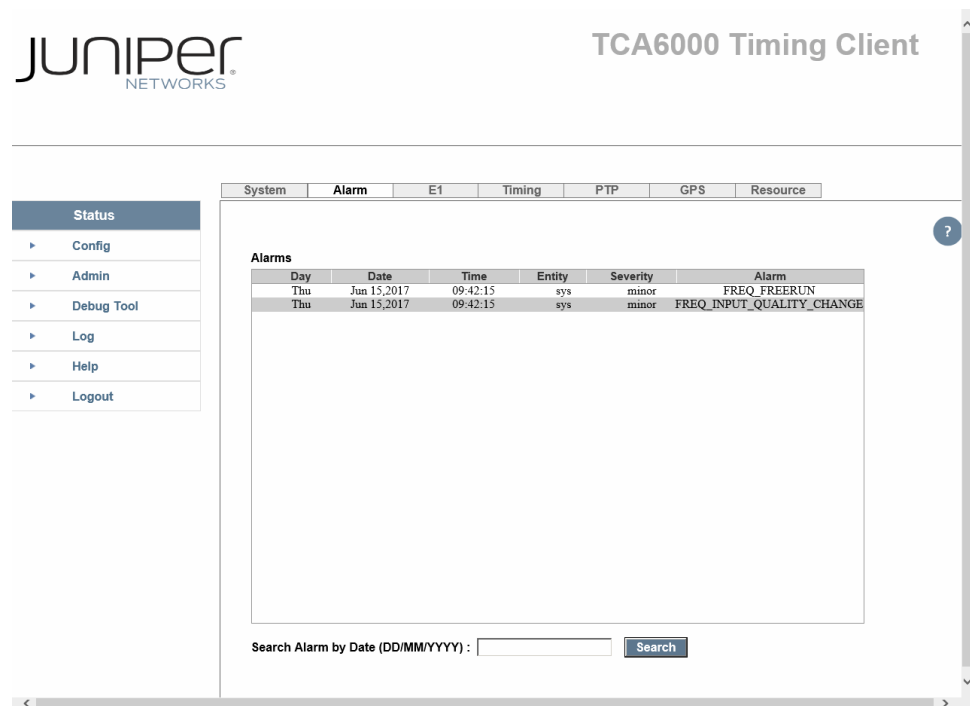


Table 6 on page 85 describes the elements that appear on the Status page—Alarm Pane of the TCA6000 and TCA6500 Timing Clients.

Table 6: Elements on the Timing Client Status Page—Alarm Pane

Element	Description
Alarms Section	This section lists the alarms the Timing Client issues.
Alarms Window	This window displays the alarms the Timing Client issues.
Time	Indicates the time an alarm occurred.
Severity	Indicates the severity of the generated alarm.
Entity	Indicates the entity this alarm is associated with. Alarms can be associated with an input/output or with the whole system.
Alarm	Describes the alarm. See Table 26 on page 128 for details.

The Status Page—E1 Pane

Figure 33: Timing Client Status Page—E1 Pane

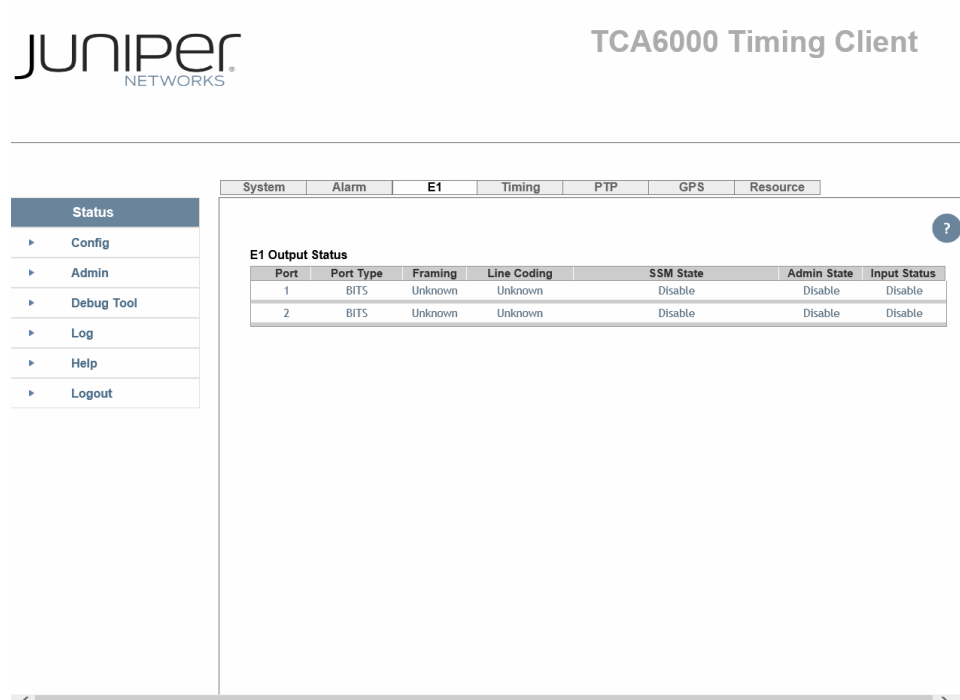


Table 7 on page 86 describes the elements that appear on the Status page—E1 Pane of the TCA6000 and TCA6500 Timing Clients.

Table 7: Elements on the Timing Client Status Page—E1 Pane

Element	Description
E1 Section	This section provides information about elements used by the Timing Client to maintain E1 parameters.
E1 Window	This section enables the setting of the E1 parameters on the Timing Client.
Port	This section indicates the E1 port number of the Timing Client.
Output Mode	Indicates the output modes of the E1 ports on the Timing Client.
Type	Indicates the type of port- BITS on the Timing Client.

Table 7: Elements on the Timing Client Status Page—E1 Pane (*continued*)

Element	Description
Frame Status	<p>Describes the Framing Status of the E1 output ports on the Timing Client as the follows:</p> <ul style="list-style-type: none"> • SF, Super-Frame • ESF, Extended Super-Frame <p>Describes the Framing Status of the T1 input ports on the Timing Client as follows:</p> <ul style="list-style-type: none"> • Normal • LFA, Loss of Frame Alignment • LMFA, Loss of Multi-Frame Alignment • RA, Remote Alarm • RAR, Remote Alarm Recovery • FAR, Frame Alignment Recovery • RRA, Receive Remote Alarm
Line Coding Status	<p>Describes Line Coding of the E1 output ports on the Timing Client as follows:</p> <ul style="list-style-type: none"> • B8ZS, Bipolar 8-Zero Substitution. <p>Describes Line Coding of the E1 input ports on the Timing Client as follows:</p> <ul style="list-style-type: none"> • Normal • LOS, Loss of Signal • LOF, Loss of Frame
SSM	<p>Indicates the E1 Synchronization Status Message for the respective port, and describes the stratum level of the signal as follows:</p> <ul style="list-style-type: none"> • E1_QUALITY_UNKNOWN • E1_REC_G_811 • E1_SSU_A • SSU_B • E1_SETS • E1_DO_NOT_USE
Admin State	Indicates the Port Administration Status in either Disable or Enable mode.
Input Status	<p>Indicates the input status of E1 output ports.</p> <p>NOTE: The Disable value is hard-coded for all E1 output ports. The support for displaying input status is not applicable for E1 input ports.</p>
Framer Gen	<p>Indicates the framer generation configured on the T1 output port. Available options are:</p> <ul style="list-style-type: none"> • FRAME_GEN1 • FRAME_GEN2 <p>NOTE: This field is available only when the Timing Client uses T1 interface type.</p>

The Status Page—Timing Pane

Figure 34: Timing Client Status Page—Timing Pane

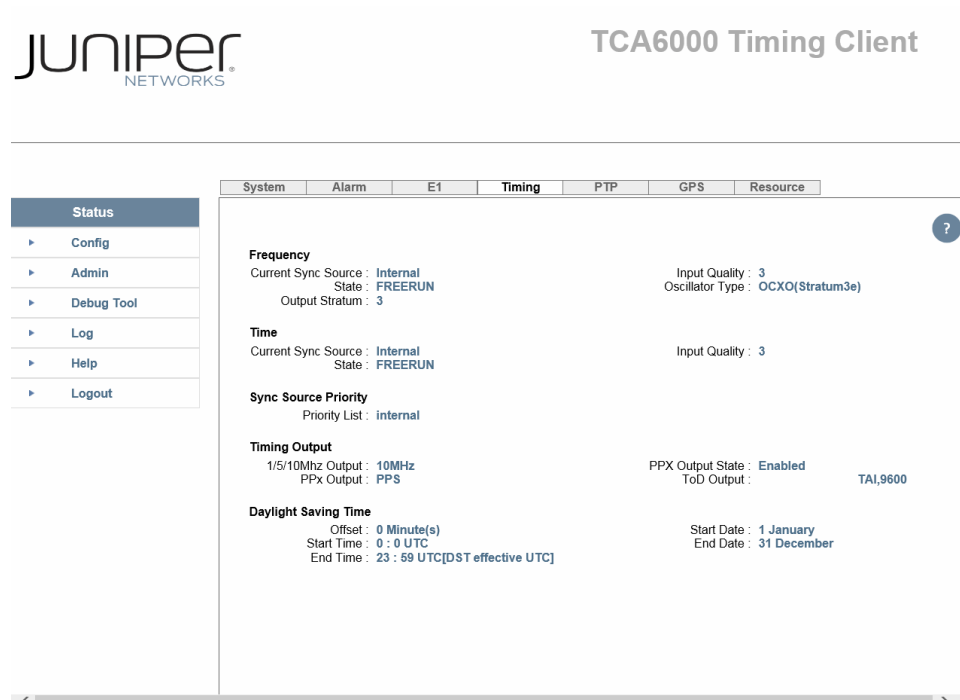


Table 8 on page 88 describes the elements that appear on the Status page—Timing Pane of the TCA6000 and TCA6500 Timing Clients.

Table 8: Elements on the Timing Client Status Page—Timing Pane

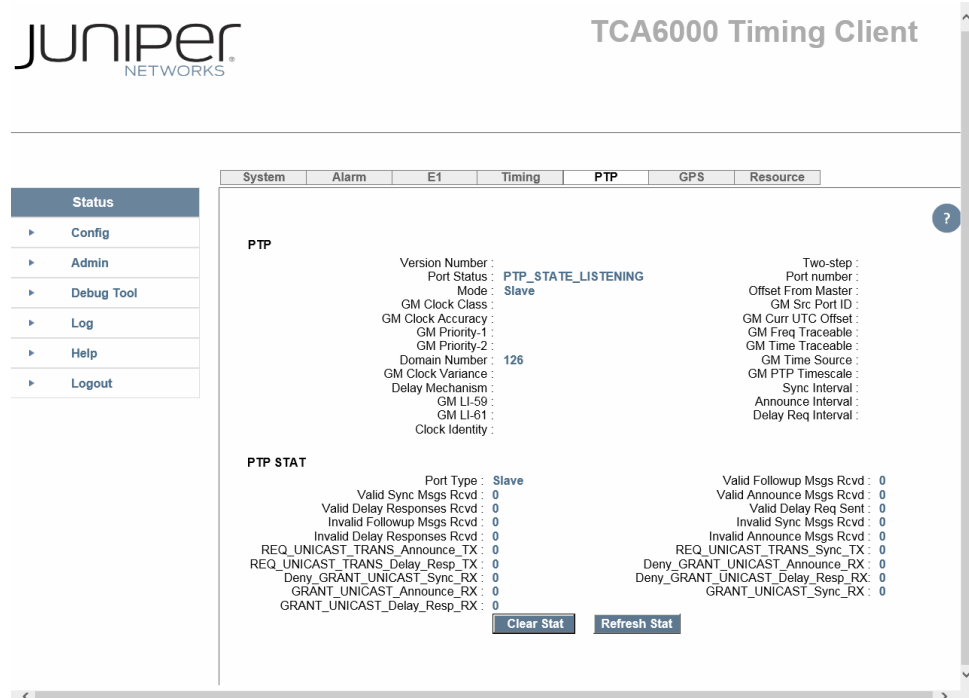
Element	Description
Frequency Section	Describes the status of frequency synchronization.
Current Sync Source	Indicates the reference source used by the Timing Client for frequency synchronization.
Input Quality	Indicates the frequency accuracy, and Stratum level (1 to 3).
State	<p>Indicates the state of the Timing Client as a frequency source:</p> <ul style="list-style-type: none"> Acquiring—in process to lock to a provisioned reference Lock—locked to a provisional reference Freerun—no reference is available Holdover—in holdover state after all references are disqualified. <p>NOTE: Needs to be in the lock state for more than 8 hours before holdover state is qualified.</p>
Oscillator Type	The type of oscillator installed in the Timing Client.
Output Stratum	Stratum level: 1 to 3.

Table 8: Elements on the Timing Client Status Page—Timing Pane (*continued*)

Element	Description
Time Section	Describes status for timing synchronization.
Current Sync Source	Indicates the reference source used by the Timing Client.
Input Quality	Input Time accuracy, Stratum 1 to 3.
State	State of the Timing Client as a time source: <ul style="list-style-type: none"> • Acquiring—in process to lock to a provisioned reference • Lock—locked to a provisional reference • Freerun—no reference is available • Holdover—in holdover state after all references are disqualified
Output Stratum	Output Stratum level: 1 to 3.
Synch Source Priority Section	Describes the priority of various available clock references the Timing Client uses for synchronization.
Priority List	Lists all available clock references in orders of priority for synchronization.
Timing Output Section	Describes the configuration of the timing outputs.
1/5/10MHz Output	Indicates if the output frequency of the 1/5/10 MHz. output is either 1MHz, 5MHz, or 10MHz.
PPx Output	Indicates the availability of the PPx output. Available options are PPS, PPM, PPS2 or PPH.
Daylight Saving Time Section	Describes the configuration of daylight saving time (DST).
Offset	Indicates the configured DST offset value.
Start Date	Indicates the date and month on which the DST starts.
Start Time	Indicates the UTC time scale (in 24-hour format) at which the DST starts.
End Date	Indicates the date and month on which the DST ends.
End Time	Indicates the DST time scale (in 24-hour format) at which the DST ends.

The Status Page—PTP Pane

Figure 35: Timing Client Status Page—PTP Pane



NOTE: You can view this pane only if the PTP support is enabled in the Timing Client.

Table 9 on page 90 describes the elements that appear on the Status page—PTP Pane of the TCA6000 and TCA6500 Timing Clients.

Table 9: Elements on the Timing Client Status Page—PTP Pane

Element	Description
PTP Section	This section provides PTP information pertaining to the Timing Client.
Version Number	IEEE 1588-2008 version number.
Port Status	Indicates the current state of the PTP port. The values are: <ul style="list-style-type: none"> PTP_STATE_INITIALIZING PTP_STATE_FAULTY PTP_STATE_DISALBED PTP_STATE_LISTENING PTP_STATE_PRE_MASTER PTP_STATE_MASTER PTP_STATE_PASSIVE PTP_STATE_UNCALIBRATED

Table 9: Elements on the Timing Client Status Page—PTP Pane (*continued*)

Element	Description
Mode	Indicates that the Timing Client is a PTP slave.
GM Clock Class	Indicates the traceability of the time or frequency distributed by the PTP Grandmaster clock. Clock classes are defined by the IEEE 1588-2008 spec, and are used in the Best Master Clock algorithm.
GM Clock Accuracy	Indicates the clock accuracy of the PTP Grandmaster clock. Clock accuracy value is also used in the Best Master Clock algorithm.
GM Priority-1	Indicates the priority-1 value of the PTP Grandmaster clock. The values range from 0 to 255. Priority-1 value is used in the Best Master Clock algorithm.
GM Priority-2	Indicates the priority-2 value of the PTP Grandmaster clock. The values range from 0 to 255. Priority-2 value is used in the Best Master Clock algorithm.
Domain Number	Indicates the current PTP domain which the Timing Client participates in.
GM Clock Variance	Indicates the inherent precision of the PTP Grandmaster clock. Clock variance is used in the BMC (Best Master Clock) algorithm.
Delay Mechanism	Indicates the delay measurement between the Grandmaster and slave. The system supports E2E.
LI-59	Indicates the last minute of the current UTC day contains 59 seconds. This field is used during leap second correction.
LI-61	Indicates the last minute of the current UTC day contains 61 seconds. This field is used during leap second correction.
Clock Identity	Indicates the local clock identity in 64 bits UUID.
Two Steps	Indicates the option for using one step or two step functions for the PTP protocol.
Port Number	Indicates the port number of the Grandmaster the PTP communicates with.
Offset From Master	Indicates the time difference between the TCA6500 Timing Client and the PTP Grandmaster.
Parent Src Port ID	Indicates the source port ID of the Grandmaster clock.
GM Current UTC Offset	Displays the offset between TAI and UTC for the Grandmaster clock. When the Grandmaster is locked to GPS. The current value of the UTC offset is 33.
GM Freq Traceable	Shows whether the frequency determining the time scale of the Grandmaster clock is traceable to a primary standard.
GM Time Traceable	Indicates whether the timestamp of the Grandmaster clock is traceable to a primary standard.

Table 9: Elements on the Timing Client Status Page—PTP Pane (*continued*)

Element	Description
GM Time Source	Indicates the time source currently in use by the Grandmaster clock. Available options are GPS or Internal clock.
GM PTP Timescale	Displays the clock time scale of the Grandmaster clock. Available options are TRUE if it is PTP, or FALSE if not PTP.
Sync Interval	Indicates the number of sync packet per second the Grandmaster sends. Values are 1, 2, 4, 8, 16, 32 or 64 pps.
Announce Interval	Indicates how long in seconds for the Grandmaster to send the announce packet. The values are 1 packet/1sec, 1packet/2sec, 1 packet/4sec, 1 packet/8sec, 2packet/1sec, 4packet/1sec, and 8packet/1sec.
Delay Req Interval	Indicates the number of delay packet per second the Grandmaster sends. Values are 1 Pkt/64Sec, 1 Pkt/32Sec, 1 Pkt/16Sec, 1 Pkt/8Sec, 1 Pkt/4Sec, 1 Pkt/2Sec, 1 Pkt/Sec, 2 Pkt/Sec, 4 Pkt/Sec, 8 Pkt/Sec, 16 Pkt/Sec, 32 Pkt/Sec, 64 Pkt/Sec, and 128 Pkt/Sec.
PTP STAT	This section displays the PTP statistics pertaining to the Timing Client.
Port Type	Indicates that the port of the Timing Client is a slave.
Valid Sync Msgs Rcvd	Indicates the total number of valid synchronization messages received by the Timing Client from the PTP source.
Valid Announce Msgs Rcvd	Indicates the total number of valid announce messages received by the Timing Client from the PTP source.
Valid Delay Responses Rcvd	Indicates the total number of valid delay responses received by the Timing Client from the PTP source.
Invalid Followup Msgs Rcvd	Indicates the total number of invalid follow up messages received by the Timing Client from the PTP source.
Invalid Delay Responses Rcvd	Indicates the total number of invalid delay responses received by the Timing Client from the PTP source.
Valid Followup Msgs Rcvd	Indicates the total number of valid follow up messages received by the Timing Client from the PTP source.
Valid Delay Req Sent	Indicates the total number of valid delay requests sent from the Timing Client to the PTP source.
Invalid Sync Msgs Rcvd	Indicates the total number of invalid synchronization messages received by the Timing Client from the PTP source.
Invalid Announce Msgs Rcvd	Indicates the total number of invalid announce messages received by the Timing Client from the PTP source.
REQ_UNICAST_TRANS_Announce_TX	Indicates the number of REQ_UNICAST_TRANS_Announce_TX messages.

Table 9: Elements on the Timing Client Status Page—PTP Pane (*continued*)

Element	Description
REQ_UNICAST_TRANS_Sync_TX	Indicates the number of REQ_UNICAST_TRANS_Sync_TX messages.
REQ_UNICAST_TRANS_Delay_Resp_TX	Indicates the number of REQ_UNICAST_TRANS_Delay_Resp_TX messages.
Deny_GRANT_UNICAST_Announce_RX	Indicates the number of Deny_GRANT_UNICAST_Announce_RX messages.
Deny_GRANT_UNICAST_Sync_RX	Indicates the number of Deny_GRANT_UNICAST_Sync_RX messages.
Deny_GRANT_UNICAST_Delay_Resp_RX	Indicates the number of Deny_GRANT_UNICAST_Delay_Resp_RX messages.
GRANT_UNICAST_Announce_RX	Indicates the number of GRANT_UNICAST_Announce_RX messages.
GRANT_UNICAST_Sync_RX	Indicates the number of GRANT_UNICAST_Sync_RX messages.
GRANT_UNICAST_Delay_Resp_RX	Indicates the number of GRANT_UNICAST_Delay_Resp_RX messages.
Clear Stat button	Click to clear PTP statistics. <i>NOTE:</i> Read-Only users cannot clear the displayed PTP statistics.
Refresh Stat button	Click to refresh PTP statistics.

The Status Page—NTP Pane

Figure 36: Timing Client Status Page—NTP Pane

JUNIPER NETWORKS TCA6000 Timing Client

Status

- Config
- Admin
- Debug Tool
- Log
- Help
- Logout

System Alarm T1 Timing NTP GPS Resource

NTP

System Peer : FREERUN_CLOCK
System Peer Mode : Unspecified
Leap Indicator : LEAP NOT IN SYNC
Stratum : 16
Precision : -17
Root Delay : 0.00000 s
Root Dispersion : 0.00761 s

Reference ID : 73.78.73.84
Reference Time : 00000000.00000000; Thu, Feb 7 6:28:16.000 2036
System Flags : Auth Monitor NTP Kernel Stats
Jitter : 0.000000 s
Stability : 0.000 ppm
Broadcastdelay : 0.000000 s
Authdelay : 0.000000 s

NTP Association

Remote	Local	St	Reach	Offset	Poll	Delay	Disp
- LOCAL CLOCK	127.0.0.1	0	0	0.000000	16	0.00000	3.99217



NOTE: You can view this pane only if the NTP support is enabled in the Timing Client.

Table 10 on page 94 describes the elements that appear on the Status page—NTP Pane of the TCA6000 and TCA6500 Timing Clients.

Table 10: Elements on the Timing Client Status Page—NTP Pane

Element	Description
NTP Section	This section enables you to view the NTP details
System Peer	Indicates the number or name of the peer used in clock synchronization.
System Peer Mode	Indicates the NTP operation mode of the peer. The values are: <ul style="list-style-type: none"> Unspecified Broadcast—The peer (selected using the broadcast messages) is used to synchronize the Timing Server clock.
Leap Indicator	Displays a warning about an impending leap second to be inserted or deleted in the last minute of the current day. The values are: <ul style="list-style-type: none"> 0—No warning. 1—Last minute has 61 seconds. 2—Last minute has 59 seconds. 3—Alarm condition, clock not synchronized.
Stratum	Indicates the stratum level of the Timing Server clock. The value ranges from 0 through 255.
Precision	Indicates the precision (in seconds) of the peer clock.
Root Delay	Indicates the total round trip delay (in seconds) to the primary reference source.
Root Dispersion	Indicates the maximum error (in seconds) relative to the primary reference source.
Reference ID	Displays the reference clock used for synchronization.
Reference Time	Indicates the time (in timestamp format) when the Timing Server clock was last updated.
System Flags	Displays the enabled NTP flags. The values are: <ul style="list-style-type: none"> None—Flags are not enabled. bclient—Broadcast Client flag is enabled. auth—Authentication flag is enabled. monitor—Monitor flag is enabled. ntp—NTP support is enabled. kernel—Kernel flag is enabled. stats—Statistics flag is enabled. calibrate—Calibrate flag is enabled. pps—PPS flag is enabled.

Table 10: Elements on the Timing Client Status Page—NTP Pane (*continued*)

Element	Description
Jitter	Indicates the magnitude of jitter (in milliseconds) between time queries.
Stability	Indicates the stability of the Timing Server clock to maintain a constant frequency.
Broadcastdelay	Indicates the round trip delay (in seconds) between the broadcast NTP servers.
Authdelay	Indicates the round trip delay (in seconds) between the authentication NTP servers.
NTP Association Section	This section enables you to view the NTP association details.
Remote	Displays the address or name of the remote NTP peer.
Local	Displays the address or name of the local clock.
St Poll	Displays the stratum of the remote peer and the polling interval (in seconds).
Reach Delay	Displays the results of the last eight poll attempts and the current estimated delay (in milliseconds) of the peer.
Offset Disp	Displays the current estimated offset (in milliseconds) and the current estimated dispersion (in milliseconds) of the NTP peer.

The Status Page—GPS Pane (When GPS Option Is Connected)

Figure 37: Timing Client Status Page—GPS Pane

JUNIPER NETWORKS TCA6000 Timing Client

Status

- Config
- Admin
- Debug Tool
- Log
- Help
- Logout

System Alarm E1 Timing PTP GPS Resource

GPS

Receiver Description : GPS
Receiver Status : Good
Antenna Status : Good
Antenna Voltage : 3.3v
Cable Delay Compensation : 1 ns
Position : 37° 24'28.8309" N; 122° 1'12.1527" W; [View Map](#)
Altitude : -20.62 m
No of Usable Satellites : 11

Satellites

Satellite Number	Signal Noise Ratio	Status
25	6.8 AMU	Acquired
14	8.4 AMU	Acquired
10	8.4 AMU	Acquired
11	13.2 AMU	Acquired
32	7.6 AMU	Acquired
31	9.4 AMU	Acquired
4	10.6 AMU	Acquired
26	4.2 AMU	Acquired
23	6.8 AMU	Acquired

Table 11 on page 96 describes the elements that appear on the Status page—GPS Pane of the TCA6000 and TCA6500 Timing Clients.

Table 11: Elements on the Timing Client Status Page—GPS Pane

Element	Description
GPS Section	This section provides information about the GPS functionality
Receiver Description	Indicates the source that the Timing Client uses to synchronize time.
Receiver Status	<p>Indicates the GPS receiver status of the Timing Client clock. Option states are:</p> <ul style="list-style-type: none"> • Good—Receiver is functioning normally. • No GPS Time. • Doing Fixes—GPS receiver is tracking minimum of three satellites for position solution • No Usable Satellites. • Survey in Progress—GPS board is in self-survey mode and waiting to complete. Do not move unit until finished. • Position is Questionable—Saved stored position does not track to the GPS location while tracking present moment. • Almanac not Complete—GPS constellation information not completely downloaded. Upon initial power-on, can take up to 12.5 minutes. • Not Tracking Satellites. • Only X usable satellite(s). • The chosen Satellite is unusable. • TRAIM rejected the fix—Timing Receiver Autonomous Integrity Monitoring, only in Timing GPS boards, will disregard satellite with highest residual range rate.
Antenna Status	<p>Indicates the condition of the connection between the Timing Client sync-server and the antenna.</p> <ul style="list-style-type: none"> • Open—Electronically open. • Short—Electronically short. • Good—Electronically good.
Antenna Voltage	Indicates the antenna voltage. Available options are 3.3v or 5.0v.
Anti-Jamming	<p>Indicates whether the anti-jamming functionality of the Resolution SMT GPS Timing Receiver is enabled or disabled.</p> <p>NOTE: This field is visible only if the TCA6500 Timing Client uses the Resolution SMT GPS Timing Receiver.</p>
Position	Indicates the coordinates of the Timing Client antenna.
Altitude	Indicates the height of the antenna as determined using GPS information relative to sea level.
Number of Usable Satellites	Indicates the number of satellites observed.
Satellites Section	This window provides information about the satellites to which the Timing Client has established a connection.
Sat Number	Indicates the number of the satellite observed.

Table 11: Elements on the Timing Client Status Page—GPS Pane (*continued*)

Element	Description
Signal to Noise Ratio (SNR)	Indicates the strength of the satellite signal. Typical SNR value should be 4 AMU or higher.
Status	Indicates the communication status between the satellite and the Timing Client. <ul style="list-style-type: none"> Acquired—Communication is established. Never Acquired—Communication with a satellite has never been established.

The Status Page—Resource Pane

Figure 38: Timing Client Status Page—Resource Pane

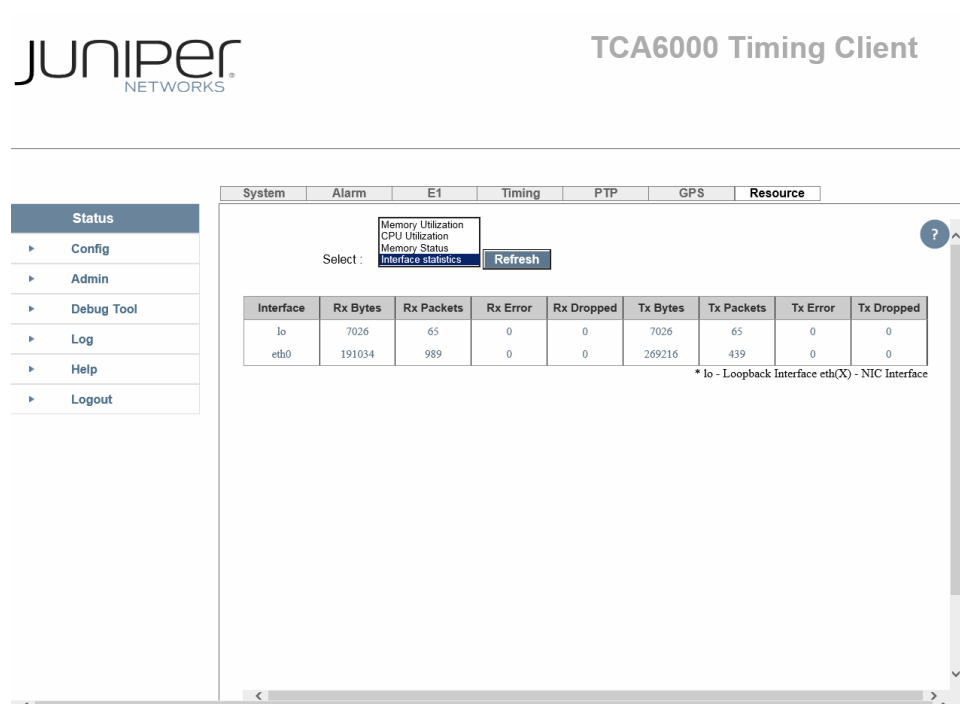


Table 12 on page 97 describes the elements that appear on the Status page—Resource Pane of the TCA6000 and TCA6500 Timing Clients.

Table 12: Elements on the Timing Client Status Page—Resource Pane

Element	Description
Memory Utilization	Indicates the process memory usage in kilobytes for duration of last 10 days. Options are: <ul style="list-style-type: none"> Average Memory Utilization—Average memory usage in kilobytes. Peak Memory Utilization—Peak memory utilization by the process. <p>The memory usage threshold value is the sum of initial memory usage and 100 kilobytes for the specified process in GUI.</p>
CPU Utilization	Indicates the CPU usage for duration of last 10 days. The CPU usage threshold value is 70%.

Table 12: Elements on the Timing Client Status Page—Resource Pane (*continued*)

Element	Description
Memory Status	<p>Displays the following memory usage status in kilobytes:</p> <ul style="list-style-type: none">• Total Memory—Total amount of physical RAM.• Free Memory—Amount of physical RAM available.• Used Memory—Amount of physical RAM in use.• Cached Memory—Amount of physical RAM used as cache memory.
Interface Statistics	<p>Displays the following interface statistics information:</p> <ul style="list-style-type: none">• Rx/Tx Byte(s)—Total number of transmitted or received bytes.• Rx/Tx Packet(s)—Total number of transmitted or received packets.• Rx/Tx Error—Total number of transmitted or received error packets.• Rx/Tx Drop—Total number of dropped packets.

CHAPTER 7

Understanding the TCA6000 and TCA6500 Config Page

This chapter describes the Config page for the Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are addressed:

- [Config Page Description on page 99](#)
- [Accessing the Config Page on page 99](#)
- [Understanding the Config Page on page 100](#)

Config Page Description

The Config pages allow you to change the IP address assigned to your TCA6000 or TCA6500 Timing Client, change the sync source priority, configure T1 output ports, set SNMP access parameters, and adjust the PTP and NTP parameters to be used by the Timing Client, manage user accounts, and configure RADIUS authentication and accounting servers.




NOTE: The Config pages are not visible to the Read-Only users.

Accessing the Config Page

To access the TCA6000 or TCA6500 Timing Client Config page:

1. Log in to the Timing Client.
2. Click the **Config** tab. The Config page appears. See [Figure 39 on page 100](#).

Figure 39: Timing Client Config Page—Network Pane


TCA6000 Timing Client

- ▶ Status
- ▶ Config
- ▶ Admin
- ▶ Debug Tool
- ▶ Log
- ▶ Help
- ▶ Logout

Network
Timing
E1
PTP
Trap
SNMPv3
Users
RADIUS

Network

LAN : ☒ LAN1

IP Address :

Mask :

Gateway :

Primary DNS :

Secondary DNS :

Domain :

Mode : ☒ Static ☐ DHCP

Speed : Mbps

Duplex :

Auto Negotiation :

Ping :

Static Route

	Network	Mask	Gateway	Interface
<input type="radio"/>	10.85.33.0	255.255.255.0	0.0.0.0	eth0
<input type="radio"/>	0.0.0.0	0.0.0.0	10.85.33.1	eth0

VLAN

VLAN : ☒ VLAN1 ☐ VLAN2

IP Address :

Mask :

Id :

Priority :

Mode : ☒ Static ☐ DHCP

Enable : ☐ Yes ☒ No



NOTE: After the Config screen opens, click the Refresh button in your browser. This will update the page.

Understanding the Config Page

- The Config Page—Network Pane on page 101
- The Config Page—Timing Pane on page 103
- The Config Page—E1 Pane on page 105
- The Config Page—PTP Pane on page 108
- The Config Page—NTP Pane on page 112
- The Config Page—Trap Pane on page 115
- The Config Page—SNMPv3 Pane on page 116
- The Config Page—Users Pane on page 118
- The Config Page—Profile Pane on page 119
- The Config Page—RADIUS Pane on page 121

The Config Page—Network Pane

Figure 40: Timing Client Config Page—Network Pane

JUNIPER NETWORKS TCA6000 Timing Client

Navigation: Status, **Config**, Admin, Debug Tool, Log, Help, Logout

Tabs: Network, Timing, E1, PTP, Trap, SNMPv3, Users, RADIUS

Network

LAN: ☒ LAN1

IP Address:

Mask:

Gateway:

Primary DNS:

Secondary DNS:

Domain:

Mode: ☒ Static ☐ DHCP

Speed: Mbps

Duplex:

Auto Negotiation: ☒ Enable

Ping:

Static Route

	Network	Mask	Gateway	Interface
<input type="radio"/>	10.85.33.0	255.255.255.0	0.0.0.0	eth0
<input type="radio"/>	0.0.0.0	0.0.0.0	10.85.33.1	eth0

VLAN

VLAN: ☒ VLAN1 ☐ VLAN2

IP Address:

Mask:

Id:

Priority:

Mode: ☒ Static ☐ DHCP

Enable: ☐ Yes ☒ No

Table 13 on page 101 describes the elements that appear on the Config page—Network pane of the TCA6000 and TCA6500 Timing Clients.

Table 13: Elements on the Timing Client Config Page—Network Pane

Element	Description
Network Section	This section allows you to change the network related parameters for the Timing Client.
LAN1 Option button	Indicates that the network setting is for LAN1.
IP Address	The IP address assigned to the selected port.
Mask	The subnet mask assigned to the selected port.
Gateway	The IP address of the gateway the Timing Client uses to communicate across the network.
Primary DNS	The IP address of the primary DNS used by the Timing Client.

Table 13: Elements on the Timing Client Config Page—Network Pane (*continued*)

Element	Description
Secondary DNS	IP address of the secondary DNS used by the Timing Client.
Domain	Domain name of the LAN.
Mode	<p>The method used by the Timing Client to obtain an IP address.</p> <ul style="list-style-type: none"> • Static—Choose this option button to manually assign an IP address. • DHCP—Select this option button if you want the DHCP server to assign an IP address to the Timing Client automatically. • Apply button—Click to activate the mode you have selected.
Speed	Allows you to select either 100 Mbps or 10 Mbps for the LAN port.
Duplex	Allows you to select either full or half duplex mode for the LAN port.
Auto Negotiation	Allows you to enable or disable auto negotiation for the LAN port.
Ping	<p>Allows you to ping a device on the network.</p> <ul style="list-style-type: none"> • Go button—Click this button to run the ping command.
Static Route Section	This section allows you to add or delete a static route.
Add	Click to add the selected static route entry.
Delete	Click to delete the selected static route entry.
VLAN Section	This section allows you to configure or change the VLAN related parameters for the Timing Client.
VLAN	Use the option button to configure or change the VLAN settings for the Ethernet port.
IP Address	Enter the IP address for the selected VLAN.
Mask	Enter the subnet mask assigned to the selected VLAN.
Id	Enter the VLAN ID ranging from 2 through 4095, which is used to identify the VLAN encapsulation packet.
Priority	Enter a priority value for the VLAN header to be used for differential services transporting the packet. This value ranges from 0 through 7.
Mode	<p>Select a mode to be used by the Timing Client to obtain an IP address for the VLAN.</p> <ul style="list-style-type: none"> • Static—Select this option to manually assign an IP address for the VLAN. • DHCP—Select this option if you want the IP address to be automatically assigned for the VLAN by using the DHCP server.
Enable	Use the option button to enable or disable VLAN encapsulation for IP packets.
Apply	Click to save and implement the changes.

The Config Page—Timing Pane

Figure 41: Timing Client Config Page—Timing Pane

JUNIPER NETWORKS TCA6000 Timing Client

Network Timing E1 PTP Trap SNMPv3 Users RADIUS

Timing config

PPx:
 PPS Squelch: ☐ Yes ☒ No
 Holdover State:
 1/5/10MHz Port: MHz

ToD

Baud Rate:
 Format:

Time Zone

Time Zone:

Daylight Saving Time

Offset: Minute(s)
 Start Date: /
 Start Time: Hour: Minute(s)
 End Date: /
 End Time: Hour: Minute(s)

Antenna Voltage

Voltage:

Antenna Cable Delay Compensation

Value: ns

SNR

SNR:

Sync Source Priority

Priority 1:
 Priority 2:

Offset Compensation

Value: ns

Table 14 on page 103 describes the elements that appear on the Config page—Timing pane of the TCA6000 and TCA6500 Timing Clients.

Table 14: Elements on the Timing Client Config Page—Timing Pane

Element	Description
Timing Config Section	This section allows the user to configure the timing output options on the Timing Client.
PPx	Allows user to set PPS, PPS2, PPM, or PPH signal for the PPx output port. Click the Apply button to commit the changes.
PPS Squelch	<p>Allows you to turn on or off the PPS squelch.</p> <ul style="list-style-type: none"> Yes—The PPS squelch is turned on, thereby disabling the PPS output when the TCA system is not locked to GPS or PTP. No (default)—The PPS squelch is turned off, thereby enabling the PPS output even when the TCA system is not locked to GPS or PTP.

Table 14: Elements on the Timing Client Config Page—Timing Pane (*continued*)

Element	Description
Holdover State	<p>Allows you to set the TCA system to remain in the holdover state or change to the internal state after 24 hours of holdover state.</p> <ul style="list-style-type: none"> • Yes—The system remains in the holdover state instead of changing to the internal state after 24 hours of holdover state. However, the system changes to the internal state when the signal is lost during acquisition, locking, or resetting the system. • No (default)—The system changes to the internal state after 24 hours of holdover state.
1/5/10MHz	Allows you to set the frequency of the 1/5/10 MHz output port.
Time Zone Section	Allows you to set the local time zones.
Daylight Saving Time Section	Allows you to adjust the clock for DST.
Offset	Allows you to select the time period (in minutes) to be adjusted for DST. The default value is 0 minute (that is, the DST is turned off).
Start Date	Allows you to select the date and month on which the DST starts. The default value is 1 st January.
Start Time	Allows you to select the UTC time scale (in 24-hour format) at which the DST starts. The default value is 00:00 UTC (GMT).
End Date	Allows you to select the date and month on which the DST ends. The default value is 31 st December.
End Time	Allows you to select the DST time scale (in 24-hour format) at which the DST ends. The default value is 23:59 DST.
Antenna Voltage	Allows you to set the antenna voltage. Available options are 3.3v or 5v.
Antenna Cable Delay Compensation (ns)	<p>Allows you to set a delay compensation value to compensate for varying cable lengths. This value ranges from -10000 through 10000 nanoseconds.</p> <p>NOTE: You are advised to enter:</p> <ul style="list-style-type: none"> • A negative delay compensation value to compensate the positive delay introduced by the cable. • A positive delay compensation value to advance the PPS output delay relative to the absolute value.
SNR	<p>Allows you to set the signal strength display format to be either AMU or dBHz.</p> <p>NOTE: This field is not visible if the TCA6500 Timing Client uses the Resolution SMT GPS Timing Receiver. The AMU is not an industry standard unit of measurement.</p>
Synch Source Priority Section	Allows you to configure the priority of various synchronization reference sources. Available options are N/A, PTP, or Internal.
Priority List	Allows you to enable a priority to be assigned to a reference source. The sync source list is arranged in orders of priority, with 1 being the highest order.
Apply	Allows you to save the current configuration and apply to memory.

Table 14: Elements on the Timing Client Config Page—Timing Pane (*continued*)

Element	Description
AntiJamming Section	This section allows you to enable or disable the anti-jamming capability of the Resolution SMT GPS Timing Receiver. NOTE: This section is visible only if the TCA6500 Timing Client uses the Resolution SMT GPS Timing Receiver.
Anti-Jamming	Allows you to enable or disable the anti-jamming capability of the Resolution SMT GPS Timing Receiver. <ul style="list-style-type: none"> • Enable—Enables the anti-jamming capability of the Resolution SMT GPS Timing Receiver. • Disable—Disables the anti-jamming capability of the Resolution SMT GPS Timing Receiver.
Apply button	Allows you to save the anti-jamming configuration.

The Config Page—E1 Pane

Figure 42: Timing Client Config Page—E1 Pane

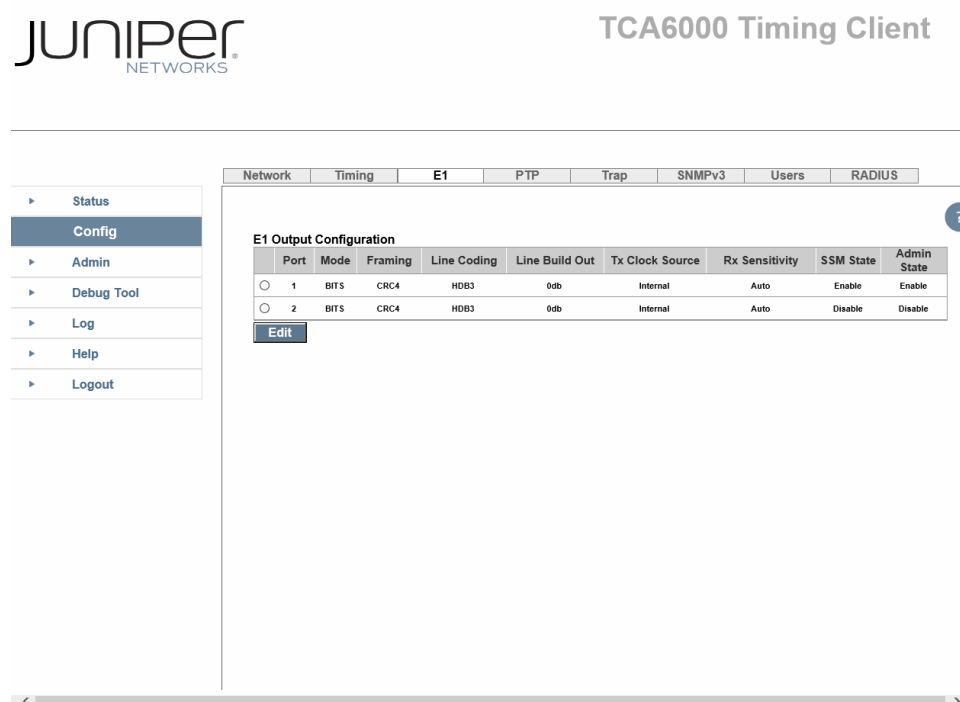


Table 15 on page 105 describes the elements that appear on the Config page—E1 pane of the TCA6000 and TCA6500 Timing Clients.

Table 15: Elements on the Timing Client Config Page—E1 Pane

Element	Description
E1 Output Configuration Section	This window displays the available E1 output ports and their current configuration.

Table 15: Elements on the Timing Client Config Page—E1 Pane (*continued*)

Element	Description
Port	Port number.
Mode	Describes E1 port mode as BITS.
Frame	<ul style="list-style-type: none"> E1 Framing modes CRC4 = Common Channel Signaling (CCS) +CRC4 No CRC4 = Common Channel Signaling (CCS) Channel Associated Signaling (CAS) is NOT supported
Coding	Describes E1 line coding, AMI or HDB3.
LBO	E1 Line Build Out (DB): <ul style="list-style-type: none"> 0dB -7.5dB -15dB -22.5dB
TxClock	Describes the Tx clock source as internal.
RxSen	Describes the Rx clock sensitivity as auto.
SSM	Describes Synchronization Status Message state. Options are Enabled or Disabled.
State	Describes admin state. Options are Enabled or Disabled.
FramerGen	Describes the framer generation configured on the T1 output port. Available options are: <ul style="list-style-type: none"> FRAME_GEN1 FRAME_GEN2 <p>NOTE: This field is available only when the Timing Client uses T1 interface type.</p>
Edit button	Allows the user to edit the parameters of the selected output port using the pull-down manuals at the bottom of the screen.
Port Number	Allows the user to configure the port number.
Mode	Allows user to configure E1 port mode. For the current software release, only BITS is supported.
Framing	Allows user to configure E1 Framing modes: <ul style="list-style-type: none"> CRC4 = Common Channel Signaling (CCS) +CRC4 No CRC4 = Common Channel Signaling (CCS) Channel Associated Signaling (CAS) is NOT supported
Line Coding	Allows user to configure E1 line coding. For the current software release, only HDB3 is supported.

Table 15: Elements on the Timing Client Config Page—E1 Pane (*continued*)

Element	Description
Framer Gen	<p>Allows user to configure first or second generation framer on the T1 output port. Available options are:</p> <ul style="list-style-type: none"> FRAMER_GEN1 FRAMER_GEN2 <p>NOTE: This field is available only when the Timing Client uses T1 interface type.</p>
Line Build Out (LBO)	<p>E1 Line Build Out (DB):</p> <ul style="list-style-type: none"> 0dB -7.5dB -15dB -22.5dB
Tx Clock Source	<p>Allows the user to configure Tx clock source. For the current software release, only Internal is supported.</p>
Rx Sensitivity	<p>Allows the user to configure the Rx Clock Sensitivity. Options are:</p> <ul style="list-style-type: none"> Auto Short Haul Long Haul
SSM State	<p>Allows the user to configure Synchronization Status Message state. Options are Enabled or Disabled.</p>

The Config Page—PTP Pane

Figure 43: Timing Client Config Page—PTP Pane



NOTE: You can view this pane only if the PTP support is enabled in the Timing Client.

Table 16 on page 108 describes the elements that appear on the Config page—PTP pane of the TCA6000 and TCA6500 Timing Clients.

Table 16: Elements on the Timing Client Config Page—PTP Pane

Element	Description
PTP Config Section	This window lists devices with which the Timing Client has a PTP relationship
Telecom Profile	Two options are available—Enabled and Disabled
Priority 1	Field not configurable
Priority 2	Field not configurable
Domain Number	Enter a value ranging between 0–254 to set the domain number associated with the network broadcast domain the Timing Client will join.
Delay Req Mode	Two options are available. Unicast or Multicast

Table 16: Elements on the Timing Client Config Page—PTP Pane (*continued*)

Element	Description
Log Mean Delay Req Interval	Available options: 32 or 64 packets/second
Log Mean Announce Interval	Field not configurable
Log Mean Sync Interval	Field not configurable
Announce Receipt Timeout	Configurable options 2-10
DSCP	Enter the Differential Service (DiffServ) value for the IP packet. NOTE: This should be configured to Explicit Forward (EF) which is a value of 46 decimal.
Apply	Click to save the PTP configuration.
Unicast Section	This section allows you to configure the unicast related parameters.
Sync	<p>Select the sync message rate that the Timing Client requests from the Grandmaster. The available options are:</p> <ul style="list-style-type: none"> • 1 packet/sec • 2 packet/sec • 4 packet/sec • 8 packet/sec • 16 packet/sec • 32 packet/sec • 64 packet/sec <p>NOTE: It is recommended to select 64 packet/sec.</p>
Delay	<p>Select the delay response message rate that the Timing Client requests from the Grandmaster. The available options are:</p> <ul style="list-style-type: none"> • 1 packet/64sec • 1 packet/32sec • 1 packet/16sec • 1 packet/8sec • 1 packet/4sec • 1 packet/2sec • 1 packet/sec • 2 packet/sec • 4 packet/sec • 8 packet/sec • 16 packet/sec • 32 packet/sec • 64 packet/sec • 128 packet/sec <p>NOTE: It is recommended to select 64 packet/sec.</p>

Table 16: Elements on the Timing Client Config Page—PTP Pane (*continued*)

Element	Description
Announce	<p>Select the announce message rate that the Timing Client requests from the Grandmaster. The available options are:</p> <ul style="list-style-type: none"> • 1 packet/1 sec • 1 packet/2 sec • 1 packet/4 sec • 1 packet/8 sec • 2 packets/1sec • 4 packets/1sec • 8 packets/1sec
Duration	Enter the Timing Client expiration duration for sending signaling messages without receiving an acknowledgement from the Grandmaster. This value ranges from 100 seconds through 3000 seconds.
Signaling	<p>Select an option button to enable or disable the sending of signaling messages to the Grandmaster.</p> <p>NOTE: When reverting to profiles other than the Telecom profile, signaling needs to be disabled.</p>
Apply	Click to save the unicast configuration.
Acceptable Master List Section	This section allows you to add or delete the acceptable Grandmasters for the Timing Client, which is used for the Ethernet network packet IP protocol.
Acceptable Master List Window	Displays a list of acceptable Grandmasters with their IP addresses.
Delete	Click to delete the selected Grandmaster entry.
IP Address	Enter the IP address of the acceptable Grandmaster for the Timing Client.
Add	Click to add the acceptable Grandmaster to the Timing Client.

TCA6000 and TCA6500 Timing Client Configurable Profiles

- Default Profile:
 - Supports One-step and Two-step modes.
 - Process Multicast Announce/Sync/Delay Response.
 - Sends Multicast Delay Request with 32 pps or 64 pps.
 - There is no Signaling/Management Packet support.
- Juniper Profile:
 - Supports One-step and Two-step modes.
 - Process Multicast Announce/Sync and Unicast Delay Response.

- Sends Unicast Delay Request with 32 pps or 64 pps.
- There is no Signaling/Management Packet support.
- Telecom Profile:
 - Supports One-step mode only.
 - Process Unicast Announce/Sync and Unicast Delay Response.
 - Sends Unicast Delay Request with 32 pps or 64 pps.
 - Supports Unicast Discovery and Signalling.
- You can use the Web Interface or the CLI to configure the Telecom profile with or without signalling. For more information about using the CLI, see [“Using Telnet with the TCA6000 and TCA6500 Timing Clients” on page 159](#).
- PTP Over Ethernet Profile:
 - Supports One-step and Two-step modes.
 - Process Multicast Announce/Sync/Delay Response.
 - Sends Multicast Delay Request with 32 pps or 64 pps.
 - There is no Signaling/Management/Unicast Packet support.

Table 17: Configuration for Each Profile

Profile	Event Message Type	Packet Type
Juniper Profile	Sync/Delay Response	Multicast
	Delay Request	Unicast
Telecom Profile	Sync/Delay Response	Unicast
	Delay Request	Unicast
Default Profile	Sync/Delay Response	Multicast
	Delay Request	Multicast
PTP Over Ethernet Profile	Sync/Delay Response	Multicast
	Delay Request	Multicast

The Config Page—NTP Pane

Figure 44: Timing Client Config Page—NTP Pane

JUNIPER NETWORKS TCA6000 Timing Client

Network Timing T1 **NTP** Trap SNMPv3 Users RADIUS

► Status
Config
 ► Admin
 ► Debug Tool
 ► Log
 ► Help
 ► Logout

Current NTP Association

Role	Prefer	IP Address	Poll Min	Poll Max	Key	Burst	Version

Edit Delete Add

Mode: Unicast Address:
 Prefer: ☐ Burst: NA
 Version: 4 Time to live: 64
 Min Poll Interval: 4 Max Poll Interval: 4
 Key: Key 1
 Save

MD5 Security Keys

Current Active Keys

```
# ntpkey_MD5key_CERN.3362878469
# Wed Jul 20 04:54:29 2006
1 MD5 "L3SVcP273u3p" # MD5 key
2 MD5 "QhMSEF.hKjL" # MD5 key
3 MD5 "D'W8dE_jPWaib" # MD5 key
4 MD5 "qWGoFa4d8:Utz" # MD5 key
5 MD5 "N*s]Nu;1(ND" # MD5 key
6 MD5 "-u0-Kch0UN5r" # MD5 key
7 MD5 "[-(YVMefmlp)?" # MD5 key
8 MD5 "qW@j4EF" # MD5 key
9 MD5 "8sp7? 4D5y_JRIG" # MD5 key
10 MD5 "t+ZPv3L=Do7N" # MD5 key
11 MD5 "L2F8c0MjY-GKR" # MD5 key
12 MD5 "7a"yVF8aB=ov" # MD5 key
13 MD5 "@G8v""abKp5h5" # MD5 key
14 MD5 "W03-a@nZCaf+~" # MD5 key
15 MD5 "Y"c numD.at:cE" # MD5 key
16 MD5 "D_C"vexA""yAH" # MD5 key
```

Save As Clear

Current New Keys

Generate Reload Save As

Upload Key

Browse... Upload



NOTE: You can view this pane only if the NTP support is enabled in the Timing Client.

Table 18 on page 113 describes the elements that appear on the Config page—NTP pane of the TCA6000 and TCA6500 Timing Clients.

Table 18: Elements on the Timing Client Config Page—NTP Pane

Element	Description
Current NTP Association Section	This section enables you to view and configure the current NTP association details.
Current NTP Association Window	Displays a list of NTP association entries with their corresponding configuration details. A maximum of 20 NTP association entries are supported.
Edit button	Click to modify the configuration details of the selected NTP entry using the elements at the bottom of the page.
Delete button	Click to delete the selected NTP entry.
Add/Edit NTP Association Section	This section enables you to add or edit NTP association details. NOTE: You can add only a maximum of 20 NTP association entries. Each NTP association entry should have a unique IPv4 address configured.
Mode	Select the NTP operation mode to be used by the Timing Client for implementing clock synchronization. The Timing Client supports only the Unicast mode. In the Unicast mode, all remote peers available in the mentioned network are synchronized to the NTP server but the NTP server is not synchronized to any of the remote peer. Remote peers synchronize their time with one NTP server at a time. If the active NTP server is disconnected, then the Timing Client will select another NTP server from the configured server list.
Address	Enter an IPv4 address for the NTP association.
Prefer	Enables this NTP association entry as the preferred server for synchronization among others.
Burst	Select the burst of packets to be sent to the server at each polling interval. Available options are: NA, Burst, iBurst, and Both.
Version	Select the version to be used for the outgoing NTP packets. The available options are 1, 2, 3, and 4. The default version is 4.
Time to live	Enter a TTL value that defines the number of hops for the NTP packets. The value ranges from 1 through 255. The default value is 64. NOTE: This field appears dimmed if you have selected the Unicast mode.
Min Poll Interval	Select the minimum polling interval for NTP messages. You can set a value ranges from 4 through 17. The default value is 6 ($2^6=64$ seconds).
Max Poll Interval	Select the Maximum polling interval for NTP messages. You can set a value ranges from 4 through 17. The default value is 10 ($2^{10}=1024$ seconds).
Key	Select the key identifier that is used to encrypt the authentication fields included in all transferred NTP packets. The available options are None, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, and 16. The key identifier is set to None (no encryption field is included in the NTP packets) by default.

Table 18: Elements on the Timing Client Config Page—NTP Pane (*continued*)

Element	Description
Save button	Click to save the changes.
Current Active Key Section	This section enables you to view the current active MD5 key list.
Current Active Key window	Displays the currently active MD5 key list, which is stored in the /etc/config/ntp/keys path.
Save As button	Click to download the currently active MD5 key list.
Current New Keys Section	This section enables you to view and configure the MD5 key list.
Current New Keys window	Displays the new MD5 key list, which is stored in the /etc/config/ntp/tempkeys path.
Generate button	Click to generate MD5 key list by using the system command ntp-keygen . This generated key list is stored in the /etc/config/ntp/tempkeys path.
Reload button	Click to reload the new MD5 key list.
Save As button	Click to download the new MD5 key list.
Upload Key Section	This section enables you to upload new MD5 keys.
Upload Key	Displays the file (including path) containing new MD5 keys. These keys are merged with the list stored in the /etc/config/ntp/tempkeys path.
Browse button	Click to locate the file containing new MD5 keys.
Upload button	Click to upload new MD5 keys.

The Config Page—Trap Pane

Figure 45: Timing Client Config Page—Trap Pane

Table 19 on page 115 describes the elements that appear on the Config page—Trap pane of the TCA6000 and TCA6500 Timing Clients.

Table 19: Elements on the Timing Client Config Page—Trap Pane

Element	Description
SNMP Section	This section allows you to set the SNMP contact parameters to be used by the Timing Client.
sysLocation	Specifies the location of the Timing Client.
sysName	Provides information describing the Timing Client.
sysContact	Specify contact information of the administrator assigned to manage the Timing Client.
ReadOnlyComm	Enter the command the network will use to request read community strings.
RWriteComm	Enter the command the network will use to request write community strings.
Apply button	Click to save SNMP parameters to memory.
Trap Section	View and specify trap destinations to which the Timing Client sends alarm information. NOTE: You can configure only a maximum of 20 Trap servers.

Table 19: Elements on the Timing Client Config Page—Trap Pane (*continued*)

Element	Description
Destination	The IP address of the trap to which the Timing Client sends SNMP data.
Port	The port number through which the Timing Client sends event information.
Add button	Create a trap destination.
Edit button	Edit the parameters of the trap destination.
Delete button	Delete the trap destination.
Address	Enter the IP address of the Trap to which the Timing Client will send alarm information.
Port	Enter the port number through which the Timing Client sends alarm information.
Save button	Save information to memory.

The Config Page—SNMPv3 Pane

Figure 46: Timing Client Config Page—SNMPv3 Pane

The screenshot shows the Juniper Networks TCA6000 Timing Client configuration interface. The left sidebar contains navigation links: Status, Config (selected), Admin, Debug Tool, Log, Help, and Logout. The main content area has tabs for Network, Timing, T1, PTP, Trap, SNMPv3 (selected), Users, and RADIUS. The SNMPv3 pane displays a table for V3User with columns Username, Auth Crypt, and Priv Protocol. Below the table are Edit, Delete, and Add buttons. A modal form for adding a new user is open, showing fields for Name, Auth Crypt (MD5 or SHA1), Auth PassPhrase, Priv Protocol (DES, AES, or No Privacy), and Priv Phrase, with a Save button.

Table 20 on page 117 describes the elements that appear on the Config page—SNMPv3 pane of the TCA6000 and TCA6500 Timing Clients.

Table 20: Elements on the Timing Client Config Page—SNMPv3 Pane

Element	Description
V3 User Section	<p>The v3 User section allows the identification of SNMPv3 users who have access to information about the Timing Client.</p> <p>NOTE: You can configure only a maximum of 20 SNMPv3 users.</p>
Username	Login name of the user.
Auth Crypt	Specifies the type of encryption a user will use to log in to the Timing Client.
Pri Protocol	Selects encryption mode on the Timing Client. Available options are DES, AES, No Privacy.
Add button	Creates a SNMPv3 user.
Edit button	Edits the parameters for the SNMPv3 user.
Delete button	Removes a user from the list.
Name	The username assigned to access the Timing Client.
Auth Phrase	Creates a unique authentication password for a user. The password must contain six or more characters.
Auth Crypt	<p>Selects encryption type:</p> <ul style="list-style-type: none"> • MD5—Use MD5 cryptographic scheme • SHA1—Use SHA1 cryptographic scheme
Pri Phrase	Creates a unique encryption privilege-phrase for messages exchanged between the user and the Timing Client.
Pri Protocol	<p>Allows you to configure the privacy protocol for the SNMPv3 user.</p> <ul style="list-style-type: none"> • DES = Use DES (Data Encryption Standard) • AES = Use AES (Advanced Encryption Standard) • No Privacy = Do not use encryption
Save button	Save information to memory.

The Config Page—Users Pane

Figure 47: Timing Client Config Page—Users Pane

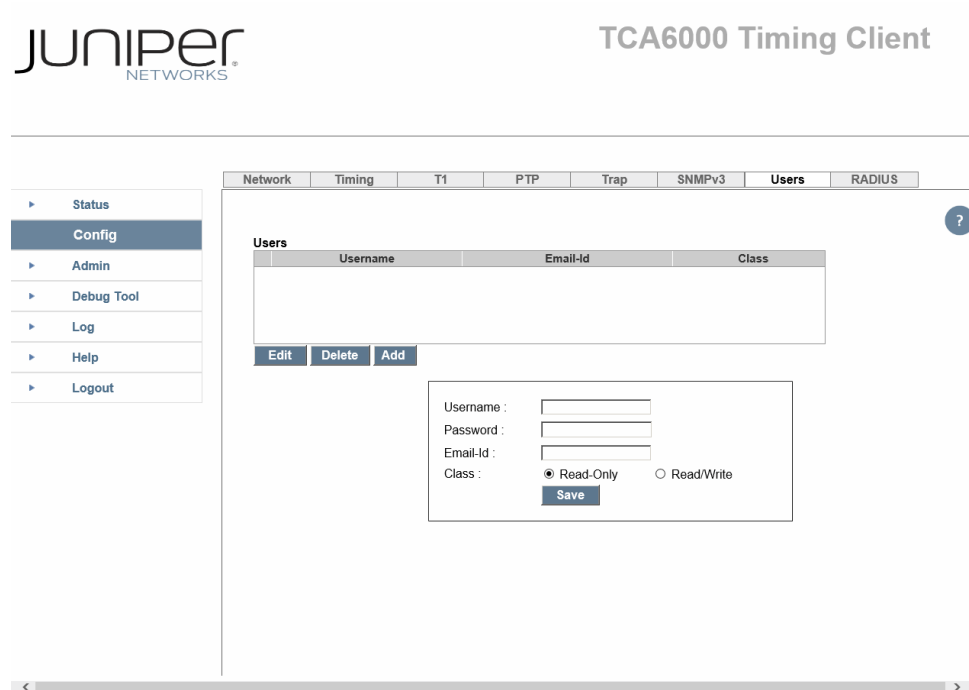


Table 21 on page 118 describes the elements that appear on the Config page—Users pane of the TCA6000 and TCA6500 Timing Clients.



NOTE: For Read/Write users, the Profile pane is available instead of the Users pane. The Users pane is visible only to the Admin user. For information about the Profile pane, see “The Config Page—Profile Pane” on page 119.

Table 21: Elements on the Timing Client Config Page—Users Pane

Element	Description
Users Section	This section allows you (Admin user) to view and configure user account details
Users Window	Displays a list of configured user accounts with their username and login class details. NOTE: <ul style="list-style-type: none"> Account information of the Admin user is not displayed in this list. Only the information of the Read-Only and Read/Write users is listed. You can create only a maximum of five user accounts.
Add button	Click to create a new user account.
Edit button	Click to modify the configuration details of the selected user account.

Table 21: Elements on the Timing Client Config Page—Users Pane (*continued*)


Element	Description
Delete button	Click to delete the selected user account from the user account list.
Username	Enter the username for the user account. The character length ranges from 4 through 12 characters. The characters that can be used are alphanumeric and underscore (that is, _).
Password	Enter the password for the user account. The character length ranges from 4 through 12 characters. The characters that can be used are alphanumeric and special characters (that is, !@#\$_).
Email-Id	Enter the e-mail address for the new user account.
Class	Select to configure the login class for the user account. The options are: <ul style="list-style-type: none"> ReadOnly—User is given show view privilege. For more information, see Table 3 on page 20. Read/Write—User is given modify privilege. For more information, see Table 3 on page 20.
Save button	Click to save the changes.

The Config Page—Profile Pane



NOTE: For Read/Write users, the Profile pane is available instead of the Users pane. The Users pane is visible only to the Admin user.

Figure 48: Timing Client Config Page—Profile Pane



JUNIPER
NETWORKS

TCA6000 Timing Client

► Status

Config

► Debug Tool

► Log

► Help

► Logout

Network
Timing
E1
NTP
Trap
SNMPv3
Profile
RADIUS

Change Password

Old Password :

New Password :

Retype New Password :

Save

Table 22 on page 120 describes the elements that appear on the Config page—Profile pane of the TCA6000 and TCA6500 Timing Clients.



NOTE: For the Admin user, Users pane is available instead of the Profile pane. Profile pane is visible only to the Read/Write user. For information about the Users pane, see “[The Config Page—Users Pane](#)” on page 118. The password of the Admin user can be changed from the Admin page.

Table 22: Elements on the Timing Client Config Page—Profile Pane

Element	Description
Change Password Section	This section allows you (Read/Write user) to change the password for your user account.
Old Password	Enter the current password.
New Password	Enter the new password to be set for your user account. The character length ranges from 4 through 12 characters. The characters that can be used are alphanumeric and special characters (that is, !@#\$%).
Retype New Password	Reenter the password typed in the New Password field.
Save button	Click to change your password and save the changes. NOTE: The new password will be effective from next login onwards. The current session is not affected.

The Config Page—RADIUS Pane

Figure 49: Timing Client Config Page—RADIUS Pane

The screenshot displays the Juniper TCA6000 Timing Client configuration interface. On the left is a navigation menu with options: Status, Config (selected), Admin, Debug Tool, Log, Help, and Logout. The main content area has tabs for Network, Timing, E1, PTP, Trap, SNMPv3, Users, and RADIUS. The RADIUS tab is active, showing the following sections:

- RADIUS Authentication Servers:** A table with columns for Server IP, Port, Retries, Timeout, and Secret Word. Below the table are buttons for Edit, Delete, and Add.
- Authentication Order:** Two dropdown menus for 'radius' and 'local', followed by an Apply button.
- RADIUS Accounting Servers:** A table with columns for Server IP, Port, Retries, Timeout, and Secret Word. Below the table are buttons for Edit, Delete, and Add.
- RADIUS Accounting Level:** Three radio button options:
 - 1: For login accounting only
 - 2: For interactive and login accounting
 - 3: For configuration, interactive and login accounting (selected)
- RADIUS Accounting Status:** Two radio button options: Enable (selected) and Disable, followed by an Apply button.

Table 23 on page 121 describes the elements that appear on the Config page—RADIUS pane of the TCA6000 and TCA6500 Timing Clients.

Table 23: Elements on the Timing Client Config Page—RADIUS Pane

Element	Description
RADIUS Authentication Servers Section	This section allows you to view and configure RADIUS authentication servers to be used by the Timing Client for user authentication.
Radius Authentication Servers window	Displays a list of configured RADIUS authentication servers with their corresponding configuration details. NOTE: You can add only a maximum of three RADIUS authentication servers.
Add button	Click to create a RADIUS authentication server.
Edit button	Click to modify the configuration details of the selected RADIUS authentication server.
Delete button	Click to delete the selected RADIUS authentication server from the server list.
Server IP	Enter the IP address of the RADIUS authentication server to be used for user authentication.

Table 23: Elements on the Timing Client Config Page—RADIUS Pane (*continued*)

Element	Description
Port	Enter the port through which the specified RADIUS authentication server is contacted for user authentication. The default port number is 1812.
Retry	<p>Enter the number of attempts to be tried for contacting the specified RADIUS authentication server. The value ranges from 1 through 10. The default value is 3.</p> <p>When all retries fail, the Timing Client contacts the next RADIUS authentication server in the authentication server list.</p>
Timeout	<p>Enter the time in seconds till which the Timing Client waits for a response from the specified RADIUS authentication server. The value ranges from 1 through 90 seconds. The default value is 3 seconds.</p> <p>If the response is not received within the specified time period and the configured retry limit is not attained, then the Timing Client once again tries to contact the authentication server.</p> <p>If the response is not received within the specified time period and the configured retry limit is attained, then the Timing Client contacts the next RADIUS authentication server in the authentication server list.</p>
Secret Word	Enter the password shared with the specified RADIUS authentication server. The character length ranges from 16 through 32 characters. The characters that can be used to define the secret word are A-Z, a-z, 0-9, and special symbols (that is, ` ! @ # \$ % ^ * () _ + - = { } [] ; < > , . /).
Save button	Click to save the configuration details of the RADIUS authentication server.
Authentication Order Section	<p>This section allows you to configure the order of authentication. The default authentication order is RADIUS server authentication and then the local authentication.</p> <ul style="list-style-type: none"> radius—User is authenticated by using configured RADIUS authentication servers. local—User is authenticated locally. <p>NOTE: The value in the first drop box takes precedence over the value in the second drop box.</p>
RADIUS Accounting Servers Section	This section allows you to view and configure RADIUS accounting servers to be used by the Timing Client for accounting.
Radius Accounting Servers window	<p>Displays a list of configured RADIUS accounting servers with their corresponding configuration details.</p> <p>NOTE: You can add only a maximum of three RADIUS accounting servers.</p>
Add button	Click to create a RADIUS accounting server.
Edit button	Click to modify the configuration details of the selected RADIUS accounting server.
Delete button	Click to delete the selected RADIUS accounting server from the server list.
Server IP	Enter the IP address of the RADIUS accounting server to be used for accounting.
Port	Enter the port through which the specified RADIUS accounting server is contacted for accounting. The default port number is 1813.

Table 23: Elements on the Timing Client Config Page—RADIUS Pane (*continued*)

Element	Description
Retry	<p>Enter the number of attempts should be made for contacting the specified RADIUS accounting server. The value ranges from 1 through 10. The default value is 3.</p> <p>When all retries fail, the Timing Client contacts the next RADIUS accounting server in the accounting server list.</p>
Timeout	<p>Enter the time in seconds till which the Timing Client waits for a response from the specified RADIUS accounting server. The value ranges from 1 through 90 seconds. The default value is 3 seconds.</p> <p>If the response is not received within the specified time period and the configured retry limit is not attained, then the Timing Client once again tries to contact the accounting server.</p> <p>If the response is not received within the specified time period and the configured retry limit is attained, then the Timing Client contacts the next RADIUS accounting server in the accounting server list.</p>
Secret Word	<p>Enter the password shared with the specified RADIUS accounting server. The character length ranges from 16 through 32 characters. The characters that can be used to define the secret word are A-Z, a-z, 0-9, and special symbols (that is, ` ! @ # \$ % ^ * () _ + - = { } [] ; < > , . /).</p>
Save button	Click to save the configuration details of the RADIUS accounting server.
RADIUS Accounting Level Section	<p>This section allows you to configure the type of accounting information to be logged in the RADIUS accounting server.</p> <ul style="list-style-type: none"> 1: For login accounting only—Only the login information is sent to the RADIUS accounting server for accounting. 2: For interactive and login accounting—The login information and interactive command details are sent to the RADIUS accounting server for accounting. 3: For configuration, interactive and login accounting—The login information, interactive command details, and configuration command details are sent to the RADIUS accounting server for accounting. <p>The default value is 3: For configuration, interactive and login accounting.</p>
Apply button	Click to activate the selected accounting level.
RADIUS Accounting Status Section	<p>This section allows you to enable or disable RADIUS accounting in the Timing Client.</p> <ul style="list-style-type: none"> Enable—Enables RADIUS accounting. Disable—Disables RADIUS accounting. <p>By default RADIUS accounting is enabled.</p>
Apply button	Click to activate the selected RADIUS accounting status.

CHAPTER 8

Understanding the TCA6000 and TCA6500 Admin Page

This chapter describes the Admin page for the Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are addressed:

- [Admin Page Description on page 125](#)
- [Accessing the Admin Page on page 125](#)
- [Understanding the Admin Page on page 125](#)

Admin Page Description

The Admin page allows you to perform administrative tasks and to set administrative parameters for the TCA6000 and TCA6500 Timing Clients.



NOTE: The Admin page is visible only for the Admin user.

Accessing the Admin Page

To access the Admin page of a TCA6000 or TCA6500 Timing Client:

1. Log in to the Timing Client.
2. Click the **Admin** tab. The Admin page appears. See [Figure 50 on page 126](#).



NOTE: After the Admin page opens, click the Refresh button in the browser to update the page.

Understanding the Admin Page

- [The Admin Page—Password Pane on page 126](#)
- [The Admin Page—Alarm Pane on page 127](#)
- [The Admin Page—Service Pane on page 131](#)

- The Admin Page—Upgrade Pane on page 133
- The Admin Page—Config Pane on page 134
- The Admin Page—Remote Log Pane on page 137
- The Admin Page—Web-Session Pane on page 138

The Admin Page—Password Pane

Figure 50: Timing Client Admin Page—Password Pane

Table 24 on page 126 describes the elements that appear on the Admin page—Password pane of the TCA6000 and TCA6500 Timing Clients.

Table 24: Elements on the Timing Client Admin Page—Password Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
System Name & Password Section	This section enables a name to be assigned to the Timing Client and change the login password.
Hostname	The name assigned to the Timing Client. This name is displayed on the Status page.
Old Password	Enter the current password.
New Password	Enter the new password to replace the old password.
Retype New Password	Reenter the new password to replace the old password.

Table 24: Elements on the Timing Client Admin Page—Password Pane (*continued*)

Element	Description
Default Password	Reset the password to the factory default.
Apply button	Saves the hostname and password changes to memory.

The Admin Page—Alarm Pane

Figure 51: Timing Client Admin Page—Alarm Pane

JUNIPER NETWORKS TCA6000 Timing Client

Web Session times out in :54m 50s

Profile

Name	State	Clear Now	Auto Clear	Severity	Send Trap	Write Log	Send Email
FREQ_INPUT_QUALITY_CHANGE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LINK_DOWN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LINK_UP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TEMPERATURE_DISABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FREQ_ACQUIRING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOG_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTP_GM_DISABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTP_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BOA_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ALARM_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOG_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CLI_MEM_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PTP_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BOA_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ALARM_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOG_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CLI_CPU_THRESHOLD_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply

Auto Clear Expiration

Timer (hour) 24 Apply

Alarm Email Recipients

SMTP : From :

User1 : User2 :

User3 : User4 :

User5 : Apply

Table 25 on page 127 describes the elements that appear on the Admin page—Alarm pane of the TCA6000 and TCA6500 Timing Clients.

Table 26 on page 128 describes the alarms.

Table 25: Elements on the Timing Client Admin Page—Alarm Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
System Name & Password Section	This section allows the configuration of alarms generated by the Timing Client.
Name	Name of the Timing Client alarm.

Table 25: Elements on the Timing Client Admin Page—Alarm Pane (*continued*)

Element	Description
State	Indicates whether the alarm is ON or OFF.
Clear Now	Check this box to clear alarms when the Apply button is pressed.
Auto Clear	Check this box to clear alarms automatically after 24 hours.
Severity	Specifies the severity level of an alarm.
Send Trap	Check this box for the Timing Client to send an alarm message to trap locations.
Write Log	Check this box for the Timing Client to record the alarm in the local log file.
Send Email	Check this box for the Timing Client to send an e-mail message of the alarm to users who have been configured to receive alarm messages.
Apply button	Save changes to memory.
Alarm Email Recipient Section	<p>Specifies the SMTP server to which the Timing Client will send alarm e-mail messages, and lists the recipients that will receive messages.</p> <ul style="list-style-type: none"> • SMTP—Enter the IP address of the mail server. • From—Enter the from address of the outbound alarm e-mails. • User X—Enter the e-mail address of the user to whom the Timing Client will send alarm e-mail messages. • Apply—Click to save alarm e-mail recipient information to memory.

Table 26: Description of Alarm Names

Alarm Name	Description
NTP_STRATUM_CHANGE	Indicates that the stratum level of the NTP server has changed.
NTP_LEAP_CHANGE	Indicates that the NTP leap seconds have changed.
NTP_STOPPED	Indicates that the NTP daemon is stopped.
NTP_AUTHFAIL	Indicates an NTP authentication failure.
SYS_CONFIG_CHANGE	Indicates the configuration has changed.
SYS_AUTHENTICATION	Indicates a system authentication failure.
GPS_ANTENNA_SHORT	Indicates an electrical short in the link to the GPS antenna.
GPS_ANTENNA_OPEN	Indicates an electrical open in the link to the GPS antenna.
GPS_NO_USABLE_SATELLITE	Indicates the GPS antenna is not receiving a signal from any satellite.

Table 26: Description of Alarm Names (*continued*)

Alarm Name	Description
GPS_LEAP_SECOND_PENDING	Provides a warning of an impending leap second change.
TIMING_OSC_DAC_RANGE	Indicates that the frequency of the oscillator is out of the tuning range.
GPS_RECEIVER_INACTIVE	The GPS receiver is not active.
TIMING_OSC_DAC_RANGE	The frequency of the oscillator is outside of the tuning range.
TIMING_NON_STRATUM_ONE	The source of the timing loop is not Stratum 1 traceable.
OVEN_TEMP_RANGE_HIGH	Indicates that the secondary oscillator oven temperature is greater than the set point temperature. This is only a status indicator as there is no impact on the oscillator primary oven control or its stability. We recommend that the severity be set to NONE.
OVEN_TEMP_RANGE_LOW	Indicates that the secondary oscillator oven temperature is less than the set point temperature. This is only a status indicator as there is no impact on the oscillator primary oven control or its stability. We recommend that the severity be set to NONE.
TE1_LOS	Indicates a loss of signal condition on the first T1/E1 timing input port.
TE1_LOF	Indicates a loss of frame condition on the first T1/E1 timing input port.
TE1_AIS	Indicates that an alarm indication signal is received on the first T1/E1 timing input port.
TE1_RAI	Indicates that a remote alarm indication signal is received on the first T1/E1 timing input port.
TE2_LOS	Indicates a loss of signal condition on the second T1/E1 timing input port.
TE2_LOF	Indicates a loss of frame condition on the second T1/E1 timing input port.
TE2_AIS	Indicates that an alarm indication signal is received on the second T1/E1 timing input port.
TE2_RAI	Indicates that a remote alarm indication signal is received on the second T1/E1 timing input port.
SYS_DIAG_FAILURE	Indicates that there is a system failure reported by the system diagnostic utility.
NTP_PEER_UNREACHABLE	Indicates that the configured NTP peer is not reachable.
PTP_SERVER_UNREACHABLE	Indicates that the PTP server configured in the PTP association table is not reachable.
PTP SERVER CHANGE	A change in the PTP Grandmaster source selection has occurred.

Table 26: Description of Alarm Names (*continued*)

Alarm Name	Description
LOSS_OF_POWER_FEED	Indicates that one of the two DC power feeds is not connected, or is not powered. Set alarm Severity to NONE if only one DC power feed is used.
FREQ_HOLDOVER	Indicates that the Timing Client is in holdover.
FREQ_FREERUN	Indicates that the Timing Client is in freerun.
FREQ_REF_INPUT_CHANGE	Indicates that the reference source for Timing Client has changed.
FREQ_REF_QUALITY_CHANGE	Indicates that the stratum level of the reference source for the Timing Client has changed.
FREQ_ACQUIRING	Indicates that the system tries to adjust the local oscillator based on the input source such as GPS, T1, E1, and PTP. If the adjustments are completed, then the system state is changed from acquiring state to locked state.
TIMEPROBE_DISABLE	Indicates that the time probe agent is disabled or accidentally turned off.
LINK_DOWN	Indicates that the Ethernet ports is down.
LINK_UP	Indicates that the Ethernet ports is up.
LICENSE_KEY_EXPIRE_WITHIN_60_DAYS	Indicates that the license key for a particular licensable feature is about to expire.
LOG_THRSHOLD_EXCEEDED	Indicates that log files (auth, daemon and event) size exceeds the configured threshold value on system.
PTP_MEM_THRSHOLD_EXCEEDED	Indicates that PTP process size in main memory exceeds its threshold value.
BOA_MEM_THRSHOLD_EXCEEDED	Indicates that web-server process size in main memory exceeds its threshold value.
SNMP_MEM_THRSHOLD_EXCEEDED	Indicates that SNMP process size in main memory exceeds its threshold value.
ALARM_MEM_THRSHOLD_EXCEEDED	Indicates that alarm manager process size in main memory exceeds its threshold value.
LOG_MEM_THRSHOLD_EXCEEDED	Indicates that log manager process size in main memory exceeds its threshold value.
CLI_MEM_THRSHOLD_EXCEEDED	Indicates that CLI process size in main memory exceeds its threshold value.
PTP_CPU_THRSHOLD_EXCEEDED	Indicates that CPU threshold value exceeds for PTP.
BOA_CPU_THRSHOLD_EXCEEDED	Indicates that CPU threshold value exceeds for web-server.
SNMP_CPU_THRSHOLD_EXCEEDED	Indicates that CPU threshold value exceeds for SNMP.

Table 26: Description of Alarm Names (*continued*)

Alarm Name	Description
ALARM_CPU_THRSHOLD_EXCEEDED	Indicates that CPU threshold value exceeds for alarm manager.
LOG_CPU_THRSHOLD_EXCEEDED	Indicates that CPU threshold value exceeds for log manager.
CLI_CPU_THRSHOLD_EXCEEDED	Indicates that CPU threshold value exceeds for CLI.

The Admin Page—Service Pane

Figure 52: Timing Client Admin Page—Service Pane

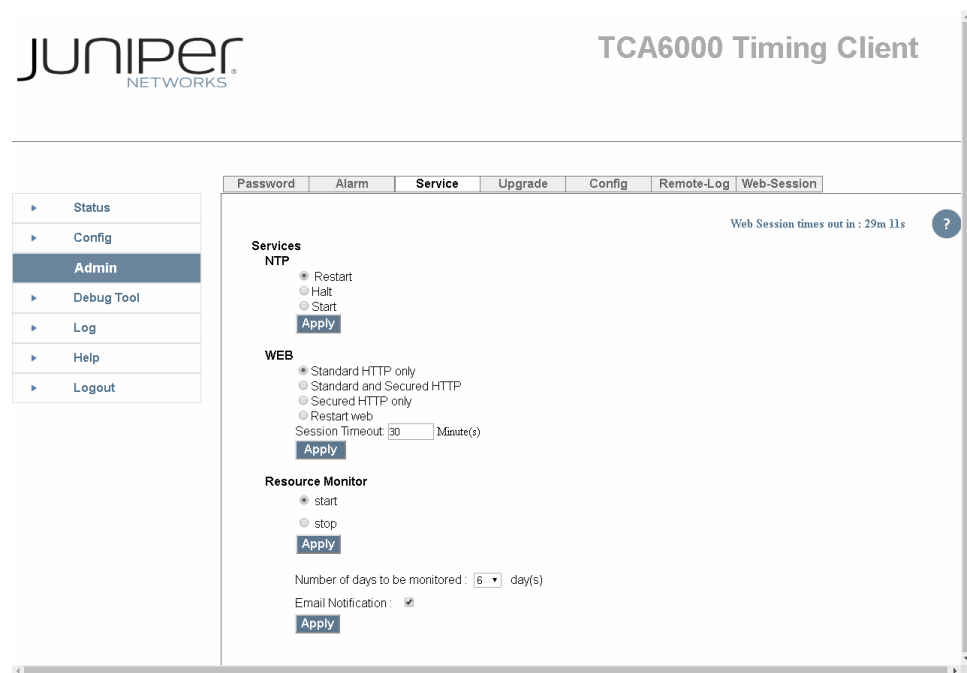


Table 27 on page 131 describes the elements that appear on the Admin page—Service pane of the TCA6000 and TCA6500 Timing Clients.

Table 27: Elements on the Timing Client Admin Page—Service Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
Services Section	Understand how to configure standard or secured HTTP, set the session timeout, and restart the PTP daemon.
PTP	<p>Enables you to manipulate the PTP daemon.</p> <ul style="list-style-type: none"> Restart—Restarts PTP operations. <p>NOTE: This field is available only if the PTP support is enabled in the Timing Client.</p>

Table 27: Elements on the Timing Client Admin Page—Service Pane (*continued*)

Element	Description
NTP	<p>Enables you to manipulate the NTP daemon.</p> <ul style="list-style-type: none"> Restart—Restarts NTP operations. This setting forcefully synchronizes its time from the configured NTP server. Start—Starts the operations of the NTP daemon. Stop—Stops the operations of the NTP daemon. <p>NOTE: This field is available only if the NTP support is enabled in the Timing Client.</p>
WEB Section	Allows to choose either standard or secure HTTP and manage the Web timeout.
Standard HTTP only	Allows to use only standard HTTP.
Standard and Secured HTTP	Allows to use either standard or secure HTTP.
Secured HTTP only	Allows to use only secure HTTP.
Restart web	Restarts the Timing Client GUI.
Session Timeout	Specifies the Web timeout period.
Resource Monitor Section	Allows you to configure notification medium, and start and stop the resource monitor.
Email Notification	Check this box for the resource monitor to send an e-mail message when alarm is raised for high CPU or RAM usage.
Start	Starts the resource monitor.
Number of Days to be Monitored	Allows you to specify the monitoring period to view the resource data.
Stop	Stops the resource monitor.
Apply button	Saves the changes.

The Admin Page—Upgrade Pane

Figure 53: Timing Client Admin Page—Upgrade Pane

The screenshot shows the Juniper TCA6000 Timing Client Admin Page. The 'Upgrade' tab is selected in the main content area. The sidebar on the left contains links for Status, Config, Admin (highlighted), Debug Tool, Log, Help, and Logout. The main content area has tabs for Password, Alarm, Service, Upgrade, Config, Remote-Log, and Web-Session. The Upgrade section includes radio buttons for TFTP, FTP, and SCP. Below these are input fields for Server, File Name, Username, and Password, followed by an 'Apply' button. The 'Halt and Reboot System' section has radio buttons for Halt and Reboot, and a dropdown menu for Software Image showing 'TCA6K-3.9.0_RC10-PTPNT-P1(Active)', with another 'Apply' button below it. A status bar at the top right indicates 'Web Session times out in : 23m 32s'.

Table 28 on page 133 describes the elements that appear on the Admin page—Upgrade pane of the TCA6000 and TCA6500 Timing Clients.

Table 28: Elements on the Timing Client Admin Page—Upgrade Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
Upgrade Section	This section allows you to set the details for downloading the software upgrade or downgrade image to the inactive flash partition.
TFTP	Select to download the upgrade or downgrade image from the TFTP server.
FTP	Select to download the upgrade or downgrade image from the FTP server.
SCP	Select to download the upgrade or downgrade image from the SCP server.
server	Enter the IP address of the server in which the image is located.
file name	For TFTP and FTP servers, enter the filename of the image. For SCP server, enter the filename of the image along with the full path where the file is located.
user name	Enter the username for accessing the server. NOTE: This field is applicable only for the SCP and FTP server.

Table 28: Elements on the Timing Client Admin Page—Upgrade Pane (*continued*)

Element	Description
password	Enter the corresponding password of the provided server username. <i>NOTE:</i> This field is applicable only for the SCP and FTP server.
Apply button	Click to download the image to the inactive flash partition.
Halt and Reboot System Section	This section allows you to halt and reboot the Timing Client.
Halt	Select to halt the current operation of the Timing Client.
Reboot	Select to reboot the Timing Client. The pull-down menu below the option buttons displays the current software image that's active. User can also use the pull-down menu to select a different image. This new image will take effect after the system finishes rebooting.
Apply button	Click to execute the corresponding operation.

The Admin Page—Config Pane

Figure 54: Timing Client Admin Page—Config Pane

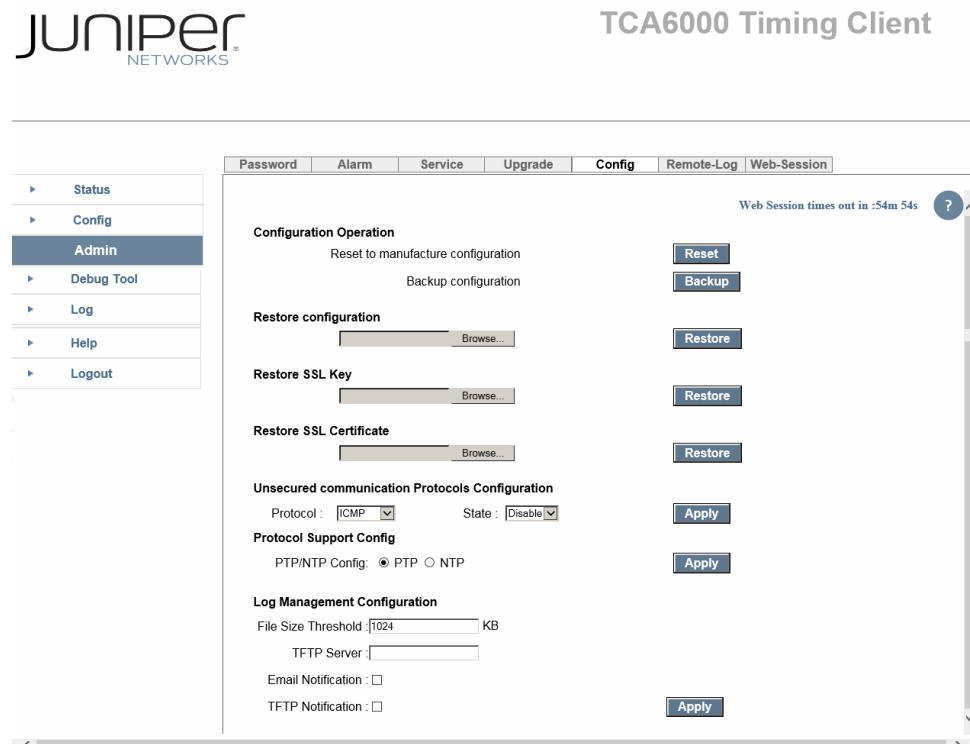


Table 29 on page 135 describes the elements that appear on the Admin page—Config pane of the TCA6000 and TCA6500 Timing Clients.

Table 29: Elements on the Timing Client Admin Page—Config Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
Configuration Operation Section	<p>Enables the backup and restore of the configuration.</p> <ul style="list-style-type: none"> Reset to manufacture configuration—Reset the current parameters to the default configuration. Backup configuration—Backup the most recent configuration to a file. Reset button—Resets the parameters to their default configuration. Backup button—Backs up the most recent configuration to a file.
Restore SSL Key	<p>Allows you to download a customized key file of .pem format. The file is downloaded locally without using any protocol. For more information about the dynamic SSL certificate support, see “Dynamic SSL Certificate Overview” on page 21.</p> <ul style="list-style-type: none"> Choose File button—Click to locate the customized key file. Restore button—Click to download the customized key file.
Restore SSL Certificate	<p>Allows you to download a customized certificate file of .pem format. The file is downloaded locally without using any protocol. For more information about the dynamic SSL certificate support, see “Dynamic SSL Certificate Overview” on page 21.</p> <ul style="list-style-type: none"> Choose File button—Click to locate the customized certificate file. Restore button—Click to download the customized certificate file.
Unsecured communication Protocols Configuration Section	This section allows you to configure unsecured transfer or communication protocols.
Protocol	<p>Allows you to select the unsecured transfer or communication protocol to be enabled or disabled. The available options are:</p> <ul style="list-style-type: none"> ICMP TFTP FTP TELNET ALL
State	<p>Allows you to enable or disable the unsecured transfer or communication protocols. The available options are:</p> <ul style="list-style-type: none"> Enable—Enables the selected unsecured transfer or communication protocol. Disable—Disables the selected unsecured transfer or communication protocol. <p>By default, all the unsecured transfer or communication protocols (ICMP, TFTP, FTP, and Telnet protocol) are enabled.</p>
Protocol Support Config	This section allows you to enable the PTP or NTP protocol support.

Table 29: Elements on the Timing Client Admin Page—Config Pane (*continued*)

Element	Description
PTP/NTP Config	<p>Select an option button to enable the corresponding protocol support in the Timing Client.</p> <ul style="list-style-type: none"> • PTP—Enables the PTP support. • NTP—Enables the NTP support. <p>NOTE: When you enable the PTP support, the NTP related commands and pages are unavailable, or vice versa.</p>
Apply button	<p>Click to reboot the Timing Client with the selected protocol support after your confirmation.</p> <p>NOTE: If you reject the rebooting of the Timing Client, the protocol change is not saved and the Timing Client continues to use the current protocol.</p>
Log Management Configuration Section	This section allows you to configure file size threshold, E-mail address and TFTP server.
File Size Threshold	Allows you to configure file size threshold for the log files stored in system. The threshold value ranges from 100 through 1024 kilobytes.
TFTP Server	<p>Allows you to configure a TFTP server. When the log file size exceeds the configured threshold, the log file is sent to the configured TFTP server.</p> <p>NOTE: Verify the SMTP Server configuration before configuring the TFTP server.</p>
Email Notification	Enables sending the log file to the configured mail server when the log file size exceeds the configured threshold.
TFTP Notification	Enables sending the log file to the configured TFTP server when the log file size exceeds the configured threshold.
Apply button	Click to apply the configuration changes done.

The Admin Page—Remote Log Pane

Figure 55: Timing Client Admin Page—Remote Log Pane

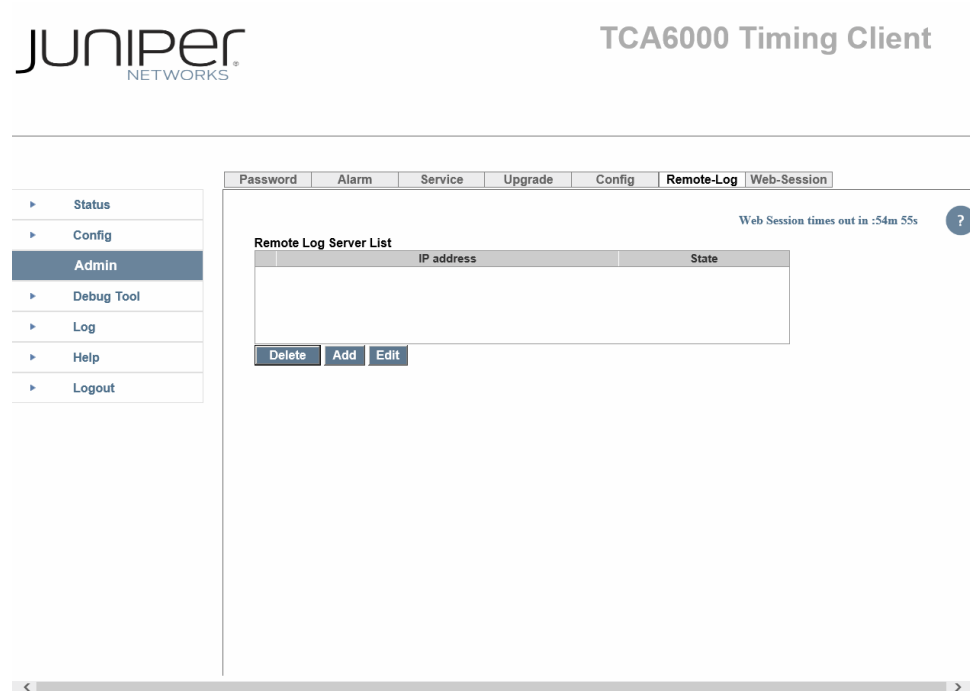


Table 30 on page 137 describes the elements that appear on the Admin page—Remote Log pane of the TCA6000 and TCA6500 Timing Clients.

Table 30: Elements on the Timing Client Admin Page—Remote Log Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
Remote Log Server List	<p>This window displays the remote log server list.</p> <ul style="list-style-type: none"> • Ip Address—Displays the IP address of remote log server. • State—Displays the ON or OFF state of remote log server. • Delete—Deletes the remote log server. • Add—Adds a new remote log server. • Edit—Modifies the remote log server. • Save—Saves the changes. <p>NOTE: You can configure only a maximum of 10 remote servers.</p>

The Admin Page—Web-Session Pane

Figure 56: Timing Client Admin Page—Web-Session Pane

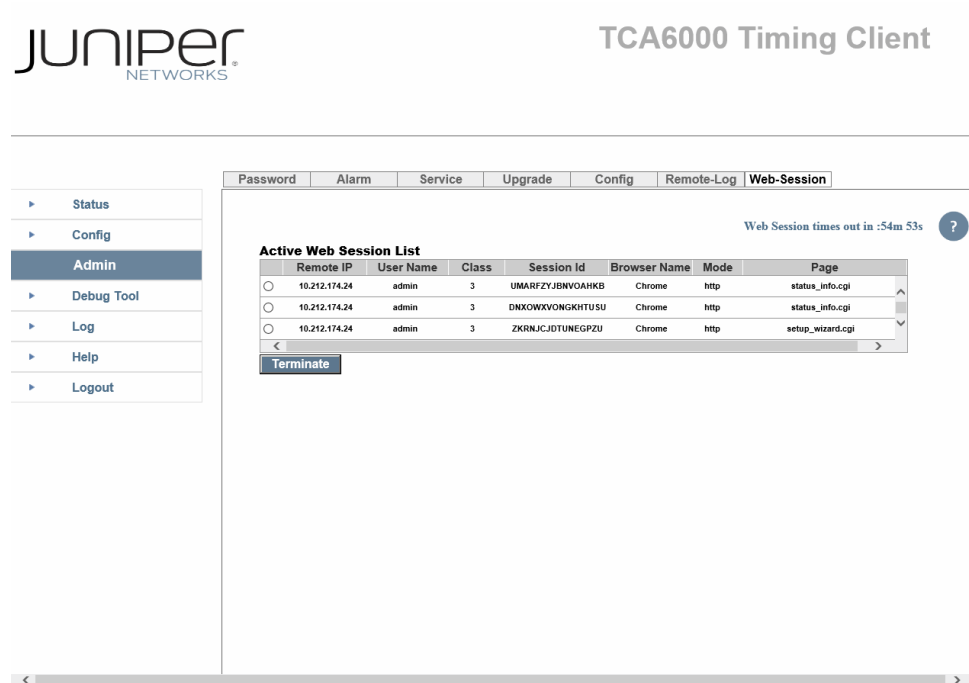


Table 31 on page 138 describes the elements that appear on the Admin page—Web-Session pane of the TCA8000 and TCA8500 Timing Clients.

Table 31: Elements on the Timing Client Admin Page—Web-Session Pane

Element	Description
Web Session times out in:	Displays the remaining time for the session to time out.
Remote IP	Displays the IP address on which the browser is hosted.
User Name	Displays the name specified by the user.
Class	Displays the access level.
Session id	Displays the session ID of the GUI terminal.
Browser Name	Displays the name of the browser.
Mode	Displays the mode (HTTP or HTTPS).
Page	Displays the name of the Web page.
Terminate	Terminates the session.

CHAPTER 9

Understanding the TCA6000 and TCA6500 Debug Tool Page

This chapter describes the Debug Tool page of the Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are addressed:

- [Debug Tool Page Description on page 139](#)
- [Accessing the Debug Tool Page on page 139](#)
- [Understanding the Debug Tool Page on page 139](#)

Debug Tool Page Description

The Debug Tool page provides the information that can be used for debugging purposes.

Accessing the Debug Tool Page

To access the Debug Tool page of a TCA6000 or TCA6500 Timing Client:

1. Log in to the Timing Client.
2. Click the **Debug Tool** tab. The Debug Tool page appears.



NOTE: After the Debug Tool page opens, click the Refresh button in the browser to update the page.

Understanding the Debug Tool Page

- [The Debug Tool Page—Processes Pane on page 140](#)
- [The Debug Tool Page—Kernel Logs Pane on page 141](#)
- [The Debug Tool Page—Registers Pane on page 141](#)

The Debug Tool Page—Processes Pane

Figure 57: Timing Client Debug Tool Page—Processes Pane

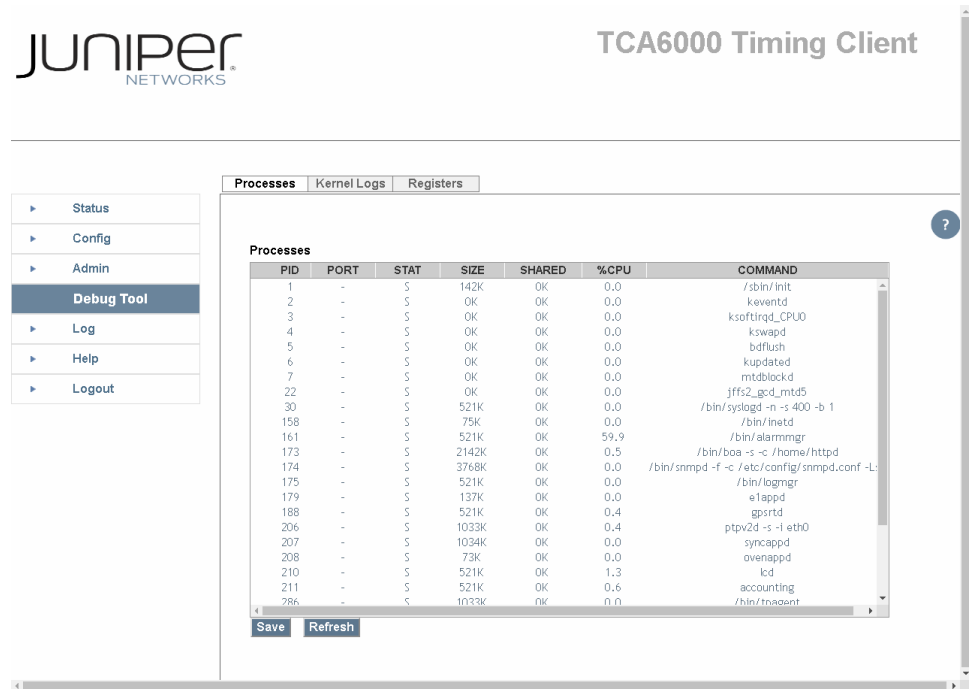


Table 32 on page 140 describes the elements that appear on the Debug Tool page—Processes pane of the TCA6000 and TCA6500 Timing Clients.

Table 32: Elements on the Timing Client Debug Tool Page—Processes Pane

Element	Description
Processes Section	Displays running processes reported to the Timing Client.
PID	Indicates the process ID number.
Port	Indicates the port associated with the process.
Stat	Indicates the process status code.
Size	Indicates the memory size in kilobytes used by the current process.
Shared	Indicates the amount of shared pages
%CPU	Indicates the percentage of CPU process usage.
Command	Indicates the name of the process and includes arguments (if any).
Save	Saves the running processes log to a file.

Table 32: Elements on the Timing Client Debug Tool Page—Processes Pane (*continued*)

Element	Description
Refresh	Refreshes the running processes page.

The Debug Tool Page—Kernel Logs Pane

Figure 58: Timing Client Debug Tool Page—Kernel Logs Pane

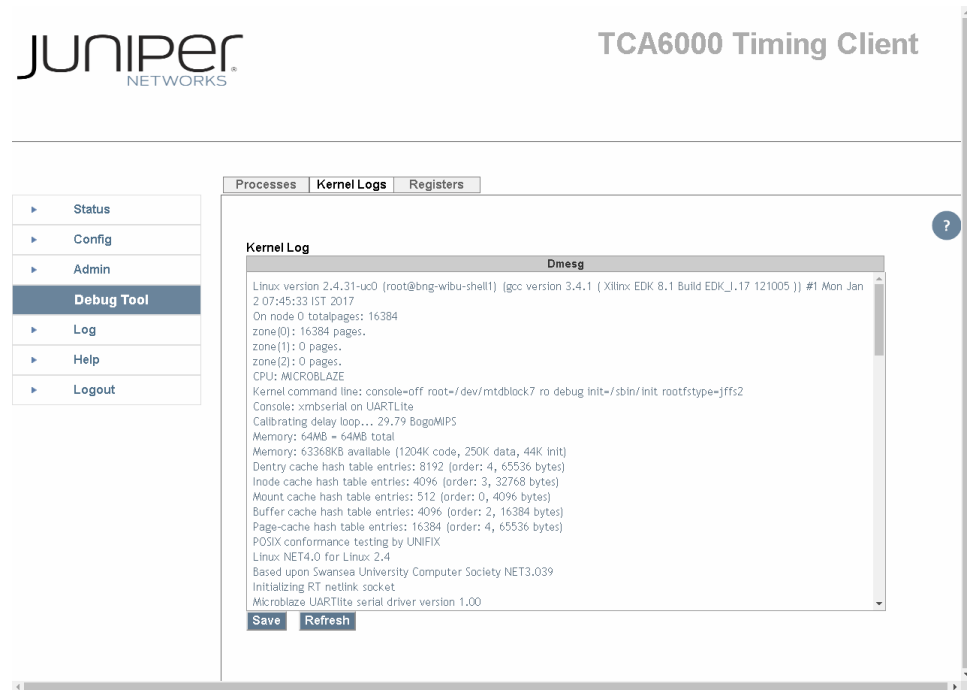


Table 33 on page 141 describes the elements that appear on the Debug Tool page—Kernel Logs pane of the TCA6000 and TCA6500 Timing Clients.

Table 33: Elements on the Timing Client Debug Tool Page—Kernel Logs Pane

Element	Description
Kernel Log	<p>This window displays kernel logs information.</p> <ul style="list-style-type: none"> Dmesg—Displays the debug messages received. Save—Saves the kernel logs to a file. Refresh—Refreshes the log page.

The Debug Tool Page—Registers Pane



NOTE: The Registers pane is visible only to the Admin user.

Figure 59: Timing Client Debug Tool Page—Registers Pane

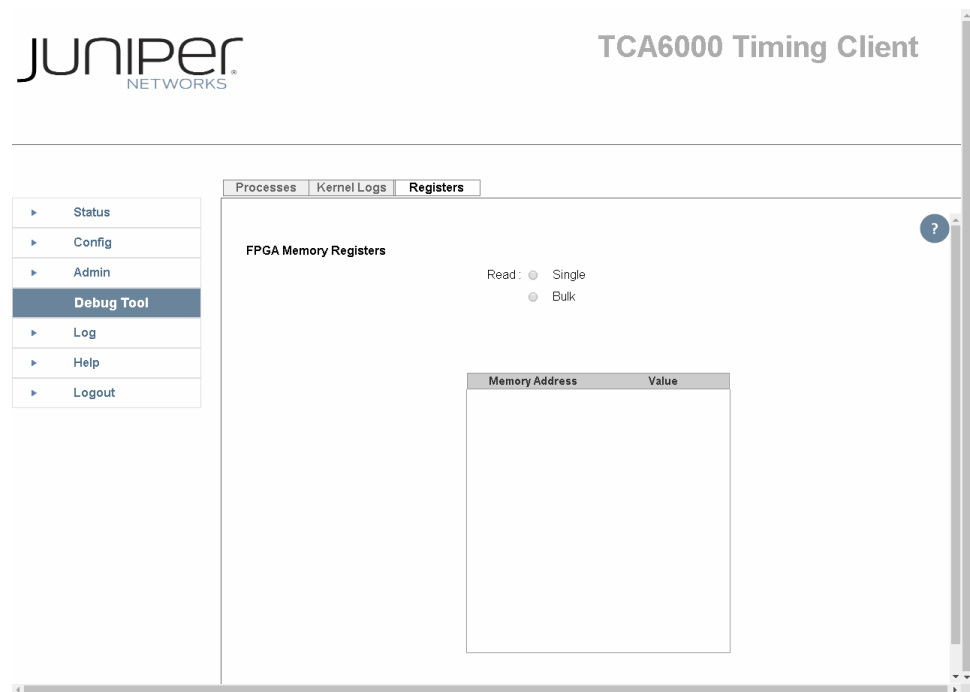


Table 34 on page 142 describes the elements that appear on the Debug Tool page—Registers pane of the TCA6000 and TCA6500 Timing Clients.

Table 34: Elements on the Timing Client Debug Tool Page—Registers Pane

Element	Description
FPGA Memory Registers	<p>This window displays FPGA registers.</p> <ul style="list-style-type: none"> Single Read—Displays a single value. Bulk Read—Displays bulk values. Show—Displays values in memory value table. Memory Address—Displays the FPGA memory address. Value—Displays the hexadecimal memory address value.

CHAPTER 10

Understanding the TCA6000 and TCA6500 Log Page

This chapter describes the Log page of the Juniper Networks TCA6000 and TCA6500 Timing Clients. The following topics are addressed:

- [Log Page Description on page 143](#)
- [Accessing the Log Page on page 143](#)
- [Understanding the Log Page on page 143](#)

Log Page Description

The Log page provides data which is reported by the Timing Client during operation.



NOTE: The **Clear** button appears dimmed for the Read-Only and Read/Write users, so they cannot clear the displayed log messages.

Accessing the Log Page

To access the Log page of a TCA6000 or TCA6500 Timing Client:

1. Log in to the Timing Client.
2. Click the **Log** section to the left of the page. The Event Log pane appears at the top. See [Figure 60 on page 144](#).



NOTE: After the Log page launches, click the Refresh button in the browser to update the page.

Understanding the Log Page

- [The Log Page—EventLog Pane on page 144](#)
- [The Log Page—SysLog Pane on page 145](#)

- The Log Page—AuthLog Pane on page 146
- The Log Page—Daemon Pane on page 147

The Log Page—EventLog Pane

Figure 60: Timing Client Log Page—EventLog Pane

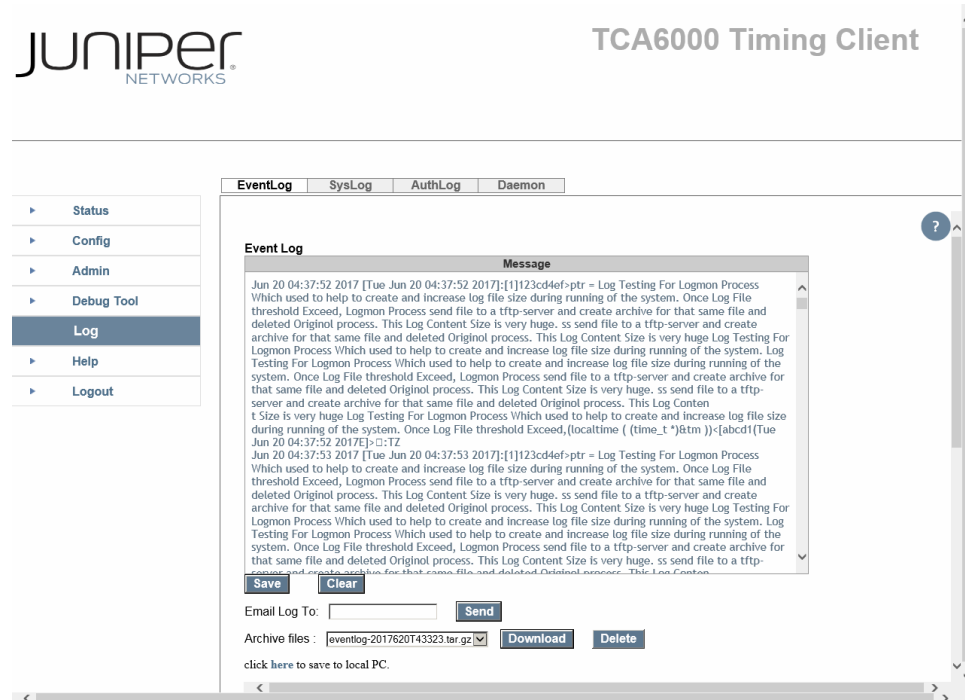


Table 35 on page 144 describes the elements that appear on the Log page—EventLog pane of the TCA6000 and TCA6500 Timing Clients.

Table 35: Elements on the Timing Client Log Page—EventLog Pane

Element	Description
EventLog	<p>This window displays event messages reported to the Timing Client. This log is used to provide operational alarm and status of the Timing Client.</p> <ul style="list-style-type: none"> • Message—Lists the event messages received. • Save as—Save the event log to a file. • Clear—Clears the log page.
Email Log To	Enter the e-mail address to send the logs.
Send	Click to send the event logs to the provided e-mail address.
Archive files	Lists the event log archive files.
Download	Click to download the selected event log archive file to system.
	<p>NOTE: When you click on Download, the following link is displayed: click here to save to local PC.</p>

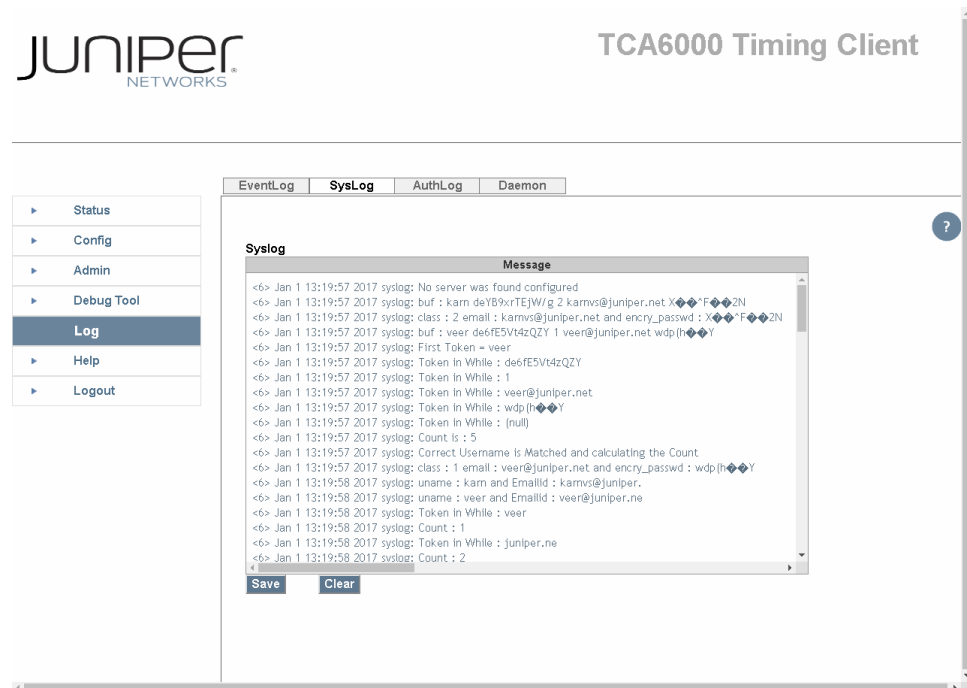
Table 35: Elements on the Timing Client Log Page—EventLog Pane (*continued*)

Element	Description
Delete	Click to delete the selected event log archive file from system.

The Log Page—SysLog Pane

The Syslog displays internal system level messages which indicate the operational state and status of the Timing Server software applications. Any error event that impacts the operational state of the system is reflected with the appropriate alarm event in the EventLog. For details, see [“The Log Page—EventLog Pane” on page 144](#).

Figure 61: Timing Client Log Page—SysLog Pane



[Table 36 on page 145](#) describes the elements that appear on the Log page—SysLog pane of the TCA6000 and TCA6500 Timing Clients.

Table 36: Elements on the Timing Client Log Page—SysLog Pane

Element	Description
SysLog	<p>This window displays system messages reported to the Timing Client.</p> <ul style="list-style-type: none"> • Message—Lists the system messages received. • Save as—Save the syslog to a file. • Clear—Clears the log page.

The Log Page—AuthLog Pane

The AuthLog pane provides a history of login events.

Figure 62: Timing Client Log Page—AuthLog Pane

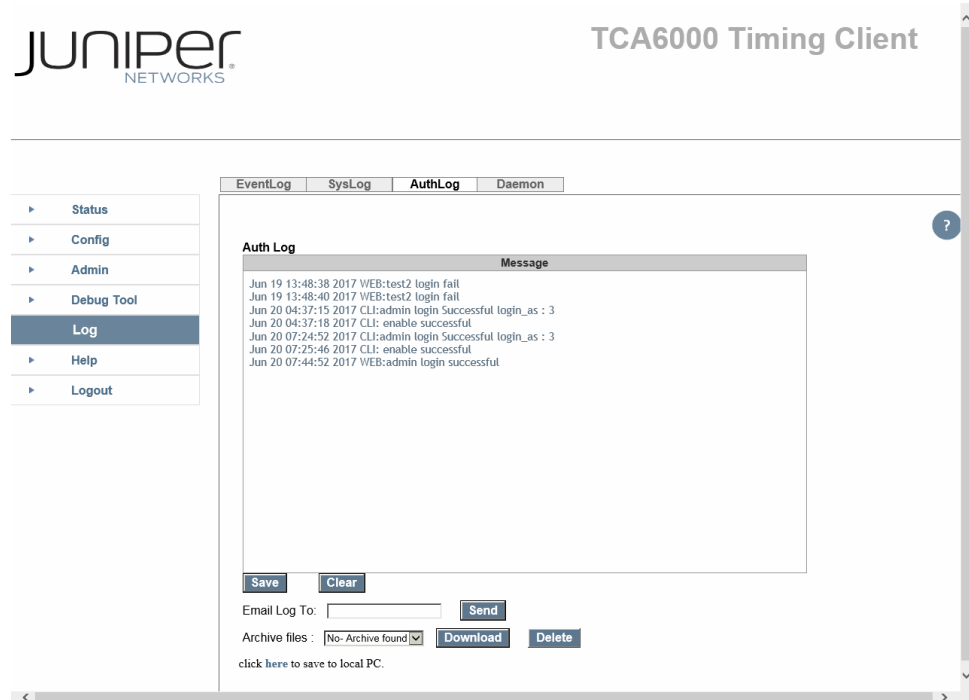


Table 37 on page 146 describes the elements that appear on the Log page—AuthLog pane of the TCA6000 and TCA6500 Timing Clients.

Table 37: Elements on the Timing Client Log Page—AuthLog Pane

Element	Description
AuthLog	<p>This window displays authentication messages reported to the Timing Client.</p> <ul style="list-style-type: none"> • Message—Lists the authentication messages received. • Save as—Save the auth.log to a file. • Clear—Clears the log page.
Email Log To	Enter the e-mail address to send the logs.
Send	Click to send the auth logs to the provided e-mail address.
Archive files	Lists the auth log archive files.
Download	Click to download the selected auth log archive file to system.
<p>NOTE: When you click on Download, the following link is displayed: click here to save to local PC.</p>	

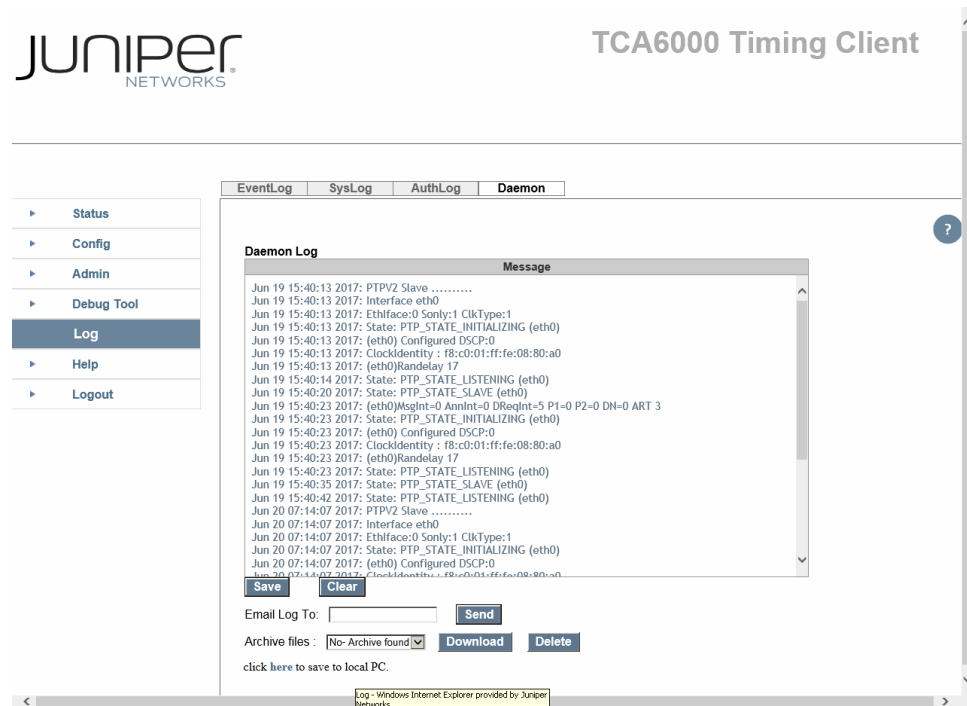
Table 37: Elements on the Timing Client Log Page—AuthLog Pane (*continued*)

Element	Description
Delete	Click to delete the selected auth log archive file from system.

The Log Page—Daemon Pane

The Daemon log displays the internal operating PTP level messages which indicate the operational state and status of the PTP protocol. Any error event that impacts the operational state of the system is reflected with the appropriate alarm event in the EventLog. For details, see “[The Log Page—EventLog Pane](#)” on page 144.

Figure 63: Timing Client Log Page—Daemon Pane



[Table 38 on page 147](#) describes the elements that appear on the Log page—Daemon pane of the TCA6000 and TCA6500 Timing Clients.

Table 38: Elements on the Timing Client Log Page—Daemon Pane

Element	Description
Daemon.log	<p>This window displays daemon messages reported to the Timing Client.</p> <ul style="list-style-type: none"> • Message—Lists the daemon messages received. • Save as—Save the daemon.log to a file. • Clear—Clears the log page.
Email Log To	Enter the e-mail address to send the logs.

Table 38: Elements on the Timing Client Log Page—Daemon Pane (*continued*)

Element	Description
Send	Click to send the daemon logs to the provided e-mail address.
Archive files	Lists the daemon log archive files.
Download	Click to download the selected daemon log archive file to system. NOTE: When you click on Download , the following link is displayed: click here to save to local PC.
Delete	Click to delete the selected daemon log archive file from system.

PART 5

Troubleshooting a TCA6000 or TCA6500 Timing Client

- [Troubleshooting a TCA6000 or TCA6500 Timing Client on page 151](#)

CHAPTER 11

Troubleshooting a TCA6000 or TCA6500 Timing Client

If you need post sales technical support, it is available through the Juniper Networks Technical Assistance Center (JTAC). For information about contacting JTAC, see “[Warranty and Support](#)” on page 211.

- [Event States and Alarm Types](#) on page 151
- [Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log](#) on page 152

Event States and Alarm Types

[Table 39 on page 151](#) shows alarms and their corresponding states.

Table 39: Event States

Alarm Condition	State
NONE	Indicates event as NONE in the Severity alarm profile.
Critical	Indicates event as Critical in the Severity alarm profile.
Major	Indicates event as Major in the Severity alarm profile.
Minor	Indicates event as Minor in the Severity alarm profile.
Clear	Indicates event alarm condition is no longer active.

[Table 40 on page 151](#) shows alarms and their corresponding types.

Table 40: Alarm Types

Alarm	Details
Transient	Outstanding alarms are used for those time persistent condition. System will automatically raise and clear these type of alarm based on the state of the condition.

Table 40: Alarm Types (*continued*)

Alarm	Details
Static	System will raise this alarm whenever the condition occurs and hold the alarm, it require user acknowledgement and manually cleared by the administrator or by the auto clear expiration timer.

Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log

Use [Table 41 on page 152](#) to identify which actions to perform when an event is reported in the event log.

Table 41: Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log

Event	Type	Description	Action
SYS_CONFIG_CHANGE	Static	One or more parameters were changed in the Config menu.	Verify changes were as expected.
SYS_AUTHENTICATION	Static	The was a failed Login / Password attempt in the unit.	Verify Login name and Password.
GPS_ANTENNA_SHORT	Transient	Antenna connection is shorted between the Cable Conductor Pin and Shield.	For TCA6500 only, check for a cable short on the center and ground shield.
GPS_ANTENNA_OPEN	Transient	Cable Connection has an open in it.	For TCA6500 only, check for a cable open on the center and ground shield.
GPS_NO_USABLE_SATELLITE	Transient	The antenna is unable to acquire any satellites with sufficient signal levels.	For TCA6500 only: <ol style="list-style-type: none"> 1. Assure the antenna has a clear view of the sky is not obstructed. For a roof antenna, find location that provides full 360-degree visibility of the horizon. 2. Validate that there is no source of high frequency interference near the antenna. Set the height of the antenna to be at least three to six feet (1-2 m) from a reflecting surface.
GPS_LEAP_SECOND_PENDING	Transient	GPS notifies of this event approximately 3 months before event.	For TCA6500 only: <ol style="list-style-type: none"> 1. This is a normal GPS operation which if occurs will happen either in June 30 or Dec. 31. 2. Verify event is cleared July 1 and Jan. 1, if does not clear reset unit.

Table 41: Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log (*continued*)

Event	Type	Description	Action
GPS_RECEIVER_INACTIVE	Transient	Internal communication to the GPS Receiver failed to respond.	For TCA6500 only: <ol style="list-style-type: none"> Potentially the CPU has lost communication with GPS Receiver. Reset unit and if it continues to occur RMA unit.
TIMING_OSC_DAC_RANGE	Transient	The Digital-to-Analog Converter (DAC) which controls the voltage adjustment for the Oscillator frequency has exceeded its range of control voltage.	Verify operational temperature is within specification of the unit.
OVEN_TEMP_DEVIATION_HIGH	Transient	Secondary oscillator Oven Temperature increase was faster than the internal oven control could compensate.	This is status only information as the internal oscillator oven temperature control will eventually compensate for this.
OVEN_TEMP_DEVIATION_LOW	Transient	Secondary oscillator Oven Temperature decrease was faster than the internal oven control could compensate.	This is status only information as the internal oscillator oven temperature control will eventually compensate for this.
SYS_DIAG_FAILURE	Transient	The boot-up System Diagnostics had one or more failures.	<ol style="list-style-type: none"> Turn power off and then back on. If unit continues to show failure, the unit is defective and RMA unit for repair or replacement.
PTP_SERVER_UNREACHABLE	Transient	There is no master PTP Grand Master available in the network for the configured domain number.	<ol style="list-style-type: none"> Check domain number should match with the Grand Master domain number. Check network for support of multicast packets. Verify Ethernet connection is functioning properly for unit.
PTP_SERVER_CHANGE	Static	A Best Master selection has occurred and the server was changed.	Verify the "other" master had an abnormal event that caused this event.

Table 41: Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log (*continued*)

Event	Type	Description	Action
LOSS_OF_POWER_FEED	Transient	One of the DC inputs has no voltage connected.	<ol style="list-style-type: none"> 1. Check cables. 2. If only one power feed being used disable alarm in Admin > Alarms and configure to "NONE".
FREQ_ACQUIRING	Transient	System tries to adjust the local oscillator based on the input source such as GPS, T1, E1, and PTP. If the adjustments are completed, then the system state is changed from acquiring state to locked state.	This is a positive indication of sync source availability.
FREQ_HOLDOVER	Transient	Local Oscillator is in Holdover state. There is no configured servers sync sources available. Only goes to this state after a sync source has been qualified for a period of time and than is not available.	Check sync source quality which was configured in the sync source table.
FREQ_FREERUN	Transient	Local Oscillator is in Freerun state. The unit has not obtained initial lock sync lock state and is operating on the local oscillator.	<ol style="list-style-type: none"> 1. Check sync source table is configured for at least one source available. If not locked with a period of time (ex. >2 hours) reboot system. 2. Verify the PTP verify PTP state is slave. 3. Verify network connections and activity. 4. This could be caused by unit not initially being locked for a period long enough to generate a holdover value. Verify the unit has been locked for 8 hours or more.
FREQ_REF_INPUT_CHANGE	Static	The reference input being used as a sync source has changed.	Verify one of the reference input such as GPS, external inputs has changed.
FREQ_INPUT_QUALITY_CHANGE	Static	The timing input quality has changed due to lower or higher quality level of the new sync source.	Verify the quality states changes were as expected.
LINK_DOWN	Static	Ethernet connection is not functional.	Verify Ethernet connection, cables, and so on.

Table 41: Troubleshooting the TCA6000 or TCA6500 Timing Client Using the Event Log (*continued*)

Event	Type	Description	Action
LINK_UP	Static	Ethernet connection is functional.	This is a positive indication of the Ethernet link status. To suppress go to Configure Admin > Alarm > Severity and set to NONE.
TIMEPROBE_DISABLE	Transient	The time probe agent is disabled or accidentally turned off.	Start or enable the time probe agent using the restart timeprobe-agent command.

PART 6

Appendixes

- [Using Telnet with the TCA6000 and TCA6500 Timing Clients on page 159](#)
- [Using the CLI to Configure PTP and Network Interface Parameters on page 181](#)
- [Using the CLI to Configure NTP Parameters on page 197](#)
- [Using the CLI to Configure User Authentication and RADIUS Accounting on page 201](#)
- [Specifications on page 205](#)
- [Agency Compliance on page 207](#)
- [Cable Specification on page 209](#)
- [Warranty and Support on page 211](#)

APPENDIX A

Using Telnet with the TCA6000 and TCA6500 Timing Clients

Use Telnet to access the Juniper Networks TCA6000 or TCA6500 Timing Client to configure and set operating parameters. This appendix addresses the following topics:

- [Accessing the Timing Client Using the CLI on page 159](#)
- [Changing the IP Address of the Timing Client using the CLI on page 160](#)
- [Resetting the Passwords of Both Admin User Account and Enable Mode to Factory Defaults on page 161](#)
- [Using the CLI to View Status and Configuration Parameters on page 162](#)
- [Using the CLI to Configure Timing Client Parameters on page 168](#)
- [Accessing the Timing Client Using SSH on page 180](#)

Accessing the Timing Client Using the CLI

To access a TCA6000 or TCA6500 Timing Client using the CLI:

1. On a computer which is on the same network segment as the Timing Client, click the **Start** button and choose **Run** from the menu. The Run dialog box appears.
2. In the **Open** field, enter the following:

telnet ip address



NOTE: If you are accessing the Timing Client for the first time, see [“Assigning an IP Address to the TCA6000 or TCA6500 Timing Client” on page 14](#) for information about connecting to the unit and accessing the user interface.

3. Click the **OK** button.
4. A DOS window appears.

5. At the User name prompt, type the username and press Enter.
6. At the Password prompt, type the corresponding password and press Enter.



NOTE: To see a list of the commands you can use, type **help**. Refer to [Table 42 on page 162](#) for a list of viewing options and [Table 43 on page 168](#) for a list of configurable elements.

Changing the IP Address of the Timing Client using the CLI

The Timing Client is assigned a default IP address by the manufacturer to allow access to the unit for the first time. The IP address should be changed prior to installing on a network. See “[Reserving an IP Address for the TCA6000 or TCA6500 Timing Client](#)” on [page 10](#) for additional information on how to reserve an IP address for the Timing Client. This section describes how to connect the Timing Client to a computer and how to use the CLI to change the IP address.

To use the CLI to change the default IP address of the Timing Client:

1. Using the computer which is connected to the Timing Client, click the **Start** button and choose **Run** from the menu. The Run dialog box appears.
2. In the **Open** field, enter the following:

`telnet 192.168.0.75`
3. Click the **OK** button.
4. A DOS window appears
5. At the User name prompt, type the username and press Enter.
6. At the Password prompt, type the corresponding password and press Enter.
7. At the prompt, type **enable** and press Enter.
8. At the password prompt, type **enable** and press Enter.
9. At the prompt, type **config eth0 ip** and press Enter.

10. At the IP address prompt, enter the IP address to be assigned to the unit and press Enter. The current IP address is shown in the brackets <>.
11. At the prompt, type **exit**, save your changes, and exit enable mode or type **help** to view additional commands.

Resetting the Passwords of Both Admin User Account and Enable Mode to Factory Defaults

You can reset passwords of the Admin user account and the enable mode to factory defaults through the CLI, GUI, or by resetting the Timing Client. For more information about resetting passwords through GUI, see [“Changing/Resetting the Login Password for Admin User” on page 26](#).



NOTE: Only the Admin user can reset passwords through the CLI command.

To reset passwords through CLI:

1. Login as **admin**.
 - a. **>admin<cr>**
 - b. **>password: admin123<cr>**
2. Enable privileged commands.
 - a. **>enable<cr>**
 - b. **>password: enable123<cr>**
3. Execute the following command to reset Admin user and enable mode passwords:
reset password

You can reset passwords of the Admin user and the enable mode without logging in to the Timing Client by resetting the Timing Client.



NOTE:

- When you reset the Timing Client, only passwords of the Admin user and the enable mode are reset whereas the existing configurations are retained.
- We recommend that you reset passwords by resetting the Timing Client only when you forget Admin user account password.

To reset the Timing Client:

1. Press the pin-hole reset pin.



NOTE: The pin-hole reset pin is available on the left side of the craft port placed in the front panel of the Timing Client.

2. Power off the Timing Client.
3. Power on the Timing Client.

Using the CLI to View Status and Configuration Parameters

The CLI can be used to view the status of Timing Client operations and to view current parameter settings. This section describes the options that are available for viewing and how to view them.

- [Options That You Can View in the CLI on page 162](#)
- [Viewing an Option in the CLI on page 168](#)

Options That You Can View in the CLI

To list the options that can be viewed, type help after the CLI session has started. [Table 42 on page 162](#) lists the options that can be viewed.

Table 42: CLI Viewing Options

Command	Description	Supported Users
enable	Turns on privileged commands	<ul style="list-style-type: none">• Admin• Read/Write
exit	Exits from current mode	<ul style="list-style-type: none">• Admin• Read/Write• Read-Only
help	Displays available list of commands	<ul style="list-style-type: none">• Admin• Read/Write• Read-Only
history	Displays a list of previously run commands	<ul style="list-style-type: none">• Admin• Read/Write• Read-Only
logout	Disconnect	<ul style="list-style-type: none">• Admin• Read/Write• Read-Only

Table 42: CLI Viewing Options (*continued*)

Command	Description	Supported Users
no show ntp-packet	Stops displaying the NTP packets.	<ul style="list-style-type: none"> • Admin • Read/Write
no show ntp-sync-status	Stops displaying the NTP synchronization status.	<ul style="list-style-type: none"> • Admin • Read/Write
quit	Disconnect	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show 1/5/10MHz	Displays 1/5/10 MHz settings	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show accounting-level	Displays the type of information to be accounted	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show accounting-server	Displays the details of the configured RADIUS accounting servers	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show accounting-status	Displays the current status of RADIUS accounting	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show active sessions	Displays all active sessions	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show alarm all	Displays all active alarms	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show alarm-email-receiver	Displays alarm's e-mail receivers	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show alarm-profile	Displays alarm's profile information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show alarm t1	Displays only T1 active alarms	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only

Table 42: CLI Viewing Options (*continued*)

Command	Description	Supported Users
show all-configuration	Displays the current configurations of the TCA system NOTE: Only the configurations available in the config.dat file are displayed with appropriate fields.	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show auth-order	Displays the configured authentication order	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show authlog	Displays authorization log {num of lines}	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show cli-banner	Displays the customized CLI banner	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show daemonlog	Displays daemon log {num of lines}	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show dst-config	Displays the configured offset, starting date and time, and ending date and time for DST	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show eventlog	Displays event log {num of lines}	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show frequency	Displays frequency status	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show gps	Displays GPS software and hardware status	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show holdover-state	Indicates whether the TCA system remains in the holdover state or changes to the internal state after 24 hours of holdover state	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show interface-stat	Displays network interface statistics	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only

Table 42: CLI Viewing Options (*continued*)

Command	Description	Supported Users
show logger-threshold	Displays configured file threshold value	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show log-monitor-config	Displays the configured notification mediums	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show memory-cpu utilization	Displays memory and CPU utilization for last 10 days	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show network	Displays network information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ntp config	Displays the details of the configured NTP association entries.	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ntp packet all	Displays all the NTP packets.	<ul style="list-style-type: none"> • Admin • Read/Write
show ntp sync-status all	Displays synchronization status of all the NTP packets.	<ul style="list-style-type: none"> • Admin • Read/Write
show ntp status	Displays the status of the configured NTP association entries.	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show partition	Displays partition information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show physical-memory	Displays physical memory details	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show pps-squelch	Displays the status of the PPS squelch	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ppx	Displays PPS settings	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only

Table 42: CLI Viewing Options (*continued*)

Command	Description	Supported Users
show ptp config	Displays PTP configuration	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ptp default-dataset	Displays the PTP parameter including domain number that is configured	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ptp parent-dataset	Displays Grandmaster priority settings and other Grandmaster parameters	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ptp stat	Displays PTP statistics	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show ptp status	Displays PTP status	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show radius-server	Displays the details of the configured RADIUS authentication servers	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show resource-monitor-config	Displays the configures resource monitoring period	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show session	Displays session information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show snmp	Displays SNMP configuration information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show snmp-trap	Displays information about trap receivers	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show snmp-v3 user	Displays SNMPv3 user information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show sync-src-priority	Displays time status	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only

Table 42: CLI Viewing Options (*continued*)

Command	Description	Supported Users
show sysinfo	Displays system information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show syslog	Displays system log {num of lines}	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show t1 config	Displays T1 port configuration	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show t1 status	Displays T1 status	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show tftp-server address	Displays configured TFTP server	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show time	Displays time status	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show time-probe	Displays status of licensable features such as time probe agent	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show timing-output	Displays timing output information	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show unsecured-communication-protocols-status	Displays the status of unsecured transfer or communication protocols such as ICMP, TFTP, FTP, and Telnet protocol.	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show user-history	Displays command history for users. NOTE: The Read-Only or Read/Write users can use this command to view only command history of their sessions. The Admin user can use this command to view command history of all users.	<ul style="list-style-type: none"> • Admin • Read/Write • Read-Only
show users	Displays details (username, class and email-id) of Read-Only and Read/Write users.	Admin

Viewing an Option in the CLI

To look at an option in the CLI:

1. Launch a Telnet session.
2. At the prompt, type **show option** and then press Enter. (Where *option* is the option that you want to view.) Information for the option is displayed.

Using the CLI to Configure Timing Client Parameters

The CLI can be used to configure the Timing Client. This section identifies and describes the element that can be configured using the CLI and describes how to configure parameters using Telnet.

- [Elements that You Can Configure in the CLI on page 168](#)
- [Using the CLI to Configure the Timing Client on page 179](#)

Elements that You Can Configure in the CLI

To list the elements that you can configure using the CLI, type **enable** at the prompt and press Enter. [Table 43 on page 168](#) list the configurable elements that appear.

Table 43: Configurable Elements in the CLI

Command	Description	Supported Users
backup tftp	Backs up the configuration file to a TFTP server.	Admin
backup scp	Backs up the configuration file (config.dat) in the specified path of the SCP server. NOTE: <ul style="list-style-type: none"> • The file path and username should not contain any space characters. • The maximum length of the CLI command should not exceed 124 characters. 	Admin
clear alarm	Clears the alarm.	<ul style="list-style-type: none"> • Admin • Read/Write
clear archive authlog	Deletes the specified authorization log archive files.	<ul style="list-style-type: none"> • Admin • Read/Write
clear archive daemonlog	Deletes the specified daemon log archive files.	<ul style="list-style-type: none"> • Admin • Read/Write
clear archive eventlog	Deletes the specified event log archive files.	<ul style="list-style-type: none"> • Admin • Read/Write
clear authlog	Clears authorization log.	Admin

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
clear daemon log	Clears daemon log.	Admin
clear eventlog	Clears event log.	Admin
clear ptp-stat	Clears the PTP statistics.	<ul style="list-style-type: none"> • Admin • Read/Write
clear syslog	Clears system log.	Admin
config 1/5/10MHz	Selects between 1 MHz, 5 MHz, and 10 MHz output on the 1/5/10 MHz port.	<ul style="list-style-type: none"> • Admin • Read/Write
config accounting	Enables or disables RADIUS accounting in the Timing Client.	<ul style="list-style-type: none"> • Admin • Read/Write
config accounting-level	<p>Configures the information to be used by the Timing Client for accounting. The values are:</p> <ul style="list-style-type: none"> • 1—For login accounting only • 2—For interactive and login accounting • 3—For configuration, interactive and login accounting 	<ul style="list-style-type: none"> • Admin • Read/Write
config accounting-server add	Adds the IP address of the RADIUS accounting server and sets other related configurations (secret word, retries, timeout, and port) to be used by the Timing Client for accounting.	<ul style="list-style-type: none"> • Admin • Read/Write
config accounting-server del	Deletes the RADIUS accounting server and its configuration from the accounting server list by using the IP address of the accounting server.	<ul style="list-style-type: none"> • Admin • Read/Write
config active-session terminate <i>session-id</i>	Terminates the active session.	<ul style="list-style-type: none"> • Admin
config alarm-email-receiver	Configures recipients of alarm e-mail notifications.	<ul style="list-style-type: none"> • Admin • Read/Write
config alarm-profile	Configures the alarm profile.	Admin
config antenna-cable-delay-compensation	<p>Configures a delay compensation value in the range of -10000 through 10000 nanoseconds to compensate antenna cable delay.</p> <p>NOTE: You are advised to enter:</p> <ul style="list-style-type: none"> • A negative delay compensation value to compensate the positive delay introduced by the cable. • A positive delay compensation value to advance the PPS output delay relative to the absolute value. 	<ul style="list-style-type: none"> • Admin • Read/Write

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config antenna-voltage	Configures the input voltage for the antenna as 3.3V or 5V.	<ul style="list-style-type: none"> Admin Read/Write
config auth-order	<p>Configures the authentication order to be followed by the Timing Client while authenticating an user. The following combination of authentication order is allowed:</p> <ul style="list-style-type: none"> RADIUS server authentication and then local authentication Local authentication and then RADIUS server authentication Only RADIUS server authentication Only local authentication 	<ul style="list-style-type: none"> Admin Read/Write
config change-password	Modifies your current login password.	Read/Write
config cli-banner-file	<p>Downloads the specified text file from the mentioned path of the configured Secure Copy Protocol (SCP) server to the /etc/config/cli_banner.txt path for customizing the CLI banner.</p> <p>The downloaded file should be a plain text file. On rebooting, the TCA system checks for the cli_banner.txt file and displays the content in the file as CLI banner.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The file cannot be downloaded from TFTP and FTP servers. The TCA system supports only 1024 characters (including spaces and new line characters) for the downloaded file, so the TCA system would truncate any extra characters in the file. The TCA system detects all special characters in the downloaded file as normal strings. The TCA system displays the default hard coded CLI banner, if no customized CLI banner is configured. The TCA system displays an empty banner, if the cli_banner.txt file is empty. 	Admin

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config cli-banner-text	<p>Configures a customized CLI banner. The CLI banner text that you have provided in this command is stored in the cli_banner.txt file in the /etc/config path. On rebooting, the TCA system checks for the cli_banner.txt file and displays the content in the file as CLI banner.</p> <p>The maximum length of the CLI banner text that you can enter in this command is 100 characters, which include spaces and special characters. You can also use special characters (such as \n, \v, \t, and so on) to format the CLI banner text provided in this command.</p> <p>NOTE:</p> <ul style="list-style-type: none"> If the cli_banner.txt file is available and already contains any content, then the existing content is replaced with the provided content. You should avoid using the following special characters in the CLI banner text: , ", and '. The TCA system displays the default hard coded CLI banner, if no customized CLI banner is configured. The TCA system displays an empty banner, if the cli_banner.txt file is empty. 	Admin
config cli-timeout	Configures the session in-action session timeout.	<ul style="list-style-type: none"> Admin Read/Write
config datetime	Configures date and time for the Timing Client.	<ul style="list-style-type: none"> Admin Read/Write
config dns0	Configures the primary DNS server IP.	<ul style="list-style-type: none"> Admin Read/Write
config dns1	Configures the second DNS server IP.	<ul style="list-style-type: none"> Admin Read/Write
config domain	Configures the domain. {domain name}	<ul style="list-style-type: none"> Admin Read/Write
config dst	Configures offset, starting date and time, and ending date and time for DST.	<ul style="list-style-type: none"> Admin Read/Write
config el output loopback	Configures the E1 input port's number of ports, mode, framing, encoding, Receive Sensitivity, SSM, and state.	<ul style="list-style-type: none"> Admin Read/Write
config el output port	<p>Configures the E1 output port's number of ports, mode, framing, encoding, LBO, SSM, state, and framer generation.</p> <p>NOTE: The framer generation setting is available only when the Timing Client uses T1 interface type.</p>	<ul style="list-style-type: none"> Admin Read/Write
config enable-password	Modifies the password of the enable mode.	Admin

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config eth0 auto-nego	Turns Auto Negotiation ON or OFF for Ethernet 0 (LAN1) port.	<ul style="list-style-type: none"> • Admin • Read/Write
config eth0 duplex	Selects the duplex mode for the Ethernet 0 (LAN1) port between half or full duplex.	<ul style="list-style-type: none"> • Admin • Read/Write
config eth0 ip	Configures IP settings for Ethernet 0 (LAN1) port : IP address, mask, and gateway.	<ul style="list-style-type: none"> • Admin • Read/Write
config eth0 ip-mode	Selects the IP mode for the Ethernet 0 (LAN1) port between Static and DHCP.	<ul style="list-style-type: none"> • Admin • Read/Write
config eth0 speed	Selects the speed for the Ethernet 0 (LAN1) port between 10 and 100 Mbps.	<ul style="list-style-type: none"> • Admin • Read/Write
config gps anti-jamming	<p>Enables or disables the anti-jamming capability for the Resolution SMT GPS Timing Receiver.</p> <p>NOTE: This command is available only if the TCA6500 Timing Client uses the Resolution SMT GPS Timing Receiver.</p>	<ul style="list-style-type: none"> • Admin • Read/Write
config holdover-state	<p>Configures the TCA system to remain in the holdover state or change to the internal state after 24 hours of holdover state.</p> <ul style="list-style-type: none"> • 1—The system remains in the holdover state instead of changing to the internal state after 24 hours of holdover state. However, the system changes to the internal state when the signal is lost during acquisition, locking, or resetting the system. • 0 (default)—The system changes to the internal state after 24 hours of holdover state. 	<ul style="list-style-type: none"> • Admin • Read/Write
config hostname	Configures the hostname. {hostname}	Admin
config language	Configures the webpages language.	<ul style="list-style-type: none"> • Admin • Read/Write
config logger-threshold	Configures the file size threshold value. The threshold value ranges from 100 KB through 1 MB. The default value is 1 MB.	• Admin
config log-monitor-notify-medium <i>option</i>	Configures the notification medium for logmon process.	• Admin
config ntp add server	Creates an NTP association entry for the specified IPv4 address. You can define the following optional parameters: prefer, burst, version, min poll, max poll, and keyid.	<ul style="list-style-type: none"> • Admin • Read/Write
config ntp del	Deletes the specified NTP association entry.	<ul style="list-style-type: none"> • Admin • Read/Write
config password	Modifies your current login password.	Admin

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config pps-squelch	Turns on or off the PPS squelch. <ul style="list-style-type: none"> On—The PPS squelch is turned on, thereby disabling the PPS output when the TCA system is not locked to GPS or PTP. Off (default)—The PPS squelch is turned off, thereby enabling the PPS output even when the TCA system is not locked to GPS or PTP. 	<ul style="list-style-type: none"> Admin Read/Write
config ppx	Configures PPx.	<ul style="list-style-type: none"> Admin Read/Write
config primary-ptp-server	Configures the primary (PTP) proprietary packet based timing protocol.	<ul style="list-style-type: none"> Admin Read/Write
config ptp add server	Adds a PTP server.	<ul style="list-style-type: none"> Admin Read/Write
config ptp slave	Configures PTP slave.	<ul style="list-style-type: none"> Admin Read/Write
config ptp slv disable	Disables the PTP protocol.	<ul style="list-style-type: none"> Admin Read/Write
config ptp slv domain	Configures the PTP domain number to be part of the same Grandmasters domain.	<ul style="list-style-type: none"> Admin Read/Write
config ptp slv dscp	Configures the Differential Service (DiffServ) of the IP packet.	<ul style="list-style-type: none"> Admin Read/Write
config ptp slv enable	Enables the PTP protocol.	<ul style="list-style-type: none"> Admin Read/Write
config ptp slv profile	Configures the profile for unicast packet types for both sync and delay request / response PTP event messages.	<ul style="list-style-type: none"> Admin Read/Write
config ptp unicast acc-master add	Adds the IP address of the acceptable Grandmasters for the Timing Client, which is used for the Ethernet network packet IP protocol.	<ul style="list-style-type: none"> Admin Read/Write
config ptp unicast acc-master del	Deletes the IP address of the acceptable Grandmasters for the Timing Client, which is used for the Ethernet network packet IP protocol.	<ul style="list-style-type: none"> Admin Read/Write
config ptp unicast announce	Configures the announce message rate that the Timing Client requests from the Grandmaster.	<ul style="list-style-type: none"> Admin Read/Write
config ptp unicast delay	Configures the delay response message rate that the Timing Client requests from the Grandmaster.	<ul style="list-style-type: none"> Admin Read/Write

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config ptp unicast duration	Configures the Timing Client expiration duration for sending signaling messages without receiving an acknowledgement from the Grandmaster.	<ul style="list-style-type: none"> • Admin • Read/Write
config ptp unicast signaling	<p>Enables or disables the sending of the signaling messages to the Grandmaster.</p> <ul style="list-style-type: none"> • enable—Enables the sending of the signaling messages to the Grandmaster. • disable—Disables the sending of the signaling messages to the Grandmaster. 	<ul style="list-style-type: none"> • Admin • Read/Write
config ptp unicast sync	Configures the sync message rate that the Timing Client requests from the Grandmaster.	<ul style="list-style-type: none"> • Admin • Read/Write
config radius-server add	Adds the IP address of the RADIUS authentication server and sets other related configurations (secret word, retries, timeout, and port) to be used by the Timing Client for user authentication.	<ul style="list-style-type: none"> • Admin • Read/Write
config radius-server del	Deletes the RADIUS authentication server and its configuration from the authentication server list by using the IP address of the authentication server.	<ul style="list-style-type: none"> • Admin • Read/Write
config resource-monitor-duration <i>days</i>	Configures the monitoring period to view the resource data.	<ul style="list-style-type: none"> • Admin
config resource-monitor-notify-medium <i>option</i>	Configures the notification medium for resource monitor.	<ul style="list-style-type: none"> • Admin
config secondary-ptp-server	Configures the secondary (PTP) proprietary packet based timing protocol.	<ul style="list-style-type: none"> • Admin • Read/Write
config snmp contact	Configures the SNMP contact.	<ul style="list-style-type: none"> • Admin • Read/Write
config snmp readonly-community	Configures the SNMP read only community.	<ul style="list-style-type: none"> • Admin • Read/Write
config snmp readwrite-community	Configures the SNMP read and write community.	<ul style="list-style-type: none"> • Admin • Read/Write
config snmp-trap add	Adds a trap receiver address to the list.	<ul style="list-style-type: none"> • Admin • Read/Write
config snmp-trap del	Deletes a trap receiver from the list.	<ul style="list-style-type: none"> • Admin • Read/Write
config snmp-v3user add	Adds a SNMPv3 user.	<ul style="list-style-type: none"> • Admin • Read/Write

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config snmp-v3user del	Deletes a SNMPv3 user.	<ul style="list-style-type: none"> Admin Read/Write
config snr	<p>Selects SNR units between AMU or dBHz.</p> <p>NOTE: This command is not available if the TCA6500 Timing Client uses the Resolution SMT GPS Timing Receiver. The AMU is not an industry standard unit of measurement.</p>	<ul style="list-style-type: none"> Admin Read/Write
config ssl-key	<p>Downloads the specified SSL key file from the mentioned path of the configured SCP server. For more information about the dynamic SSL certificate support, see “Dynamic SSL Certificate Overview” on page 21.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The file cannot be downloaded from TFTP and FTP servers. You must download the corresponding certificate file. The file path and username should not contain any space characters. 	Admin
config ssl-cert	<p>Downloads the specified SSL certificate file from the mentioned path of the configured SCP server. For more information about the dynamic SSL certificate support, see “Dynamic SSL Certificate Overview” on page 21.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The file cannot be downloaded from TFTP and FTP servers. You must download the corresponding key file. The file path and username should not contain any space characters. 	Admin
config static-route add	<p>Adds a static route that defines a gateway IP address for reaching the destination network. The gateway IP address acts as an interface IP address for the next hop.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The gateway IP address should be in the same subnet of the eth0 interface IP address. TCA supports only one default gateway for eth0 interface. You can create only 10 static routes (inclusive of default routes). For a list of default routes, see Table 45 on page 194. 	<ul style="list-style-type: none"> Admin Read/Write
config static-route del	<p>Deletes a static route.</p> <p>NOTE: You cannot delete default routes. For a list of default routes, see Table 45 on page 194.</p>	<ul style="list-style-type: none"> Admin Read/Write
config sync-src-priority	Configures the highest priority Sync Source that the Timing Client should use. Choices include: PTP or Internal.	<ul style="list-style-type: none"> Admin Read/Write
config tftp-server [server-ip]	Configures the TFTP server IP address.	<ul style="list-style-type: none"> Admin

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
config timezone	Configures the time zone information.	<ul style="list-style-type: none"> • Admin • Read/Write
config unsecured-communication-protocols	<p>Enables or disables unsecured transfer or communication protocols such as ICMP, TFTP, FTP, and Telnet protocol. The values are:</p> <ul style="list-style-type: none"> • 1—Specifies the ICMP. • 2—Specifies the TFTP. • 3— Specifies the FTP. • 4—Specifies the Telnet protocol. • 5—Specifies all the preceding protocols. <p>By default, all the unsecured transfer or communication protocols are enabled.</p>	<ul style="list-style-type: none"> • Admin
config user add	Creates a new user account with login class as Read-Only or Read/Write.	Admin
config user class	Modifies the login class for the Read-Only or Read/Write user account.	Admin
config user del	Deletes the Read-Only or Read/Write user account.	Admin
config user password	Creates a new password for the Read-Only or Read/Write user account.	Admin
config user email	Creates a new e-mail address for the Read-Only or Read/Write user account.	Admin
config web	Configures the web enable/disable.	<ul style="list-style-type: none"> • Admin • Read/Write
config web-mode	Configures the web mode.	Admin
config web-timeout	Configures the web-timeout. [min]	Admin
debug ntp-packet <i>source IP</i>	Displays the detailed information about NTP packets from the specific IP address for debugging purposes.	<ul style="list-style-type: none"> • Admin • Read/Write
debug ntp-validity all	Displays validity of all the NTP packets for debugging purposes.	<ul style="list-style-type: none"> • Admin • Read/Write
ftp	Installs the specified software image from the configured FTP server.	Admin
halt	Halts the system.	<ul style="list-style-type: none"> • Admin • Read/Write

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
no debug ntp-packet	Stops displaying the detailed information about NTP packets from the specific IP address for debugging purposes.	<ul style="list-style-type: none"> • Admin • Read/Write
no debug ntp-validity	Stops displaying validity of all the NTP packets for debugging purposes.	<ul style="list-style-type: none"> • Admin • Read/Write
no trace ntp-packet	Stops tracing the NTP packets for debugging purposes.	<ul style="list-style-type: none"> • Admin • Read/Write
ping	Pings the remote host.	<ul style="list-style-type: none"> • Admin • Read/Write
reboot	Reboots the system.	<ul style="list-style-type: none"> • Admin • Read/Write
reset config	Restores the TCA6500 Timing Client to the manufacturer default configuration.	Admin
reset password	Restores the default password value.	Admin
restart ntp	Restarts the NTP daemon. Executing this command forcefully synchronizes its time from the configured NTP server.	Admin
restart timeprobe-agent	Starts or enables the time probe agent.	<ul style="list-style-type: none"> • Admin • Read/Write
restart ptp	Starts PTP operations	Admin
restore tftp	Restores the configuration file from a TFTP server.	Admin
restore scp	<p>Restores the configuration file from the mentioned path of the SCP server.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • The file path and username should not contain any space characters. • The maximum length of the CLI command should not exceed 124 characters. 	Admin
save tftp authlog	Saves the author log to a TFTP server.	<ul style="list-style-type: none"> • Admin • Read/Write
save tftp daemonlog	Saves the daemon log to a TFTP server.	<ul style="list-style-type: none"> • Admin • Read/Write
save tftp eventlog	Saves the event log to a TFTP server.	<ul style="list-style-type: none"> • Admin • Read/Write

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
save tftp syslog	Saves the system log to a TFTP server.	<ul style="list-style-type: none"> Admin Read/Write
save scp authlog	Saves the author log in the specified path of the SCP server. NOTE: <ul style="list-style-type: none"> The file path and username should not contain any space characters. The maximum length of the CLI command should not exceed 124 characters. 	<ul style="list-style-type: none"> Admin Read/Write
save scp daemonlog	Saves the daemon log in the specified path of the SCP server. NOTE: <ul style="list-style-type: none"> The file path and username should not contain any space characters. The maximum length of the CLI command should not exceed 124 characters. 	<ul style="list-style-type: none"> Admin Read/Write
save scp eventlog	Saves the event log in the specified path of the SCP server. NOTE: <ul style="list-style-type: none"> The file path and username should not contain any space characters. The maximum length of the CLI command should not exceed 124 characters. 	<ul style="list-style-type: none"> Admin Read/Write
save scp syslog	Saves the system log in the specified path of the SCP server. NOTE: <ul style="list-style-type: none"> The file path and username should not contain any space characters. The maximum length of the CLI command should not exceed 124 characters. 	<ul style="list-style-type: none"> Admin Read/Write
save tftp archives authlog	Saves the authorization log archive files to the specified TFTP server.	<ul style="list-style-type: none"> Admin Read/Write
save tftp archives daemonlog	Saves the daemon log archive files to the specified TFTP server.	<ul style="list-style-type: none"> Admin Read/Write
save tftp archives eventlog	Saves the event log archive files to the specified TFTP server.	<ul style="list-style-type: none"> Admin Read/Write
start ntp	Starts the operations of the NTP daemon.	Admin
start resource-monitor	Starts the resource-monitor.	Admin
stop ntp	Stops the operations of the NTP daemon.	Admin

Table 43: Configurable Elements in the CLI (*continued*)

Command	Description	Supported Users
stop resource-monitor	Stops the resource-monitor.	Admin
tftp	Installs a software upgrade image file by TFTP.	Admin
tftp license	Upload TFTP license for value-added features.	<ul style="list-style-type: none"> • Admin • Read/Write
trace ntp-packet all	Traces all the NTP packets for debugging purposes.	<ul style="list-style-type: none"> • Admin • Read/Write
scp	<p>Installs the specified software image from the mentioned path of the configured SCP server.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • The file path and username should not contain any space characters. • The maximum length of the CLI command should not exceed 124 characters. 	Admin

Using the CLI to Configure the Timing Client

To use the CLI to configure the Timing Client:

1. Launch a CLI session as described in [“Accessing the Timing Client Using the CLI” on page 159](#).
2. At the prompt, type **enable** and press Enter.
3. At the password prompt, type **enable** and press Enter.
4. At the prompt, enter the configuration command for the element to be changed or configured.
5. At the element prompt, enter the value to be used to replace the current value shown in the brackets < > and press Enter or just press Enter to retain the current value.
6. When changing the elements have been completed, enter exit and press Enter to save your changes and return to exit the enable condition.

Accessing the Timing Client Using SSH

To access the Timing Client using SSH:

1. Using a computer connected on the same network segment as the Timing Client, run the SSH client software (such as the free-ware “PuTTY” or TuTTY”).
2. Enter the IP address of the Timing Client in the hostview window.



NOTE: If the Timing Client is being accessed for the first time, see [“Assigning an IP Address to the TCA6000 or TCA6500 Timing Client” on page 14](#) for information about connecting to the unit and accessing the user interface.

3. Click the **OK** button. A DOS window appears.
4. At the login prompt, type the login name chosen and press Enter.
5. At the User name prompt, type the username and press Enter.
6. At the Password prompt, type the corresponding password and press Enter.

To see a list of available commands, type help.

Refer to [Table 42 on page 162](#) for a list of viewing options and [Table 43 on page 168](#) for a list of configurable elements.

APPENDIX B

Using the CLI to Configure PTP and Network Interface Parameters

The TCA6000 and TCA6500 Timing Clients are equivalent with respect to these features. The TCA6500 Timing Client has the additional function of having an integrated GPS receiver. Reference to the TCA6000 Timing Client applies also for the TCA6500 Timing Client. This document addresses the configuration for the PTP functionality in order to communicate with the TCA8000 Timing Server or third-party Grandmaster. Since the Ethernet physical layer and packet protocol (UDP/IP) are part of the connectivity this is also covered in the document even though this is a general requirement in order to access also the management interface of the system. Similarly this applies to the VLAN which is optional. All configuration commands are preceded by config and status commands preceded by show, except where noted with an asterisk (*).

- [Timing Client PTP Functions on page 181](#)
- [PTP Profile Types on page 181](#)
- [PTP Profile Configuration on page 183](#)
- [Sync Source Selection on page 190](#)
- [Ethernet Port Network Configuration on page 191](#)
- [VLAN Port Association \(optional\) on page 192](#)
- [Static Route IP \(optional\) on page 194](#)

Timing Client PTP Functions

The TCA6000 and TCA6500 Timing Clients are equivalent with respect to these features. The TCA6500 Timing Client has the additional function of having an integrated GPS receiver. Reference to the TCA6000 Timing Client applies also for the TCA6500 Timing Client.

PTP Profile Types

Default Profile:

- Supports OneStep and TwoStep modes.
- Process Multicast Announce/Sync/Delay Response.

- Sends Multicast Delay Request with 32 pps or 64 pps.
- There is no Signaling/Management Packet support.

Brilliant/Juniper Type I:

- Supports OneStep and TwoStep modes.
- Process Multicast Announce/Sync and Unicast Delay Response.
- Sends Unicast Delay Request with 32 pps or 64 pps.
- There is no Signaling/Management Packet support.

Telecom Profile without Signaling:

- Supports OneStep mode only.
- Supports Unicast Announce/Sync and Unicast Delay Response.
- There is no Signaling/Management Packet support.

Entry of the Slave IP address is configured at the Grandmaster (TCA8000 Timing Server).

Telecom Profile with Signaling:

- Supports OneStep mode only.
- Supports Unicast Announce/Sync and Unicast Delay Response.
- Supports Unicast Discovery and Signaling.
- Slave supports signaling messages for:

Sends REQUEST UNICAST TRANSMISSION for Announce

Sends REQUEST UNICAST TRANSMISSION for SYNC

Sends REQUEST UNICAST TRANSMISSION for Delay Response

Process GRANT UNICAST TRANSMISSION for Announce

Process GRANT UNICAST TRANSMISSION for SYNC

Process GRANT UNICAST TRANSMISSION for Delay Response

Sends CANCEL UNICAST TRANSMISSION for Delay Response

Acceptable Master Support. Maximum Acceptable Masters is 2

Sync Rate can be configured from 1 pps to 64 pps



NOTE: 32 pps or 64 pps (recommended) required for meeting performance specifications.

Delay Rate can be configured to 1 Pkt/64Sec, 1 Pkt/32Sec, 1 Pkt/16Sec, 1 Pkt/8Sec, 1 Pkt/4Sec, 1 Pkt/2Sec, 1 Pkt/Sec, 2 Pkt/Sec, 4 Pkt/Sec, 8 Pkt/Sec, 16 Pkt/Sec, 32 Pkt/Sec, 64 Pkt/Sec, or 128 Pkt/Sec.



NOTE: 32 Pkt/Sec or 64 Pkt/Sec (recommended) required for meeting performance specifications.

Announce Rate can be configured to 1pkt/1sec, 1pkt/2sec, 1pkt/4sec, 1pkt/8sec, 2pkt/1sec, 4pkt/1sec, or 8pkt/1sec.

PTP Over Ethernet Profile:

- Supports One-step and Two-step modes.
- Process Multicast Announce/Sync/Delay Response.
- Sends Multicast Delay Request with 32 pps or 64 pps.
- There is no Signaling/Management/Unicast Packet support.

PTP Profile Configuration

Configuration requires the second level of login which is after login using admin / admin (or user assigned information) the config login needs to be executed which is “en” at the prompt followed by entering the password “enable”.

The network parameters of the Ethernet interface should be configured before configuring the PTP profile information.

The following parameters are set for the PTP profile through the configuration commands:

Table 44: Configuration Commands

Parameter	Value
Domain number	0 through 254
Delay Req Mode	0: Unicast 1: Multicast
Telecom Profile	0: Telecom Profile Disable 1: Telecom Profile Enable 2: PTP over Ethernet

Table 44: Configuration Commands (*continued*)

Parameter	Value
Delay Req Interval	0: 1 Pkt/64Sec
	1: 1 Pkt/32Sec
	2: 1 Pkt/16Sec
	3: 1 Pkt/8Sec
	4: 1 Pkt/4Sec
	5: 1 Pkt/2Sec
	6: 1 Pkt/Sec
	7: 2 Pkt/Sec
	8: 4 Pkt/Sec
	9: 8 Pkt/Sec
	10: 16 Pkt/Sec
	11: 32 Pkt/Sec
	12: 64 Pkt/Sec
	13: 128 Pkt/Sec
Announce Receipt Timeout	2 through 10

The parameter options for the configuration command can be obtained for the configuration commands by adding a question-mark (?) after typing in # config, such as "# config ptp slave?"



NOTE: Configuration for Default, Brilliant/Juniper Type I and Telecom with or without Signaling profiles can also be done through the Web Interface.

- [Default Profile Configuration Command on page 184](#)
- [Brilliant/Juniper Type I Profile Configuration Command on page 185](#)
- [Telecom Profile—Without Signaling Configuration Command on page 186](#)
- [Telecom Profile—With Signaling Configuration Command on page 187](#)
- [PTP Over Ethernet Profile Configuration Command on page 189](#)
- [Status Commands on page 189](#)

Default Profile Configuration Command

The profile is configured with other PTP parameters within a configuration string. The Sync and Delay_Response rates at the Grandmaster are required to match the Timing Client Sync and Delay_Request packet rates.

ptp slave:

The parameters that are required to be configured are the PTP Domain # (0-254), the Sync / Delay_Request packet type as being multicast, the profile type as not being Telecom Profile, the Delay_Request packet rate and the Announce message type response from the Grandmaster timeout interval.

ptp slv—[domain #=20] [Default Profile = 1 0 (multicast) & (Telecom Profile disabled)] [Delay Req Interval = 6] [Announce Receipt Timeout=10]



NOTE: Only Delay Req Interval rates of 32 pps or 64 pps are supported and 64 (6) is recommended.

```
# config ptp slave 20 1 0 6 10
```

ptp slv dscp—Configures the Differential Service (DiffServ) of the IP packet which transports the PTP event and signaling messages. This should be configured to Explicit Forward (EF) which is a value of 46 decimal.

```
# config ptp slv dscp 46
```

config ptp slv disable—Disables the PTP protocol. Only after your confirmation, the PTP protocol is disabled.



NOTE: This command is applicable for all profile types.

```
# config ptp slv disable
Are you sure you want to disable slave ptp? y/n
y
```

config ptp slv enable—Enables the PTP protocol. Only after your confirmation, the PTP protocol is enabled.



NOTE: This command is applicable for all profile types.

```
# config ptp slv enable
Are you sure you want to enable slave ptp? y/n
y
```

Brilliant/Juniper Type I Profile Configuration Command

The profile is configured with other PTP parameters within a configuration string. The Sync and Delay Response rates at the Grandmaster are required to match the Timing Client Sync and Delay_Request packet rates.

ptp slave:

- The parameters that are required to be configured are the PTP Domain # (0-254), the Sync / Delay_Request packet type as being unicast, the profile type as not being Telecom Profile, the Delay_Request packet rate and the Announce message type response from the Grandmaster timeout interval.

Example configuration:

```
# config ptp slave
```

- [domain #] [0: unicast 1: multicast] [0: Telecom Profile disabled 1: Telecom Profile enabled 2: PTP over ethernet] [Delay Req Interval] [Announce Receipt Timeout: 2~10]



NOTE: Only Delay Req Interval rates of 32 pps or 64 pps are supported and 64 (6) is recommended.

```
# config ptp slave 20 0 0 6 10
```

ptp slv dscp:

- Configures the Differential Service (DiffServ) of the IP packet which transports the PTP event and signaling messages. This should be configured to Explicit Forward (EF) which is a value of 46 decimal.

Example: # config ptp slv dscp 46

Telecom Profile—Without Signaling Configuration Command

The profile is configured with other PTP parameters within a configuration string. In order for the Grandmaster to recognize the slave unit, the Timing Client IP address of the Timing Client needs to be configured at the Grandmaster for the Ethernet network IP protocol communication link. The Sync and Delay_Response rates at the Grandmaster are required to match the Timing Client Sync and Delay_Request packet rates.

ptp slave—The parameters that are required to be configured are the PTP Domain # (0-254), the Sync / Delay_Request packet type as being unicast, the profile type as Telecom Profile, the Delay_Request packet rate and the Announce message type response from the Grandmaster timeout interval.

```
# config ptp slave
[domain #] [0: unicast 1: multicast] [0: Telecom Profile disabled 1:
Telecom Profile enabled 2: PTP over ethernet] [Delay Req Interval]
[Announce Receipt Timeout: 2~10].
```



NOTE: The TCA6000 supports Delay Req Interval rates of 32 pps or 64 pps are supported and 64 pps (6) is recommended.

```
# config ptp slave 20 0 1 6 10
```

ptp slv dscp—Configures the Differential Service (DiffServ) of the IP packet which transports the PTP event and signaling messages. This should be configured to Explicit Forward (EF) which is a value of 46 decimal.

```
# config ptp slv dscp 46
```

ptp unicast signaling—Enables or disables the signaling messages to be sent to the Grandmaster.

```
config ptp unicast signaling disable
```



NOTE: If signaling is disabled, you need to have slave entry manually in the master unicast list.

Telecom Profile—With Signaling Configuration Command

The profile requires individual parameters to be entered. Even though some parameters are not directly associated with the profile, these parameters will be shown here for consistency with the other profile configuration string.

ptp slave—The parameters that are required to be configured are the PTP Domain # (0-254), the Sync / Delay_Request packet type as being unicast, the profile type as Telecom Profile, the Delay_Request packet rate and the Announce message type response from the Grandmaster timeout interval.

Example configuration:

```
# config ptp slave
[domain #] [0: unicast 1: multicast] [0: Telecom Profile disabled 1:
Telecom Profile enabled 2: PTP over ethernet] [Delay Req Interval] [Announce
Receipt Timeout: 2~10]

# config ptp slave 20 0 1 6 10
```

ptp slv domain—Configures the PTP domain number to be part of the same Grandmaster(s) domain. The values can be 0 to 254 and needs to be configured as the same domain number of the associated Grandmaster(s).

```
# config ptp slv domain 20
```

ptp slv profile—Configure the profile for unicast packet types for both Sync and Delay_Request /Response PTP event messages.

```
# config ptp slv profile 2
```

ptp unicast sync—Configures the Sync message rate that the Timing Client requests from the Grandmaster.



NOTE: The TCA6000 Timing Client supports Sync rates of 32 pps or 64 pps are supported and 64 pps (6) is recommended.

```
# config ptp unicast sync 6
```

ptp unicast delay—Configures the Delay_Response message rate that the Timing Client requests from the Grandmaster.



NOTE: The TCA6000 Timing Client supports Delay_Request/Response rates of 1 Pkt/64Sec, 1 Pkt/32Sec, 1 Pkt/16Sec, 1 Pkt/8Sec, 1 Pkt/4Sec, 1 Pkt/2Sec, 1 Pkt/Sec, 2 Pkt/Sec, 4 Pkt/Sec, 8 Pkt/Sec, 16 Pkt/Sec, 32 Pkt/Sec, 64 Pkt/Sec, and 128 Pkt/Sec.

```
# config ptp unicast delay 6
```

ptp unicast announce—Configures the Announce message rate as 1pkt/1sec, 1pkt/2sec, 1pkt/4sec, 1pkt/8sec, and 2pkt/1sec, 4pkt/1sec, or 8pkt/1sec that the Timing Client requests from the Grandmaster.

```
# config ptp unicast announce 0
```

ptp unicast duration—Configures the Timing Client expire duration for sending signaling messages without receiving acknowledgement from the Grandmaster. The duration can be configured in 1 second increments from 100 to 3000.

```
# config ptp unicast duration 3000
```

ptp unicast acc-master add—Adds the IP-address of the acceptable Grandmaster(s) for the Timing Client which is used for the Ethernet network packet IP protocol.

```
# config ptp unicast acc-master add 192.168.50.101
```

ptp unicast acc-master del—Deletes the IP-address of the acceptable Grandmaster(s) for the Timing Client which is used for the Ethernet network packet IP protocol.

```
# config ptp unicast acc-master del 192.168.50.101
```

ptp unicast signaling—Enables or disables the signaling messages to be sent to the Grandmaster.

```
# config ptp unicast signaling enable
```



NOTE: When reverting back to other profiles, signaling needs to be disabled.

ptp slv dscp—Configures the Differential Service (DiffServ) of the IP packet which transports the PTP event and signaling messages. This should be configured to Explicit Forward (EF) which is a value of 46 decimal.

```
# config ptp slv dscp 46
```

PTP Over Ethernet Profile Configuration Command

The profile is configured with other PTP parameters within a configuration string. The Sync and Delay_Response rates at the Grandmaster are required to match the Timing Client Sync and Delay_Request packet rates.

ptp slave:

The parameters that are required to be configured are the PTP Domain # (0-254), the Sync or Delay_Request packet type as being multicast, the profile type as PTP over Ethernet, the Delay_Request packet rate and the Announce message type response from the Grandmaster timeout interval.

ptp slv—[domain #=20] [Default Profile = 1 2 (multicast) & (PTP over Ethernet)] [Delay Req Interval = 6] [Announce Receipt Timeout=10]

```
# config ptp slave 20 1 2 6 10
```

config ptp slv disable—Disables the PTP protocol. Only after your confirmation, the PTP protocol is disabled.



NOTE: This command is applicable for all profile types.

```
# config ptp slv disable
Are you sure you want to disable slave ptp? y/n
y
```

config ptp slv enable—Enables the PTP protocol. Only after your confirmation, the PTP protocol is enabled.



NOTE: This command is applicable for all profile types.

```
# config ptp slv enable
Are you sure you want to enable slave ptp? y/n
y
```

Status Commands

Most status commands can be executed at the first level of login except where noted by an asterisk (*). These commands require the second level of login which is the same level as when configuration commands are executed.

ptp config—Displays the configuration parameters of the PTP for the Default, Brilliant/Juniper Type I, Telecom Profile without Signaling, or PTP over Ethernet profile.

ptp unicast-config—Displays the configuration parameters of the PTP for Telecom Profile with Signaling.

ptp default-dataset—Displays the PTP parameter including Domain # that is configured.

ptp utc-prop—Displays the UTC time information that is being used within the PTP timestamps including the offset.

ptp timescale-prop—Displays the PTP timestamp source type.

ptp stat—* Displays the valid and invalid PTP message event counters.

clear ptp stat: *Clears the counters

ptp dscp—Displays the Differential Service value for the IP packets which transport the PTP event and signaling messages.

ptp status—Displays the operation mode of the Timing Client (slave), state and PTP domain number.

Sync Source Selection

The Sync (Synchronization) Source selection provides a priority selection for the TCA6000/6500 Timing Clients. The selected clock source is used to provide the clock reference for the external timing ports, that is T1/E1, 10/5/1 MHz and Pulse-per-Second (PPS). The TCA6000 Timing Client should be configured for “ptp”, that is the IEEE1588v2 recovered timing. The TCA6500 Timing Client has two source selections which are the “ptp” and the GPS recovered timing. Since GPS is a higher Stratum level than PTP recovered timing, it is normally configured as the higher priority source.

- [Configuration on page 190](#)
- [Status Commands on page 191](#)

Configuration

sync-src-priority—Configures the priority selection for the timing source that is used with starting with the highest priority first in the string. Both products use the internal reference oscillator when a source is not available.

```
# config sync-src-priority ptp internal
```

**NOTE:**

- 'Internal' should always be the lowest priority.

Status Commands

sync-src-priority—Displays the Sync Source selections with highest priority being displayed first.



NOTE: If 'internal' was not specified the status will not display this selection although it is still in the sync source selection as the lowest priority.

Ethernet Port Network Configuration

The Ethernet port is required to be configured with the appropriate Ethernet and IP parameters.



NOTE: You cannot configure Ethernet and VLAN port addresses to be in the same subnet (that is, all logical and physical interfaces should be configured to be in different subnets).

- [Configuration on page 191](#)
- [Status Commands on page 192](#)

Configuration

The reference to eth0 (LAN port) is for the single TCA6000 Timing Client Ethernet port.

eth0 speed—Configures the Ethernet port to either 10 or 100 Mbps. It is recommended to use 100 Mbps (default).

eth0 duplex—Configures the Ethernet port as half or full duplex. For performance requirements to be achieved, full duplex (default) is required.

eth0 auto-nego—Configures the Ethernet port as being able to auto negotiate the speed and half/full duplex (yes / no). It is recommended this be disabled (default), that is no.

eth0 ip—Configures the port IP address, IP Mask and Gateway.

```
config eth0 ip 192.168.50.120 255.255.255.0 192.168.50.1
```

eth0 ip-mode—Configures the IP address as being a static or dynamic.

```
# config eth0 ip-mode static
```

ptp slv dscp—Configures the Differential Service (DiffServ) of the IP packet which transports the PTP event and signaling messages. This should be configured to Explicit Forward (EF) which is a value of 46 decimal.

```
# config ptp slv dscp 4
```

Status Commands

show network—Displays the network configuration and MAC address of the Ethernet port.

VLAN Port Association (optional)

VLAN port association is not required for the operation of IEEE1588v2 and is used only when it is required to encapsulate the IEEE1588v2 timing packets and signaling (if enabled) into a VLAN packet format. If the Ethernet switch in which the TCA6000 Timing Client is connected supports port based VLAN then this operation can be accomplished within the actual Ethernet switch. Two VLANs are supported for the single Ethernet port. When using VLANs the application would be that one VLAN is associated with PTP message events which are on the same VLAN as the PTP Grandmaster Ethernet port (LAN1). The second VLAN would be associated with the management system within the network. Following is the configuration commands to attach a VLAN to IEEE1588v2 (PTP) event messages. Configuration requires the second level of login which is after login using admin / admin (or user assigned information) the config login needs to be executed which is “en” at the prompt followed by entering the password “enable”. The network parameters of the Ethernet interface should be configured before configuring the VLAN information.



NOTE: You cannot configure Ethernet and VLAN port addresses to be in the same subnet (that is, all logical and physical interfaces should be configured to be in different subnets).

- [Configuration Commands on page 192](#)
- [Status Commands on page 193](#)

Configuration Commands

The second VLAN is configured in a similar manner by using VLAN2 instead of VLAN1.

eth0 vlan1 ip—Configures the VLAN Ethernet IP address.

```
# config eth0 vlan1 ip 192.168.1.100 255.255.0.0
```

eth0 vlan1 id—Assigns a unique VLAN ID that is used for the VLAN encapsulation packet. This value can be in the range from 2 through 4095.


```
# config eth0 vlan1 id 100
```



NOTE: If the VLAN ID you have configured is already being used by any other VLAN, a warning message is displayed.

eth0 vlan1 priority—This assigns the 3 bit priority in the VLAN header which is used for differential services transporting the packet. It is recommended this be configured to the high priority level and use the value 7.

```
# config eth0 vlan1 priority 7
```

eth0 vlan1 ip-mode—Configures the IP address as being a static or dynamic.

```
# config eth0 vlan1 ip-mode static
```

ptp slv dscp—Configures the Differential Service (DiffServ) of the IP packet which transports the PTP event and signaling messages. This should be configured to Explicit Forward (EF) which is a value of 46 decimal.

```
# config ptp slv dscp 46
```

ptp slv interface—Configures the VLAN 1 or 2 configuration parameters to be used to encapsulate the PTP signaling and event messages.

```
# config ptp slv interface eth0 1
```

eth0 vlan1 enable—VLAN encapsulation of the IP packet is enabled.

```
# config eth0 vlan1 enable
```



NOTE: After VLAN related configuration restart PTP by using the command “# restart ptp”.

eth0 vlan1 disable—VLAN encapsulation of the IP packet is disabled.

```
# config eth0 vlan1 disable
```



NOTE: After VLAN related configuration restart PTP by using the command “# restart ptp”.

Status Commands

ptp interface—Displays if there is VLAN encapsulation enabled and if it is which VLAN1 and 2 encapsulation parameters are being used for the PTP event and signaling messages.

network—Displays the network IP and port parameters which includes the VLAN enable/disable information.

vlan—Show the VLAN parameters for VLAN 1 and 2.

Static Route IP (optional)

Static routing provides a way of configuring path selection in the network which LAN1 or LAN2 are connected. The network connectivity is achieved by manually adding routes into the local static route table (maximum 10 static routes).



NOTE: TCA supports only one default gateway for eth0 interface.

- [Configuration Commands on page 194](#)
- [Status Commands on page 194](#)
- [Examples on page 194](#)

Configuration Commands

static-route add—Adds the static route, mask and gateway IP-Addresses.

```
config static-route add 192.168.60.0 255.255.255.0 10.0.0.1
```

static-route del—Deletes the static route, mask and gateway IP-Addresses.

```
config static-route del 192.168.60.0 255.255.255.0 10.0.0.1
```

Status Commands

static-route-config—Shows the static route list which were configured.

static-route-status—Shows the static route list which were configured and its LAN1 (eth0) port association.

Examples

The following are default routes which cannot be modified, that is deleted

Table 45: Default Routes

Network	Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Eth0
0.0.0.0	0.0.0.0	192.168.0.1	Eth0

Example 1: If the user wants to reach the 2.2.2.2 IP address by using the Gateway as 192.168.0.100 on Eth0 interface

```
# config static-route add 2.2.2.0 255.255.255.0 192.168.0.100
```

After adding the route for 2.2.2.0 network all the packets for 2.2.2.0 n/w goes through "Eth0" interface.

Table 46: Network Configurations

Network	Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Eth0
0.0.0.0	0.0.0.0	192.168.0.1	Eth0
2.2.2.0	255.255.255.0	192.168.0.100	Eth0

Example 3: To delete the static routes:

```
config static-route del 2.2.2.0 255.255.255.0 192.168.0.100
config static-route del 3.3.3.0 255.255.255.0 192.168.1.200
```


APPENDIX C

Using the CLI to Configure NTP Parameters

This appendix explains the configurations to be done for the NTP functionality in the Timing Client in order to communicate with the TCA8x00 Timing Server or third-party Grandmaster. All configuration commands are preceded by **config** and status commands preceded by **show**, except where noted with an asterisk (*).

- [NTP Mode on page 197](#)
- [Enabling the NTP Support in the Timing Clients using the CLI on page 197](#)
- [NTP Association Configuration or Status on page 198](#)
- [Start, Restart, and Stop Commands—NTP on page 199](#)

NTP Mode

NTP is used to synchronize system clocks among a set of distributed Timing Servers and Timing Clients. The Timing Client supports only the Unicast mode. In the Unicast mode, all remote peers available in the mentioned network are synchronized to the NTP server but the NTP server is not synchronized to any of the remote peer. Remote peers synchronize their time with one NTP server at a time. If the active NTP server is disconnected, then the Timing Client will select another NTP server from the configured server list.

Enabling the NTP Support in the Timing Clients using the CLI

By default, the PTP support is enabled in the Timing Client. You should enable the NTP support to view the NTP commands and GUI pages for configuring NTP.



NOTE: Only the Admin user can change the protocol support.

To enable the NTP support through the CLI:

1. Login as admin.
 - a. **>admin<cr>**

- b. `>password:admin<cr>`
2. Enable privileged commands.
 - a. `>enable<cr>`
 - b. `>password:enable<cr>`
3. Execute the corresponding command to enable the NTP support and then type **y** to confirm rebooting the Timing Client with the enabled protocol support.


```
# config protocol-support ntp
System reboot is required to make changes effective. Do you want to reboot (y/n)
Y
```



NOTE: If you reject the rebooting of the Timing Client, the protocol change is not saved and the Timing Client continues to use the PTP.

NTP Association Configuration or Status

You can configure the NTP functionality in the Timing Client by creating NTP association entries with the supported NTP modes. The commands used to configure NTP functionality can be executed only at the Enable mode. You can enter into this Enable mode by using the **enable** command after logging in to the Timing Client.

While creating the entry, the default values are set for the optional parameters if optional parameters are not configured. You can add only a maximum of 20 entries. Each entry should have a unique IPv4 address.

The following parameters are set while creating the NTP association entry.

Table 47: NTP Configuration Commands

Parameter	Value	Default Value
prefer	0 and 1	0
burst	0 through 3	0
version	1 through 4	4
min poll	4 through 17	6
max poll	4 through 17	10
keyid	0 through 16	0

The parameter options for the configuration command can be obtained by adding a question-mark (?) after typing in # config, such as "# config ntp add server ?".

- [Configuration Commands on page 199](#)
- [Status Commands on page 199](#)

Configuration Commands

ntp add server—Creates an NTP association entry for the specified IPv4 address with the NTP mode set to Unicast. While creating the entry, you can define the optional parameters: prefer (0 and 1), burst (0 through 3), version (1 through 4), min poll (4 through 17), max poll (4 through 17), and keyid (0 through 16).

```
# config ntp add server 2.4.6.8 1 0 4 6 10 7 where [prefer=1], [burst=0],  
[version=4], [min poll=6], [max poll=10], [keyid=7]
```

ntp del—Deletes the specified NTP association entry.

```
# config ntp del 2.4.5.6
```

Status Commands

ntp config—Displays the details of the configured NTP association entries.

ntp status—Displays the status of the configured NTP association entries.

Start, Restart, and Stop Commands—NTP

You can start, restart, and stop the NTP daemon.

start ntp*—Starts the the operations of the NTP daemon.

restart ntp*—Restarts the NTP daemon. Executing this command forcefully synchronizes its time from the configured NTP server.

stop ntp*—Stops the operations of the NTP daemon.

APPENDIX D

Using the CLI to Configure User Authentication and RADIUS Accounting

This appendix explains the CLI commands used to configure user authentication and RADIUS accounting in the TCA6000 and TCA6500 Timing Clients. The TCA6000 and TCA6500 Timing Clients work the same in case of these features.

- [User Authentication on page 201](#)
- [RADIUS Accounting on page 202](#)

User Authentication

User authentication enables the user logging in to the Timing Client to be authenticated either locally, using RADIUS authentication servers, or both based on the authentication order.

- [Configuration Commands on page 201](#)
- [Status Commands on page 202](#)

Configuration Commands

radius-server add—Adds the IP address of the RADIUS authentication server to be used by the Timing Client for user authentication. While adding the IP address, you can set the optional parameters secret word, retries (1 to 10), timeout (1 to 90), and port, that is [secret-word] [retries] [timeout] [port].



NOTE: The default values are set for the retries, timeout, and port options, if not configured. You can use the same command for modifying the configuration details of existing RADIUS authentication server. You can add only three RADIUS authentication servers.

```
# config radius-server add 192.168.0.2 auth123 5 50 1800 where  
[secret-word=auth123], [retries=5], [timeout=50 seconds], [port=1800]
```

radius-server del—Deletes the RADIUS authentication server and its configuration by using the IP address of the server. The server is no longer used by the Timing Client for user authentication.

```
#config radius-server del 192.168.0.2
```

auth-order—Configures the authentication order to be followed by the Timing Client.

```
#config auth-order radius [Only RADIUS server authentication]
```

Status Commands

radius-server—Displays the details of the configured RADIUS authentication servers.

auth-order—Displays the configured authentication order.

RADIUS Accounting

RADIUS accounting enables the Timing Client to remotely account users logged in to the Timing Client.

- [Configuration Commands on page 202](#)
- [Status Commands on page 203](#)

Configuration Commands

accounting-server add—Adds the IP address of the RADIUS accounting server to be used by the Timing Client for accounting. While adding the IP address, you can set the optional parameters secret word, retries (1 to 10), timeout (1 to 90), and port, that is [secret-word] [retries] [timeout] [port].



NOTE: The default values are set for the retries, timeout, and port options, if not configured. You can use the same command for modifying the configuration details of existing RADIUS accounting server. You can add only 3 RADIUS accounting servers.

```
# config accounting-server add 192.169.0.2 auth123 5 50 1814 where  
[secret-word=auth123], [retries=5], [timeout=50 seconds], [port=1814]
```

accounting-server del—Deletes the RADIUS accounting server and its configuration by using the IP address of the server. The server is no longer used by the Timing Client for accounting.

```
#config accounting-server del 192.169.0.2
```

accounting-level—Configures the information (1: For login accounting only, 2: For interactive and login accounting, 3: For configuration, interactive and login accounting) to be used by the Timing Client for accounting. Default value is 3.

```
# config accounting-level 1 where [1=For login accounting only]
```

accounting—Enables or disables RADIUS accounting in the Timing Client.

```
# config accounting enable
```

Status Commands

accounting-server—Displays the details of the configured RADIUS accounting servers.

accounting-level—Displays the type of information to be accounted.

accounting-status—Displays the current status of RADIUS accounting.

APPENDIX E

Specifications

This appendix lists the specifications for the Juniper Networks TCA6000 and TCA6500 Timing Clients.

- [Physical Dimensions on page 205](#)
- [Power Specifications on page 205](#)
- [Environmental Specifications on page 206](#)

Physical Dimensions

[Table 48 on page 205](#) lists the physical dimensions of the TCA6000 and TCA6500 Timing Clients.

Table 48: Physical Dimensions

Dimension	Specification
Height	1.75 in (4.45 cm)
Width	8.5 in (21.59 cm)
Depth	12 in (30.48 cm)

Power Specifications

[Table 49 on page 205](#) lists the power specifications for the TCA6000 and TCA6500 Timing Clients.

Table 49: Power Specifications

Dimension	Specification
Power Consumption	Max 15 W
Input Voltage	DC version: –18 to –60 VDC

Environmental Specifications

[Table 50 on page 206](#) lists the environmental specifications for the TCA6000 and TCA6500 Timing Clients.

Table 50: Environmental Specifications

Dimension	Specification
Operating Temperature	+ 40° F to +144° F (-40° C to + 65° C)
Storage Temperature	-104° F to +176° F (-40° C to +80° C)
Operating Humidity	0% to 85% non-condensing,

APPENDIX F

Agency Compliance

- [Agency Compliance on page 207](#)

Agency Compliance

The Juniper Networks TCA6000 and TCA6500 Timing Clients are "Suitable for deployment" in any environment where the following compliance certifications are accepted:

- EMC testing to:
 - ETSI EN301-489-1
 - ETSI EN301-444
 - EN 300-386 and reports FCC, ICES 003, EN55022, AS/NZS CISPR22, VCCI
 - EN 301-489-1 and EN301-444 (Spurious Rad emissions above 1 GHz on the GPS version)
- Safety testing to:
 - IEC 60950-1, EN 60950-1+A11
 - UL/CSA 60950-1 and certification by TUV for TUV T-mark (European)
 - cTUVus—mark (North America) and CB test report, CB certificate (worldwide)

APPENDIX G

Cable Specification

- [Console Cable Specification on page 209](#)

Console Cable Specification

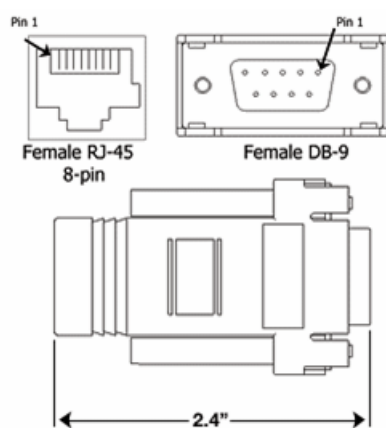
To communicate with a Juniper Networks TCA6000 or TCA6500 Timing Client, a standard RJ-45 to DB-9 cable is used.

Table 51: Signal Flow Diagram

From RJ-45	Signal	Direction	Signal	To DB-9
1	RTS (not connected)	→	CTS	8
2	DTR / TXD Time-of-Day* (not connected)	→	DTS / TXTOD*	6
3	TXD	→	RXD	2
4	GND	↔	GND	5
5	GND	↔	GND	5
6	RXD	←	TXD	3
7	DSR (not connected)	←	DTR	4
8	CTS (not connected)	←	RTS	7

* Available only for TCA6500.

Figure 64: Console Cable Connectors



APPENDIX H

Warranty and Support

- [Requesting Technical Support on page 211](#)
- [Self-Help Online Tools and Resources on page 211](#)
- [Returning a Hardware Component to Juniper Networks, Inc. on page 212](#)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

Returning a Hardware Component to Juniper Networks, Inc.

If a problem cannot be resolved by the JTAC technician, a Return Materials Authorization (RMA) is issued. This number is used to track the returned material at the factory and to return repaired or new components to the customer as needed.



NOTE: Do not return any component to Juniper Networks, Inc. unless you have first obtained an RMA number. Juniper Networks, Inc. reserves the right to refuse shipments that do not have an RMA. Refused shipments will be returned to the customer through collect freight.

For more information about return and repair policies, see the customer support webpage at <https://www.juniper.net/support/guidelines.html>.

For product problems or technical support issues, contact the Juniper Networks Technical Assistance Center (JTAC) using the Case Manager link at <https://www.juniper.net/support/> or at 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

To return a hardware component:

1. Determine the part number and serial number of the component.
2. Obtain an RMA number from the Juniper Networks Technical Assistance Center (JTAC). You can send e-mail or telephone as described above.
3. Provide the following information in your e-mail message or during the telephone call:
 - Part number and serial number of component
 - Your name, organization name, telephone number, and fax number
 - Description of the failure
4. The support representative validates your request and issues an RMA number for return of the component.
5. Pack the component for shipment.