+44(0)1425 270 333
email: sales@dtrack.com
website: dtt.dtrack.com

Overview of Applications

for

Tracker 27xx Series

Data Track Technology Ltd
153 Somerford Road Christchurch Dorset BH23 3TY UK

Application List

INTRODUCTION

The Tracker 2700 range features a powerful scripting capability that enables a whole variety of application specific scripts to be run on the Tracker platform. These applications allow users to provide a number of value added services as well as the local management of devices to reduce break/fix costs and reduce system downtime. This document provides a brief description of some of these applications

PBX ALARM APPLICATIONS

Alcatel 4400 Maintenance Alarms

This Tracker application monitors serial alarm data output from an Alcatel 4400 switch. It identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. The Alcatel 4400 alarms can be configured to be output spontaneously on a nominated serial port by a configuration setting on the switch.

Alcatel 4400 Network Toll Fraud

The application monitors the CDR output from the 4400 via an Ethernet link, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Alcatel 4400 Serial Toll Fraud

The application monitors the CDR output from the 4400 via a serial link, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Alcatel OmniPCX 4400 SNMP Alarms

This application processes SNMP traps from the Alcatel OmniPCX PBX or the earlier 4400 hardware provided it is running software release 4 or later. For any OmniPCX 4400 that has been configured to deliver its SNMP traps to the Tracker, this application will accept the traps, filter them using a set of predefined rules and deliver the alarm content as a Tracker alert to a central management system.

Avaya Definity Call Processing

This application reads Definity call records on serial1 and passes them out on serial2 after internal processing to update the call date and billing information as defined in the associated configuration files.

Note: This application is only supported by the Tracker 2700 and Mitel 7100 MAP variants of the Tracker product.

Avaya Definity INADS Alarm Reporting

This application requires two internal modems to be fitted in the Tracker; one to receive alarms from the Definity's internal modem and the other to re broadcast the message once filtered. The application monitors one of the Tracker's internal modems waiting for an INADS alarm dial-out from the Definity. When a valid

message is received, the application identifies key fields within the alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system.

Avaya Definity Toll Fraud Reporting

The Toll Fraud application supports the legacy Avaya Definity running software from release 7 as well as later Avaya IP products running MultiVantage software including DefinityServer, MediaServer and MediaGateway.

While the legacy Definity outputs CDR data via a serial port, the newer IP products output via IP to a remote host 'server'. The IP address and listening port on the server is configurable on the Definity. There are two protocol options for the IP CDR output: No protocol and 'Reliable Session Protocol' (RSP). At the time of writing, RSP is not fully supported by Avaya and therefore not supported in the Tracker.

The CDR record format is customisable on the Avaya system using the 'CDR System Parameters' settings. This application supports the following CDR formats:

- Standard Printer format.
- International Direct format.
- Data Track Customised format.

The application monitors the CDR output, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Avaya Media Server Maintenance Alarms

This application processes Avaya Media Server SNMP traps as defined in the Avaya G3-AVAYAMIB Version 3.1.1. At the time of issue, the following Media server product families are supported: S83xx, S85xx and S87xx. The Media Server must be configured to deliver traps to the Tracker. This application will accept traps from the Media Server, filter them using a set of user-defined rules and deliver the alarm content as a Tracker Alert to a central management system.

The process of dealing with the traps is split into two parts: trap capture and alarm reporting. Trap capture receives the trap from the Media Server and converts it into a textual form suitable for processing by the alarm reporting application. Trap capture is provided by the trapcatd process that runs independently of the alarm reporting application and provides trap information on an internal device readable by the alarm reporting application.

The Alarm Reporting application reads each text message from the device provided by trapcatd, identifies key fields and applies a set of user-defined rules to determine if an alert should be delivered to the central management system.

Avaya SDX Maintenance Alarms

This Tracker application monitors serial alarm data output from an Avaya SDX switch. It identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. The Avaya SDX alarms can be configured to be output spontaneously on a nominated serial port by a configuration setting on the switch.

Ericsson MD110 Alarm Reporting

The application monitors alarm data output from the MD110, identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. The recommended interface is via one of the V24 Ports at the rear of the MD110.

MD110 alarms are output in the form of a spontaneous report printout. Each report includes header information which identifies the reporting device, software version, date and time. Within the report there will be one or more alarm messages classified by Alarm class. This application processes the report and extracts each of the alarms it contains.

Ericsson MD110 Toll Fraud Reporting

The application monitors the CDR output from the MD110, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

HMGCC Chubb Alarm Monitoring

The Chubb alarm comprises a multi-line record. Each record starts with a space padded alarm ID number followed by the date, the time and an optional descriptive text split over a number of lines. The application monitors the output from the Chubb device, validates correctly formatted alarm records, extracts key fields from within each record and then applies a set of user-defined rules to determine if the alarm should be delivered to a central management system.

Intel PBX IP Media Gateway SNMP Alarms

This application processes SNMP traps from the Intel PIMG devices that have been configured to be delivered to the Tracker. This application will accept the traps, filter them using a set of user defined rules and deliver the alarm content as a Tracker alert to a central management system.

Interactive Intelligence Communite SNMP Alarms

This application processes SNMP traps from the Interactive Intelligence Communite Voicemail/ Unified messaging product. In this document we shall refer to the product as Communite. For any Communite system that has been configured to deliver its SNMP traps to the Tracker, this application will accept the traps, filter

them using a set of predefined rules and deliver the alarmcontent as a Tracker alert to a central management system.

Intertel AXXESS Alarm Monitoring

The application monitors diagnostic messages output from the Intertel Axxess system, identifies key fields within each message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. The Axxess system can be configured to output diagnostic messages via a local serial port or via a TCP port on the local Network. This application supports both output options.

Intertel AXXESS Toll Fraud Reporting

The application monitors the CDR output from the AXXESS, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Mitel 3100 ICP Alarms

This application processes Mitel 3100 ICP SNMP Alarm notification traps that are delivered to the Tracker. The process of dealing with the traps is split into two parts: Trap capture and Alarm reporting.

Trap capture involves receiving the trap from the 3100 ICP and converting it into a textual form suitable for processing by the Alarm reporting application. The 3100 ICP must be configured to deliver its SNMP traps to the Tracker.

Alarm reporting involves reading each text message, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system. In the case of the Mitel 3100 ICP, this is the 3100 ICP Alarm Reporting Application.

Mitel 3300 ICP Maintenance Alarm Reporting

This application processes Mitel 3300 ICP Maintenance Alarms output on TCP port 1751. The 3300 ICP must be configured to output maintenance alarms.

The application makes use of the Tracker TCP data logging facility to collect the alarms from the 3300 ICP. The data logging process makes the alarm data available to the application in the form of an internal device within the Tracker 2700.

Alarm reporting involves reading each entry in the alarm output, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system.

Mitel 3300 ICP SNMP Alarms

This application processes Mitel 3300 ICP SNMP Alarm notification traps that are delivered to the Tracker. The process of dealing with the traps is split into two parts: Trap capture and Alarm reporting.

Trap capture involves receiving the trap from the 3300 ICP and converting it into a textual form suitable for processing by the Alarm reporting application. The 3300 ICP must be configured to deliver its SNMP traps to the Tracker.

Alarm reporting involves reading each text message, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system. In the case of the Mitel 3300 ICP, this is the 3300 ICP Alarm Reporting Application (m3300snmp.app).

Mitel SX2000 Call Processing

This application reads Mitel SX2000 PABX call records on serial1 and passes them out on serial2 after internal processing to update the call date and billing information as defined in the associated configuration files.

Note: This application is only supported by the Tracker 2700 and Mitel 7100 MAP variants of the Tracker product.

Mitel SX2000 Serial Alarms

This Tracker application monitors serial alarm data output from a Mitel SX2000 switch. It identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system.

Mitel SX2000 SNMP Alarms

This application processes Mitel SX2000 SNMP Alarm notification traps delivered to the Tracker. The process of dealing with the traps is split into two parts: Trap capture and Alarm reporting.

Trap capture involves receiving the trap from the SX2000 and converting it into a textual form suitable for processing by the Alarm reporting application. The SX2000 must be configured to deliver its SNMP traps to the Tracker.

Alarm reporting involves reading each text message, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system. In the case of the SX2000 this is the SX2000 Alarm Reporting Application (sx2000snmp.app).

Mitel SX2000 Toll Fraud Reporting

The application monitors the CDR output from the SX2000, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Nortel BCM SNMP Alarms

This application processes Nortel BCM SNMP Alarm notification traps delivered to the Tracker. The process of dealing with the traps is split into two parts: Trap capture and Alarm reporting.

Trap capture involves receiving the trap from the BCM and converting it into a textual form suitable for processing by the Alarm reporting application. The BCM must be configured to deliver its SNMP traps to the Tracker.

Alarm reporting involves reading each text message, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system. In the case of the BCM this is the Nortel BCM SNMP Alarms Application (bcmal.app).

Nortel Meridian Alarm Reporting

The application monitors serial alarm data output from the Meridian, identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. Meridian alarms can be configured to output spontaneously on a nominated V24 port by system programs running on the switch. Some of these programs, such as the Error Monitor, are permanently resident while others are more diagnostic in nature and are loaded only when required. It is also possible to configure the meridian to load and run a set of diagnostics automatically as part of a daily routine. Once loaded, each program generates a specific set of alarms or messages.

From Meridian software release 25 an alternative formatted or ‘fancy’ format output is available. This application supports both formatted and unformatted Meridian alarms.

Nortel Meridian Call Server SNMP Alarms

This application processes Nortel Meridian SNMP Alarm notification traps delivered to the Tracker. The process of dealing with the traps is split into two parts: Trap capture and Alarm reporting.

Trap capture involves receiving the trap from the Meridian and converting it into a textual form suitable for processing by the Alarm reporting application. The Meridian must be configured to deliver its SNMP traps to the Tracker.

Alarm reporting involves reading each text message, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system. In the case of the Meridian this is the Nortel meridian Alarms Application (maridianal.apps).

Nortel Meridian Call Processing

This application reads Nortel Meridian PABX call records on serial1 and passes them out on serial2 after internal processing to update the call date and billing information as defined in the associated configuration files.

Note: This application is only supported by the Tracker 2700 and Mitel 7100 MAP variants of the Tracker product.

Nortel Meridian Toll Fraud Reporting

The application monitors the CDR output from the Meridian, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Meridian call logging output can be configured to output on a nominated V24 port. There are two formats supported: 'old' format and 'new' format. Meridian systems running software release 16 or later tend to be set to the 'new' format.

Nortel Meridian Passport 4400 Alarm Reporting

This application processes Meridian Passport 4400 series SNMP alarm notification traps delivered to the Tracker. The 4400 series software comprises a number of discrete modules each of which generate their own traps. This application will accept traps from any module that conforms to the standard 4400 trap. The process of dealing with the traps is split into two parts: trap capture and alarm reporting.

Trap capture receives the trap from the Passport 4400 and converts it into a textual form suitable for processing by the alarm reporting application.

The Alarm Reporting application reads each text message from the device provided by trap capture, identifies key fields and applies a set of user-defined rules to determine if an alert should be delivered to the central management system.

Nortel Meridian Passport 6400 Alarm Reporting

This application processes Meridian Passport 6400 and 7400 series SNMP alarm notification traps delivered to the Tracker. The Passport generates 6 different traps each of which represents different alarm severity ranging from 1 (critical) through to 6 (unknown). This application will accept traps from any Meridian Passport 6400/7400. The process of dealing with the traps is split into two parts: trap capture and alarm reporting.

Trap capture receives the trap from the Passport 6400/7400 and converts it into a textual form suitable for processing by the alarm reporting application.

The Alarm Reporting application reads each text message from the device provided by trap capture, identifies key fields and applies a set of user-defined rules to determine if an alert should be delivered to the central management system.

Nortel Meridian Processor Load Monitoring

A Meridian can be configured to deliver various reports that show how it is performing. One of these is TFS004 which details the Meridian Processor loading figure and percentage real-time utilisation (%RTU). The Meridian

can be configured to deliver this report to any V24 port (usually the maintenance port) at fixed time intervals up to a maximum rate of every half-hour. The Tracker application monitors the output from the Meridian port and applies a set of user-defined rules to determine if the report should be delivered to a central management system.

Nortel Meridian CallPilot SNMP Alarms

This application processes SNMP alarm notifications from the Meridian CallPilot voicemail system. The process of dealing with the Meridian CallPilot traps is split into two parts: trap capture and alarm reporting.

The application accepts traps from the CallPilot and converts them into a textual form suitable for processing. The application then filters them using a set of user-defined rules and determines whether an alert should be delivered to a central management system.

Nortel Meridian IP Trunk and Line SNMP Alarms

Meridian IP Line Cards (also known as ITG, Internet Telephony Gateway) enable integrated voice and data services on the Meridian LAN with connectivity between sites provided by IP Trunk cards.

The application first converts the traps in to a textual form, secondly, it identifies key fields and applies a set of user-defined rules to determine if an alert should be delivered to the central management system.

Nortel Succession CSE1000 SNMP Alarms

This application processes SNMP asynchronous alarm traps from the Succession Call Server 1000. The application supports Succession CS1000 software releases 2, 3 and 4. This application will accept traps, filter them using a set of user-defined rules and deliver the alarm content as a Tracker Alert to a central management system.

The application accepts traps from the Succession 1000 and converts them into a textual form suitable for processing. The application then filters them using a set of user-defined rules and determines whether an alert should be delivered to a central management system.

Riello Multiswitch SNMP Alarms

This application processes SNMPv1 asynchronous alarm traps from the Riello Multiswitch automatic transfer switch. The application will capture the traps, filter them using a set of user defined rules and deliver the alarm content as a Tracker alert to a central management system.

The application accepts traps from the Riello Multiswitch and converts them into a textual form suitable for processing. The application then filters them using a set of user-defined rules and determines whether an alert should be delivered to a central management system.

Siemens EMS 601 Alarm Reporting

This Tracker application monitors alarm data output from the EMS 601, identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. The recommended interface to the PBX is via one of the V24 Ports at the rear of the PBX.

Siemens EMS 601 Toll Fraud Reporting

The application monitors the CDR output from the EMS 601, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Siemens Hicom 300E Alarm Reporting

This Tracker application monitors alarm data output from the Hicom 300E, identifies key fields within each alarm message and applies a set of user-defined rules to determine if the message should be delivered to a central management system. The recommended interface to the PBX is via one of the V24 Ports at the rear of the PBX.

Siemens Hicom 300E Toll Fraud Reporting

The application monitors the CDR output from the 300, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Siemens Hipath 3000 SNMP Alarms

This application processes SNMP alarm notification traps from Hipath 3000 and Hicom 150e systems that have been configured to deliver their traps to the Tracker. The alarm traps are converted into ASCII format, filtered using a set of user-defined rules and, where appropriate delivered as a Track alert to a central management system.

Siemens Hipath 3000 Toll Fraud Reporting

The application monitors the CDR output from the Hipath 3000, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Siemens Hipath 4000 Toll Fraud Reporting

The application monitors the CDR output from the Hipath 4000, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the

call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

Siemens Realitis/IDX Alarm Monitoring

The Realitis/IDX Alarm Monitoring process is triggered either at regular, configurable time intervals or when it detects an alarm exception record in the call data stream. Once triggered the application logs on to the Realitis/IDX, retrieves the error table and looks for new or changed entries. These error alarm entries are processed against a set of user-defined rules to determine if the error should be delivered to a central management system. The interval timer is reset after each login.

Siemens IsDX Automated Backup

This application enables the Tracker to backup the IsDX configuration files on a user defined schedule. The files are stored locally on the Tracker but can be copied to a central storage area as a secondary backup. When the need arises to restore the configuration files on the Tracker back to the IsDX, this can be done remotely.

Siemens Realitis/IDX Clock Set Utility

The internal clock on the Siemens Realitis/IDX switch is known to drift over a period. This application will log into the Realitis/IDX and set the clock to the current date and time of the Tracker 2700. The OSL level, user and key required to log into the Realitis/IDX are stored in the Tracker application configuration file. The application can be invoked manually from the command prompt of the Tracker, or scheduled to run automatically using the Tracker's internal scheduler.

Siemens Realitis/IDX Toll Fraud Reporting

The application monitors the CDR output from the Realitis/iSDX, converts the binary record to an ASCII representation, identifies key fields within each call record and applies a set of user-defined rules. These rules are used to identify possible fraudulent traffic patterns. If the call(s) are identified as being possibly fraudulent then an alarm is delivered to a central management system. The alarm includes the last call data record that triggered the alarm event.

From Realitis/iSDX software release 6.1 onward, the number of dialled digits supported in the CIL record was increased from 18 to 24 digits. This application collects 18 digits and if more than 18 digits are supplied, only the first 18 digits will be collected.

In addition to the toll fraud functionality, the application will also detect alarm records from the PBX that can be can be embedded in the call data stream. These can then be made available to the Alarm Reporting application if it is running on the Tracker.

TRACKER APPLICATIONS

Tracker Generic String Match Alarm Reporting

The application monitors ASCII data output from a managed device on a serial interface and applies a set of user-defined rules to each line of data received to determine if an alarm should be delivered to a central management system. The managed device must be configured to output data spontaneously on a V24 port. Each line of data is processed independently.

Tracker 2700 Digital Input Alarms

This application monitors the Tracker 2700 digital inputs and provides a facility for generating customised alerts or setting digital outputs based on the input state. The application provides greater customisation and output options than the built-in digital alarm facility. The state of the 16 digital inputs is continually monitored for change and when one occurs the application passes the following information to the rule processor:

- The current state of each of the 16 inputs.
- An indication of state change for each of the 16 inputs.
- The current state of each of the 7 outputs.

The rule processor applies a set of user-defined rules that determine the action to be taken based on individual or combined states of inputs and outputs. Available actions include delivery of an alert or the setting of a digital output. If required, the application can be configured to set the digital outputs to a known state at start-up.

Tracker 300 Controller Alarms

This application polls one or more Tracker 300 controllers for data. It then stores any data received into a file on the Tracker 2700. Users can set the Tracker 2700 to send out an alarm if the data from a Tracker 300 is out of normal operating parameters.

Tracker 2700 SNMP Alarms

This application processes SNMP Alarm notification traps delivered from other Tracker 2700s that have been configured to deliver SNMP alarms to the managing Tracker. The process of dealing with the traps is split into two parts: Trap capture and Alarm reporting.

Trap capture involves receiving the trap and converting it into a textual form suitable for processing by the Alarm reporting application.

Alarm reporting involves reading each text message generated by the trap capture, identifying key fields and applying a set of user-defined rules to determine if an alert should be delivered to a central management system.

Tracker 2750 Digital Module Alarms

This application monitors inputs on the Digital I/O modules installed in the Tracker and provides a facility for generating customised alerts or setting digital outputs based on the input state. Digital I/O pins are individually configurable as inputs or outputs and given labels to indicate their function. This application checks the state of the inputs once per second and passes the following information to the rule processor:

- The current state of each of the inputs.
- An indication of state change for each of the inputs.

The rule processor applies a set of user-defined rules that determine the action to be taken based on individual or combined states of inputs and outputs. Available actions include delivery of an alert or the setting of a digital output.

Tracker 2610 Temperature & Humidity Monitor

The Tracker 2610 can be configured to output temperature and humidity readings at preset intervals and to issue an alarm message if one of its user definable setpoints is exceeded. These setpoints are High Temperature, Low Temperature, High Humidity and Low Humidity. This application is designed to recognise an alarm message or temperature or humidity readings outside of user definable limits and to deliver an alarm message to a central management system. The alarm message will include a description of the alarm as well as the current temperature and humidity readings.

Device Healthcheck

This application will cause the Tracker to sequentially 'Ping' the IP addresses of user defined devices at user defined intervals to ensure that each device is available.

If a device fails to respond to the ping request for a number of user defined times then the Tracker will send an alarm message to a central management system. The Tracker will keep attempting to ping all devices and should a previously failed device respond it will send another alarm message to indicate that the device is now available.

Digital Alert Delivery

Custom alert delivery methods are associated with alert destinations and provide alternative mechanisms for delivering Tracker alert notifications in situations where a non-standard delivery mechanism or message format is required. Delivery methods are optional, licensed software modules identified by the file extension `.adm`.

For Trackers fitted with a digital input/output interface, the Digital Delivery method allows you to define alert destinations that set the state of one or more digital output pins. When an alert is delivered to that destination, the corresponding output pins are set. Each destination would define a specific set of output pins and their state; High (+5v), Low (0v) or Flashing. Note that alerts delivery to a digital delivery destination will always report 'success' even if no digital port is fitted.

GENERAL APPLICATIONS

Power Management

The Pulizzi IPC range enables users to control the mains power supplied to remotely located equipment from central management premises. Users can power up or down individual devices, a group or all devices in a pre defined sequence. This Tracker application provides a user friendly menu system as an interface to the Pulizzi unit. The connection between the Pulizzi and the Tracker is via a serial connection.

Cisco Router Backup

This application will allow the Tracker to automatically connect to the Cisco router at user defined periods and download either or both of the Router Configuration file and the Router Boot image. These files can be stored in Tracker memory and/or collected by a central management system. In the event of a router problem these files can be used to re program the router without having to visit the site. The router Configuration file is usually between 20 and 40K and the Boot image between 10 and 20 Meg.

The Tracker is normally connected to the router management interface via a serial port. The application operates with the following Cisco Routers – 2500, 2600, 3500, 3600, 4500 and 7000 series.

Generic UPS SNMP Alarms

This application processes SNMP asynchronous alarm traps from managed UPS devices that implement the MIB-II UPS MIB as defined in RFC-1628.

The generic UPS MIB defines 4 trap types:

- Type 1: upsTrapOnBattery
- Type 2: upsTrapTestCompleted
- Type 3: upsTrapAlarmEntryAdded
- Type 4: upsTrapAlarmEntryRemoved

This application will capture trap types 1, 3 and 4, filter them using a set of user-defined rules and deliver the alarm content as a Tracker Alert to a central management system.

Note: Some manufacturers' implementation of the generic UPS MIB does not adhere to the standard MIB specification. While considerable effort has been made to accommodate the more common variations, it is possible that this application may not be able to correctly interpret the alarms from some generic UPS agents.

SNMP V1 Trap Relay

This application processes SNMP v1 traps from any device that has been configured to deliver SNMP alarms to the managing Tracker and encapsulates the data content from the original trap in a Tracker alert for onward

delivery to an alarm management system. The data fields from the original trap are passed without interpretation or labelling.

The process of dealing with the traps is split into two parts:

Trap capture

Trap relay

Trap capture involves receiving the SNMP trap and converting it into a textual form suitable for processing by the trap relay application. This facility is provided by the trapcatd process that runs independently of the trap relay application. The devices to be monitored must be configured to send their traps to the Tracker.

Trap relay involves reading each trap message generated by trapcatd, identifying key fields and applying a set of user-defined rules to determine if the trap should be delivered to a network central management system. This document covers the configuration of both trap capture and the trap relay application.

Stratus Fault Tolerant Server SNMP Alarms

This application processes SNMP traps from the Stratus Fault Tolerant Server. This application supports Stratus software release 1.15 to 1.3. This application will accept the traps, filter them using a set of user-defined rules and deliver the alarm content as a Tracker alert to a central management system.

Siemens Verint Ultra Voice Recording SNMP Alarms

This application processes SNMP asynchronous alarm traps from the Verint Ultra Voice Recorder. The application supports Ultra version 9. This application will accept the traps, filter them using a set of user-defined rules and deliver the alarm content as a Tracker alert to a central management system.

Lapis RAID Monitoring

This application provides automated monitoring of a Lapis RAID Array and allows alerts to be delivered to a remote management centre in the event of a fault condition. The frequency at which the RAID array is checked and the rules used to determine if an alert should be raised are user configurable. The application also stores a snapshot of the RAID status for use by the Raidstatus utility.

Generic Network SNMP Alarms

This application processes the 5 standard generic SNMPv1 network traps defined for MIB-II: cold-start, warm-start, link-up, link-down, authentication failure and EGP Neighbour loss. This application will accept the traps, filter them using a set of user-defined rules and deliver the alarm content as a Tracker Alert to a central management system. The application requires Tracker firmware as follows:

- Tracker 2700 firmware 10303 or later
- Tracker 2750 firmware 20103 or later

- Tracker 2740 firmware 30101 or later

MGE UPS Serial Alarms

This application collects alarm notification messages from an MGE Systems UPS. The alarm notifications can be filtered using a set of user-defined rules and then delivered as a Tracker Alert to a central management system.