



SNMP Agent Option for TimePictra

Release 3.0

Administrator's Guide

097-48361-30

Issue 1

October 2002

Symmetricom, Inc.
2300 Orchard Parkway
San Jose, CA 95131-1017
U.S.A.

<http://www.symmetricom.com>

Copyright © 2002 Symmetricom, Inc.
All rights reserved. Printed in U.S.A.

All product names, service marks, trademarks, and registered trademarks used in this document are the property of their respective owners.

Chapter 1 Introduction and General Information

Materials Provided	6
General	6
Topics included in this Guide	6
Naming Conventions used in this Guide	6
Acronyms Used in the Guide	7
Description of the Agent	8
Event Forwarding	9
Handling Requests	10
Information Model	10
FAQ Regarding the MIB	12
Responsibilities of the System Administrator	15
System Requirements	16
Software Requirements	16
Hardware Requirements	16
Prerequisite Knowledge	17
Related Documentation	18

Chapter 2 Installation

In This Chapter	20
Overview	21
Installing the TimePictra SNMP Agent	22
Prerequisites	22
Removing the TimePictra SNMP Agent	24
Uninstalling TimePictra SNMP Option	24
Configuring the Agent	25
Starting The Agent	26
Master Agent	26
Stopping the Agent	27
Enable Tracing	28
TimePictra Tracing	28

Chapter 3 Special Features and Limitations of the Agent

Special Features	30
SET a Single Attribute	30
Get getAllActiveAlarms Attribute	30
Get getAllActiveAlarmsOnNE Attribute	30
Limitations of the Agent	31

Chapter 4 Troubleshooting

Troubleshooting Hints	34
---------------------------------	----

Appendix A Traps and Fields

Traps and Fields	38
----------------------------	----

Introduction and General Information

TimePictra SNMP Agent System Administrator's Guide provides information necessary to install, manage, and maintain the TimePictra SNMP Agent.

Materials Provided

1

The TP Software SNMP Agent option includes the materials listed below:

- TimePictra Software SNMP Agent System Administrator's Guide (Documentation).
- TimePictra CD - SNMP Option

General

The TimePictra SNMP Agent System Administrator's Guide provides information necessary to install, manage, and maintain the TimePictra SNMP Agent (referred to also as the Agent). It assumes the user is familiar with HP-UX 11.xx, SNMP Research's EMANATE Master Agent, and TimePictra software administering.

Topics included in this Guide

This guide includes the following topics:

- A description of the Agent Software.
- Minimum system resources required to run the Agent.
- Responsibilities of the System Administrator.
- Basic SNMP Administration tasks, such as installing and configuring the Agent.
- Description about the special features provided by the Agent.
- Solutions for the common problems, which may be encountered during application usage.

Naming Conventions used in this Guide

This guide uses several naming conventions to refer to the same objects. The usage of multiple terms for the same object helps to define the relationship between the objects in different situations.

Table A lists naming conventions, the objects and their corresponding names.

Table A. Naming Conventions

Object	Names used for the object
TimePictra	TP software, TP
HP-UX Workstation	TP workstation, TP system, host system, element Manager. Hewlett Packard Unix operating system
TP SNMP Agent	SNMP Agent, Sub Agent, Agent

Acronyms Used in the Guide

Table B lists lists the all Acronyms with the descriptions used in this document.

Table B. Acronyms

Acronym	Description
TP	TimePictra
NE/ NSU	Network Element/Network Synchronization Unit
SNMP	Simple Network Management Protocol
TL1	Transaction Language 1
MIB	Model Information Base

Description of the Agent

1

TimePictra provides a user friendly Graphical User Interface (GUI) to facilitate the management of NEs. It also provides an SNMP agent to interface with higher-layer network management systems. The TP SNMP agent is the component that supports this SNMP interface.

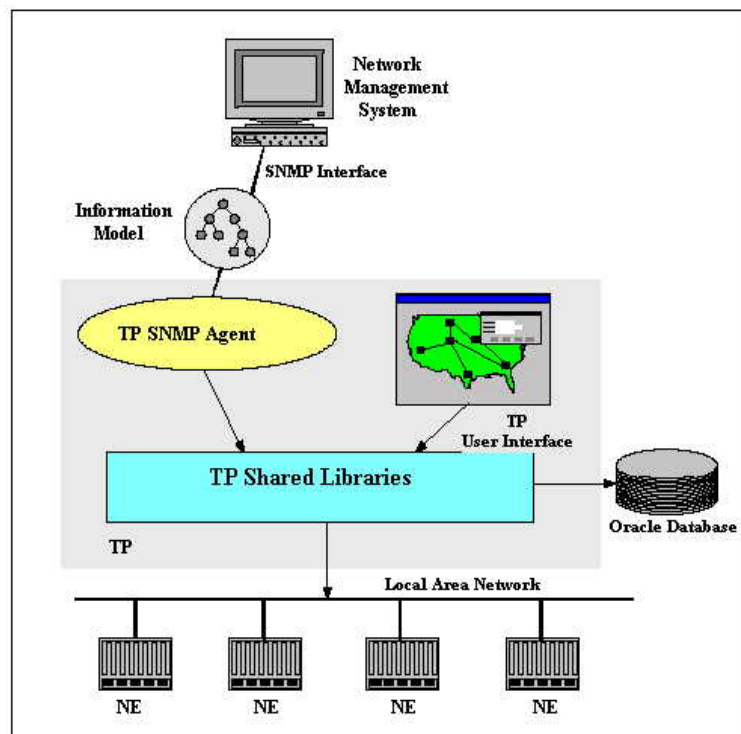
The TP SNMP agent works as a proxy agent, translating the requests and responses between the external SNMP manager and the TimePictra Element Management System.

The TP SNMP Agent translates (as required) the information (commands, data, status information, events, etc.) that passes between TP software and a higher-layer network management system. The Agent provides the following functions:

- Allows higher-layer manager to access upto 1500 network elements (NEs).
- Enables the manager to perform standard SNMP GET and SET operations as per the information model.
- Translates TP-generated events to SNMP traps so that the manager can process them.

Figure 1 shows that within the TP application, the Agent interacts with other modules using the TP Shared Libraries.

Figure 1. The Information Model and TimePictra



In a general sense, the Agent has two main functions - forwarding of events (event forwarding) and handling requests. Event forwarding involves the processing and forwarding of events from network elements and the system itself to the higher-layer manager. Request handling involves the processing of GET/SET requests between the higher-layer manager and the system or network elements.

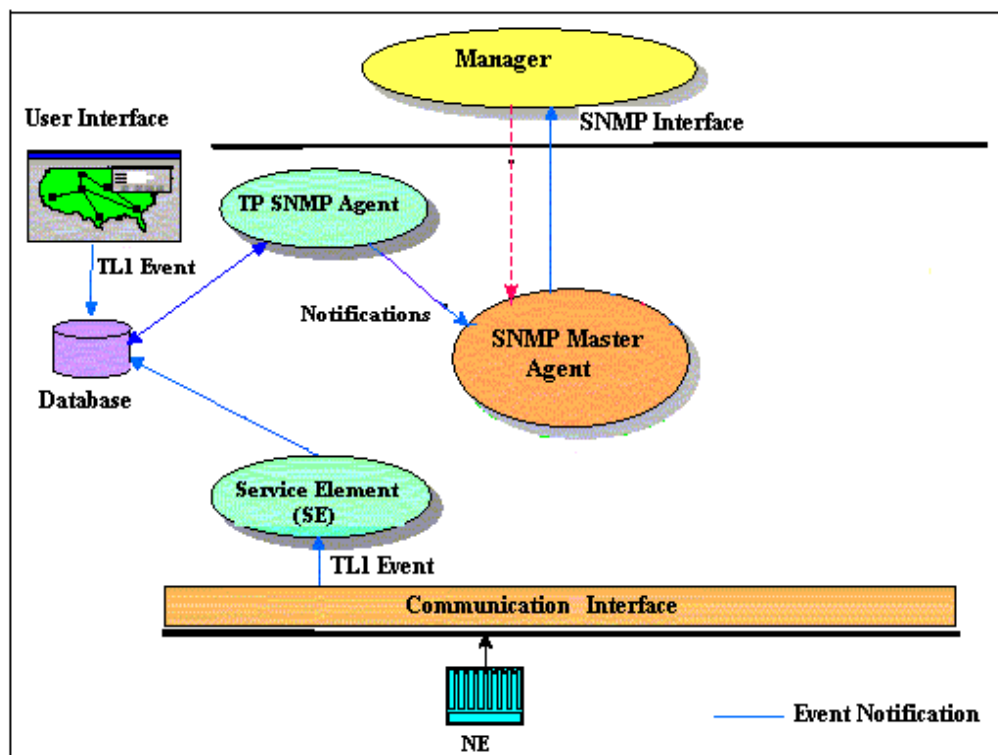
Event Forwarding

The Agent application may emit traps, which could be either due to change on the NE side or due to the change on the database side. In the TimePictra model, the database first receives events from various sources and places those events into corresponding tables. Then the DBAgent, which is a part of TimePictra application, forwards those events to Trap SubAgent. The Trap Subagent maps these events to SNMP traps and dispatches to the configured managers.

In the TP event model shown in Figure 2, the database does the following in the order shown:

- Receives TL1 events from the ServiceElement (SE) or the user interface.
- Processes them.
- Notifies the TP SNMP Agent of the events.

Figure 2. TimePictra Event Model



Events and Traps can be classified under the categories shown in Table C

1 Table C: Events and Traps

Event/ Trap	Description
NE Alarms	These are the alarmed events generated by the NEs
NE Events	These are the non-alarmed events generated by the NEs
SystemAlarms	These are alarmed events generated by TP
SystemEvents	These are non-alarmed events generated by TP
NE Creation/Deletion	Network Element Creation/ Deletion traps will be emitted for NEs
Attribute Value Change	Traps generated whenever there is any change in the attributes
All Attribute Value Change	Any change in the configuration parameters of NE generates these traps
ErrorMessage	These traps are generated when there is an error message from GES Package

Handling Requests

The Agent receives SNMP requests from the manager over SNMP-UDP Stack. The request will be for a GET or SET operation on the NE. The Agent validates these requests based on the community name and if valid, sends it to the TimePictra application.

After getting the response from the TP, Agent builds the corresponding SNMP responses and sends it to the requesting manager.

Information Model

All information supported by TP SNMP is modeled in the TP SNMP MIB. Figures 3 and 4 show the MIB structure.

Figure 3. TimePictra SNMP MIB Structure (1 of 2)

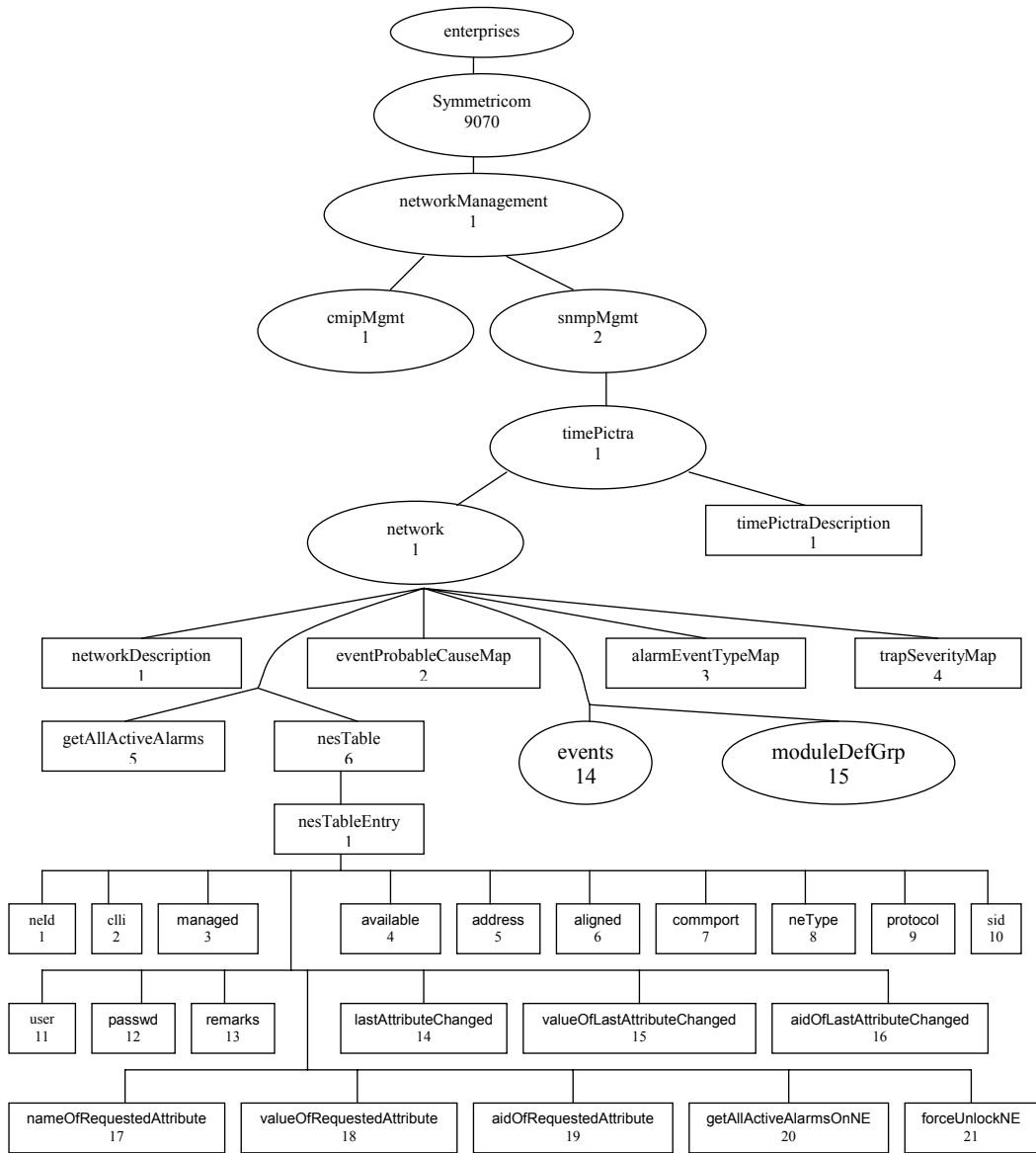
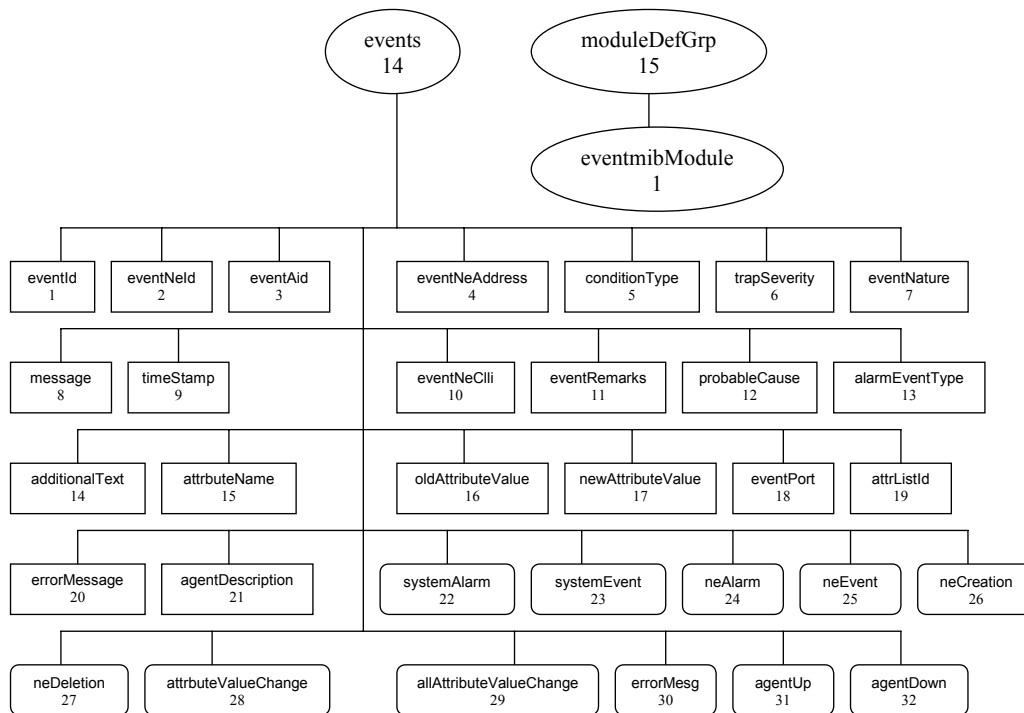


Figure 4. TimeScan SNMP MIB Structure (2 of 2)



FAQ Regarding the MIB

What is eventmibModule and moduleDefGrp in generic SNMP Mib?

We organized our Generic MIB definitions as a group of MIB modules. Eventsmibmodule (a MODULE-IDENTITY) contains the trap and related definitions. The module moduleDefGrp is an object identity under which we register all other MIB modules. In the future, if we want to create a module, we can create it and register it under moduleDefGrp.

What is 'events' and NOTIFICATION-TYPE?

It may seem that sub-attributes of a 'notification-type' should fall under the 'notification-type' but in the actual Mib declaration both fall under 'events' object-identity.

NOTIFICATION-TYPE is a macro from standards denoting that the definition is a trap. 'events' is an object identity registered to keep all the information related to traps. We will register all the traps and related attributes under events.

What are OBJECT-TYPE, OBJECT-IDENTITY and MODULE-IDENTITY?

The OBJECT-TYPE construct is used to define an object type. An object type is a class of management information or a mechanism to organize related object types. This construct is used to define table, row, columnar and scalar objects.

The OBJECT-IDENTITY construct is used to assign an OID value to an object identifier in a MIB Module.

The MODULE-IDENTITY construct is used to specify information about SNMP MIB modules. This includes revision history, name of the organization which has authority over definitions, contact for tech queries, etc.

Is it possible to acknowledge an active alarm on TimePictra using an SNMP?

It is not possible to acknowledge an active alarm on TimePictra through SNMP Agent. Managers can only view the alarms emitted by SNMP Agent. This feature is not supported in current agent implementation.

How do we collect performance data from the SSUs via the SNMP Mib?

Current SNMP MIB does not have objects to query performance-related data for a particular NE. This feature is not supported in current agent implementation.

Can TL1 Command Bundles be triggered via SNMP interface?

This feature is not supported in current agent implementation.

What attributes can be set via SNMP on each element?

All attributes that are settable via the standard TimePictra "Configuration View Modify" interface, are settable via the SNMP interface also. For example, we can set the following attributes of ITH card for 55400 NE through SNMP Agent:

DSCTIME, HFQLEVL, MANCHAN, PIRANGE, REVERT, SPRDCHN, SYNCMDE', 'WTRSS', etc.

All the NETYPES (TS, HP4, HP5, etc.) that are managed by TimePictra are accessible from SNMP Agent.

Does SNMP MIB provide status of the 'Resiliency' machines?

This feature is not supported in current agent implementation.

I cannot find 'attrNameListId' in the MIB file 'event-mib.my'.

attrNameListId is used in 'event-mib.my' but defined in another mib file called 'timepictra.my'. MIB Attribute 'attrListId' (OID: 1.3.6.1.4.1.9070.1.2.1.1.14.19) is also used in Event 'errMesg'.

What is 'errorMesg' event?

When you get an 'errorMesg' event, it means the SNMP GET/SET operation performed from the SNMP Manager (e.g., NetCool, HP OpenView, etc.) has failed. This event tells the NetCool user "what" failed and "why" it failed. In that instance, the NetCool NMS user has to check TimePictra EMS to get into specifics and analysis. SNMP protocol has some limitations, and that is why this innovation was developed: to send error information back (to SNMP Manager) with errorMesg Event. If the GET/SET failed, the "errorMessage" will have the attributeName on which the operation has failed.

What is 'eventNeClli' and 'eventNeId'?

'eventNeClli' (INTEGER) (1.3.6.1.4.1.9070.1.2.1.1.14.2) is the unique alphabetic (can have numbers in it) name a customer sees on the launch pad or maps. It is a unique name given to a specific network element.

'eventNeId' (OCTET_STRING) (1.3.6.1.4.1.9070.1.2.1.1.14.10) is a unique numeric ID used inside TimePictra and not as useful to a customer as 'eventNeClli'. It is a unique numeric ID given to a specific network element.

How can a customer uniquely identify a specific alarm or event?

For a customer's own logical ID for a event or alarm, just using 'eventId' is enough but one can also use 'eventId + eventNeClli + eventAid + conditionType' for more clarity and information.

Can 'eventId' be used to match a clear event with the related alarm or event?

No, 'eventId' uniquely identifies any event, be it clear event, normal event, or alarm. To match a clear event with related alarms/events, one has to match "eventNeClli + eventAid + conditionType" between the alarm/event and the clearing event. If a customer's logical id primary purpose is to match clear with event/alarms, then the logical id should have "eventNeClli + eventAid + conditionType".

What is "getAllActiveAlarms"?

When a manager does an SNMP GET on variable "getAllActiveAlarms", for all NEs (Network Elements), all alarms present in TimePictra are reported by the SNMP Agent to the SNMP Manager. It is important to note the alarms are not queried directly from the NEs themselves because the TimePictra database (from where the alarms are picked) is always current with the all the active alarms on the NEs.

Can a manager distinguish automatic alarms and ones that come by doing SNMP GET on variable "getAllActiveAlarms"?

No, this feature is not in the current SNMP Mib, but "all" such synchronization alarms (that come from by doing SNMP GET on variable "getAllActiveAlarms") should arrive to MOM (Manager or Managers) within seconds after MOM makes the GET request. Note that the word *synchronization* is not used in the context of timing and frequency products.

Responsibilities of the System Administrator

The System Administrator is responsible for maintenance of the TP system and the Agent.

The main responsibilities of the system administrator are as follows:

- Installing the Agent Software.
- Configuring the Agent.
- Ensuring TP and the SNMP agents are running correctly.

System Requirements

1

The hardware and software described in the following sections is required to run the Agent.

Software Requirements

In addition to the software requirements detailed in the section entitled "System Requirements" in the TimePictra Software System Administrator's Guide, the Agent requires Master Agent. The Master Agent is the agent protocol engine and performs the authentication, authorization, access control, and privacy functions. The EMANATE Master Agent comes with EMANATE tool kit 15.x which receives both SNMPv1 and SNMPv2 traps. (This Agent is provided and used with the TimePictra SNMP Option)

Hardware Requirements

The Agent runs on the same workstation on which the TimePictra software runs. Refer to the TimePictra System Administrator's Guide for information on the hardware required to run TimePictra Software.

Prerequisite Knowledge

The procedures in this manual assume that the system administrator is experienced in HP-UX 11.xx, Master Agent, and TP administration. This knowledge is useful, and in some cases, necessary when performing tasks in this manual.

Related Documentation

1

Some procedures in this document may refer you to information that is contained in the TimePictra System Administrator's Guide.

Installation

This chapter provides installation information.

In This Chapter

The procedures in this chapter explain how to do the following:

- Install the TimePictra SNMP Option
- Uninstall the TimePictra SNMP Option
- Start SNMP Agents
- Stop SNMP Agents
- SNMP Configuration files
- Enable Tracing

The procedures in this chapter assume that the following is true.

- TimePictra is installed, configured and running correctly.
- The Administrator has sufficient knowledge and experience with HP-UX 11.xx, TimePictra, and the system hardware.

Note: TimePictra version 2.0 is a prerequisite for the SNMP option. Before attempting to install the SNMP Option, ensure that the TimePictra Software version 2.0 is installed and running

Overview

The installation program, `swinstall`, does the following:

- Checks for hardware/software dependencies.
- Copies the Agent's files, to their respective directories. The Agent will be installed in the directory `/opt/osmf/SNMP`. The following directory structures will be created for the SNMP Agent under the directory `/opt/osmf/SNMP`:

`/opt/osmf/SNMP` (Main Directory)

`/opt/osmf/SNMP/bin` (Agent executable)

`/opt/osmf/SNMP/config` (contains configuration files)

`/opt/osmf/SNMP/mibs` (contains the mib files)

`/opt/osmf/SNMP/utils` (contains scripts)

`/opt/osmf/utils` (contains script *tpagent*)

- Modifies the TimePictra database to flag the availability of the SNMP option.
- Registers the Agent with the Master Agent.
- Configures the boot/shutdown sequence for the SNMP Option.

Installing the TimePictra SNMP Agent

To install the Agent, use the Software Distributor, as described in the following procedure.

Prerequisites

1. TimePictra must be already installed.
2. TimePictra database must be running.
3. TimePictra SNMP Option CD is available.

Procedure A. Installing the SNMP for TimePictra

Step	Action
1	Start a shell with user root.
2	Type the following commands to start the PFS daemons: <pre>/usr/sbin/pfs_mountd & /usr/sbin/pfsd &</pre>
3	Edit the file <code>"/etc/pfs_fstab"</code> to contain the following entry: <pre>/dev/dsk/c1t2d0 /SD_CDROM pfs-rrip xlat=unix 0 0</pre> Where <code>/dev/dsk/c1t2d0</code> is the special device file for the CD-ROM drive. <i>Note:</i> If the special device file for your system is different from that described above, make changes accordingly.
4	Type the following command to give read/write permission to the root user for the <code>pfs_fstab</code> file: <pre>chmod 775 /etc/pfs_fstab</pre>
5	Type the following command to mount the CD onto the system: <pre>/usr/sbin/pfs_mount /dev/dsk/c1t2d0 /SD_CDROM</pre> Where <code>/dev/dsk/c1t2d0</code> is the special device file for the CD-ROM drive. <i>Note:</i> If the special device file for your system is different from that described above, make changes accordingly.
6	Start UNIX software installer by entering the following command at prompt: <pre>/usr/sbin/swinstall</pre>

.....

Procedure A. Installing the SNMP for TimePictra (Cont'd)

Step	Action
7	Click on Source Depot Path , then enter <code>"/cd_mount_dir/DEPOT,"</code> then click OK. <i>Note:</i> <code>cd_mount_dir</code> is the directory where the TimePictra installation depot exists.
8	In the Software Selection window, highlight Depot, then click on Actions>Install Analysis . Install analysis should begin and then complete with a status of Ready. If the analysis fails, examine the logfile and rectify any problems that exist before proceeding.
9	After install analysis completes, click DONE , then click Yes to begin the installation. After Yes is clicked, the installation process starts. This phase should complete with no errors.
10	When the status shows Completed and Percent Complete=100%, click Done. <i>Note:</i> If the installation fails, examine the logfile and rectify any problems that exist.

End of Procedure



Removing the TimePictra SNMP Agent

This is a destructive procedure and users must be very careful, as it removes the product and all relevant data.

Uninstalling TimePictra SNMP Option

Uninstall procedure is performed using the standard Unix package removal script: "swremove".

To successfully remove TimePictra SNMP Option, check that the TimePictra Database is running and all the SNMP daemons are down.

To uninstall the Agent follow the steps in Procedure B.

Procedure B. Procedure to start the SNMP Agent

Step	Action
1	Log onto the server and start a shell with a User root
2	Source the environment by executing the following command: <code>./opt/osmf/config/env/osmf-db.env</code>
3	Execute the following command to stop SNMP daemons running on the server: <code>tpagent stop SNMP</code> This would stop all SNMP processes.
4	Start Unix uninstaller by executing the following command at the prompt: <code>/usr/sbin/swremove</code> (this displays the list of all the products installed on the server)
5	On the GUI that comes up, select TimePictra SNMP Option and click on Action > remove analysis.
6	If analysis goes through successfully, click on Done to start TimePictra SNMP Option removal. Click Yes > to proceed with removal. If removal analysis fails, go through the logfile and take corrective actions.

End of Procedure

Configuring the Agent

Master Agent reads its configuration information from the file `/opt/osmf/SNMP/config/snmpd.cnf` when starting.

- Configuring the Agent for SNMP Research's EMANATE Master Agent
 - Customizing the Configuration file: By default any manager can do GET/SET operations. To receive the traps, the trap destination should be configured properly.
 - Modify the keyword line “snmpTargetAddrEntry” to use the IP address of machine to receive SNMP traps from TimePictra. Only the IP address should be changed.

Example: 192.168.5.211:162 changed to
15.1.153.65:162

- Set the start flag to 0 in the following configuration files (if they exist):
 - `/etc/rc.config.d/SnmpTrpDst`
 - `/etc/rc.config.d/SnmpHpunix`
 - `/etc/rc.config.d/SnmpMaster`
 - `/etc/rc.config.d/SnmpMib2`
- Ensure that the port used by the SNMP Agent is in the `/etc/services` file. The default entry is shown below:
 - `snmp-trap 162/udp trapd #Simple Network Management Protocol Traps`
- Stop any existing SNMP daemons if running

Starting The Agent

Startup and shutdown process of the Master Agent and Sub Agent are integrated with system boot and system shutdown. If you want to start the agent manually, follow the steps given below.

Master Agent

1. Ensure that SNMP ports are defined in the **/etc/services** file. Type the command (this command must be run from Korn shell [ksh]). The user should be a root user.

```
grep "snmp" /etc/services
```

Should result in the output:

```
snmp 161/udp
```

```
snmp-trap 162/udp
```

2. Start a shell with user root.

3. Enter the following command to source the right environment:

```
. /opt/osmf/config/env/osmf-db.env
```

4. Enter the following command to start Agent:

```
tpagent start SNMP
```

Note: If any errors are encountered, refer to the section titled "Troubleshooting Hints".

Stopping the Agent

1. Start a shell with user root.
2. Source the environment by entering the following command:
 - **`/opt/osmf/config/env/osmf-db.env`**
3. Enter the following to stop the Agent:
`tpagent stop SNMP`

Enable Tracing

In the SNMP Agent, two types of tracing can be enabled:

- TP Tracing.
- Master Agent Tracing.

Note: Tracing should only be used for short periods of time or troubleshooting. Large amounts of data can be generated with tracing and may affect disk space if left running.

TimePictra Tracing

To enable TimePictra tracing follow the specified instructions in Procedure C.

Procedure C. TimePictra Tracing

Step	Action
1	If the agent is already running, stop the agent with the following command as user root: <code>tpagent stop SNMP</code>
2	Export the following environment variables: a. SV_TRACEMASK: This variable specifies the global mask for trace output. For 'SNMPAgent' specify the value as 0x4000. b. SV_TRACELEVEL: This variable specifies the level of trace information to record. For 'SNMP Agent' specify the value as 07. c. The variable SV_TRACEFILE specifies the output file to output the trace information. This variable is set to <code>/var/opt/osmf/share/log/tpsnmpd.trc</code> file within the agent code. So this variable need not be exported.
3	Start the Agent with the command: <code>/opt/osmf/SNMP/utis/tpsnmpd.ks start</code>

End of Procedure

Special Features and Limitations of the Agent

In this section the special features supported by the Agent and any known limitations are explained.

Chapter 3

Special Features

A simple SNMPSET sets a list of attributes in the NE and not a single attribute of interest, but here you can set the value of single attribute. The manager needs to know about the current alarm status in order to SYNC up with the Agent. Therefore the snmpget, which basically has the functionality of retrieving all the attribute values, has been modified to get all the active alarms and alarms specific to a requested NE.

SET a Single Attribute

A single attribute value can be set. To set a value of a single attribute of the NE, send the SET request in the following format:

The syntax is: **snmpset <ipaddress/hostname> <attribute aid> <ne_id> <aid> <attr_name_list_id> <attribute type> <"attribute name=attribute value">**

For example: To set attribute ECHO with the value ON. The set command should be given as below:

```
snmpset 134.15.15.7  
1.3.6.1.4.1.167.1.1.1.2.4.54.5.67.79.77.45.49.8.84.83.51.48.45.67.79.77.  
Octetstring "ECHO=ON"
```

Get getAllActiveAlarms Attribute

When the manager sends a get request for an attribute, the agent polls the current alarms table. If there are any alarms there in the table the agent emits all the traps corresponding to each alarm.

The syntax is: **snmpget <ipaddress/hostname> <attribute oid>**

Get getAllActiveAlarmsOnNE Attribute

When the manager sends a get request for an attribute, the agent polls the current alarms table. If there are any alarms there in the table on the NE requested, the agent emits traps corresponding to each alarm.

The syntax is: **snmpget <ipaddress/hostname> <attribute oid.NEindex>**

Limitations of the Agent

To get a single attribute value of a particular NE from the database is not supported in this version.

.....

This page intentionally left blank.



Troubleshooting

This chapter provides solutions for few common problems, which the user may come across during the application usage.

Troubleshooting Hints

Table 1: Troubleshooting Hints

Common Errors	Cause and Corrective Action
General Errors	
Failure in Get/set	<p>Case 1 Configuration errors in Master Agent Configuration file. Case 2 Problem with GES package.</p> <p>Corrective Action 1 Stop the SNMP Agent Stop Master Agent Open Master Agent configuration file and configure the community names properly. Refer to the section entitled "Configuring the Agent" Start Master Agent and SNMP Agent.</p> <p>Corrective Action 2 Install the GES package Run the script: <code>./opt/osmf/DB/mv/install_ges.ks</code></p> <p><i>Note:</i> This script must be run as 'otroot' user.</p>
Failure in receiving Traps	<p>Case 1 Master Agent configuration issues. Case 2 DBAgent is not up. Case 3 Entries in the env table are not set.</p> <p>Corrective Action 1 In the Master Agent configuration file, configure the trap destinations properly. Refer to the section, "Configuring the Agent".</p> <p>Corrective Action 2 Start the DB Agent.</p> <p>Corrective Action 3 Execute the following Scripts: <code>./opt/osmf/SNMP/utis/tp_snmpflag.ks</code> <code>./opt/osmf/DB/trlog/trlog.ks enable</code></p>
System Generated	<p>Case 1 Events are not logging into tpm.</p> <p>Corrective Action 1 Enable the trlog triggers. Execute the script: <code>./opt/osmf/DB/trlog/trlog.ks enable</code></p>

Table 1: Troubleshooting Hints (Cont'd)

Common Errors	Cause and Corrective Action
NE Generated	<p>Case 1 Events are not logging into tpm.</p> <p>Corrective Action a Start the DB jobs. Execute this command from the SQL prompt: @/opt/osmf/admin/osmf_db_jobs.run</p> <p>Corrective Action b Enable the triggers AFTER_INS_UPD_CURRENT_ALARMS and AFTER_INS_HISTORIC_EVENTS. Execute the following command from the SQL prompt: @opt/osmf/DB/mv/aa.trg</p>

.....

This page intentionally left blank.



Traps and Fields

App. A

Traps and Fields

Table 2: Traps and Fields

Occasion/Event of occurrence of Traps	Emitted Traps	Fields
Error message from GES Package.	ErrorMessage Trap	Event Neld EventAid AttributeListId EventClli Error Message
Change in the configuration parameters of NE	AllAttributeValueChange Trap	EventNeld EventNeAddress EventNeClli EventAid AttributeListId NewAttributeValue
Change in the attributes of nesTable, cardsTable, almEvtTable, inputChannelTable, portTable, thresholdsTable, or tl1CmdsTable.	AttributeValueChange Trap	EventId EventNeld EventNeAddress EventNeClli EventAid AttributeListId AttributeName OldAttributeValue NewAttributeValue
NE deletion.	NE Deletion Trap	EventNeld EventNeAddress EventNeClli
NE Creation	NeCreation Trap	EventNeld EventNeAddress EventNeClli
An event from NE with event severity of none, noalarm, or clear	NeEvent Trap	EventId EventNeld EventNeClli EventNeAddress EventAid EventPort Event Severity Event Nature Condition Type Message TimeStamp

A

Table 2: Traps and Fields (Cont'd)

Occasion/Event of occurrence of Traps	Emitted Traps	Fields
An event from the NE with event severity of major, minor, or critical.	NeAlarm Trap	EventId EventNeld EventNeClli EventNeAddress EventAid EventPort Event Severity Event Nature Condition Type Message TimeStamp
An event from TimePictra Software with event severity of none, noalarm, or clear	SystemEvent Trap	EventNeld EventId EventNeAddress EventNeClli EventAid EventPort Event Severity Event Nature Condition Type Message TimeStamp
An event from TimePictra Software with event severity of major, minor, or critical.	SystemAlarm Trap	EventId EventNeld EventNeAddress EventNeClli EventAid EventPort Event Severity Event Nature Condition Type Message TimeStamp

If this chapter is used for Specifications, the specifications of the equipment are included.

.....

This page intentionally left blank.

