NORTEL NETWORKS

Preside Multiservice Data Manager

Management Data Provider

User Guide

241-6001-309

Preside Multiservice Data Manager

Management Data Provider

User Guide

Publication: 241-6001-309
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003

Printed in Canada

Publication history

December 2003

14.3 RSUP Standard
Commercial availability

Contents

About this document **15**
Who should read this document and why 15
What you need to know 16
How this document is organized 16
What's new in this document 17
Text conventions 19
Related documents 20
Preside Management Data Provider (MDP) 20
Preside Multiservice Data Manager (MDM) 21
Passport 6400 21
Passport 7400/15000/20000 21
DPN 21
Vector 21

Chapter 1
Introduction **23**
Collecting data 24
Data conversion 24
Converting switch data to bulk data format 25
Converting switch data to published format 29
Archiving 31
Transferring data to down-stream applications 33
Supporting MDP 34
Hosts 34
MDP workstations 37
Configuring MDP 37

Controlling MDP processes 38
MDP logs 38
MDP directory structure 39
Passport support 42
Passport data flow 42
Datatypes 45
Data models 46
Data collection - Passport 48
Data collection - MDP 51
Passport data file names 52
Statistics Retrieval System 58
Value-added applications 58
DPN-100 support 60
DPN-100 data flow 60
Datatypes 62
Data collection 63
DPN-100 data file names 63
Value-added applications 68
Vector support 69
Vector data flow 69
Datatypes 71
Vector data conversion 71
Vector data file names 75

Chapter 2
Configuration **81**

Customizing an MDP configuration 82
MDP Configuration tool 85
Configuring file transfers to customer hosts 87
Configuring customer host connections 88
Transferring files to customer hosts 90
Checking file type destinations 91
Backing up converted files 91
Transferring files to multiple directories on the same host 92
Setting the File Mover Manager log level 92

Scheduling customized data analysis programs 93
Backing up daily published format files 93
File transfer failures 94
Configuring data file retention 94
Setting the data file retention time 95
Setting the minimum available disk space 96
Setting the Disk Manager log level 96
Configuring BDF archiving 96
Configuring BDF archiving 97
Configuring the initial BDF archival directory structure 97
Changing an existing BDF archival directory structure 98
Configuring the disk space threshold for halting BDF archiving 99
Configuring the disk space threshold for SNMP warnings 99
Configuring MDP file processing audits 101
Configuring the audit of MDP file processing 101
Configuring the File Processing Audit log level 102
Configuring log archiving 103
Configuring log archiving 103
Configuring the initial log archival directory structure 103
Changing an existing log archival directory structure 104
Configuring MDP surveillance 105
Customizing MDP data directories 106
Opening the MDP Flexible Directory Installation window 107
Customizing data directory location 107
Returning a customized directory to a standard MDP directory 109
Flexible Directory Installation window 110
Restrictions on directory customization 112
Recording directory customization 113
Setting a secondary MDP mount point (Vector, only) 114
Configuring the Outage Controller 115
Setting the local MDP host as primary or secondary 115
Identifying the secondary MDP host 116
Scheduling the Outage Calculator 116
Identifying the MDM host 116
Setting the Outage Controller log level 117

Enabling outage calculation 117
Launching the MDP Topology Generator 117
Archiving outage files 118
Transferring outage files to customer hosts 118
Configuring availability calculation 118
Availability calculator configuration 119
Service window configuration 120
Start life configuration 121
Availability report generation 122

Chapter 3
Configuring MDP for Passport 125
Prerequisites 125
Storing Passport raw data 126
BDF data management 126
Converting Passport raw data to BDF 127
Setting the BDF field delimiter 127
Setting BDF data compression 128
Including the DMId with BDF filenames 128
Including the DMId and RDF version with BDF records 129
Retaining backwards compatibility for BDF records 129
Customizing BDF records 130
Setting the BDF conversion log level 132
Setting the BDF conversion escape character 132
Creating empty BDF files 133
Archiving BDF records 133
Assigning data to outage calculation 134
Setting the File Manager log level 134
PF data management 134
Converting Passport accounting raw data to PF 135
Setting PF data encoding 135
Enabling PF backward compatibility 135
Setting PF data storage format 136
Collecting Passport data 136
Defining the Passport network 137

Managing data collection entries 137
Setting data collection options 140
Scheduling data collection 144
Configuring SRS 145
Selecting Passport components and attributes 152
Configuring outage calculation 156
Prerequisites 157
Setting the BDF field delimiter 157
Calculating combined outages 157
Setting the minimum threshold for outages 157
Setting the maximum threshold for outages 158
Setting the number of days to keep unmatched OOS records 158
Setting the Outage Calculator log level 158

Chapter 4
Configuring MDP for DPN-100 161
Prerequisites 162
Storing DPN-100 raw data 162
BDF data management 163
Converting DPN-100 raw data to BDF 163
Archiving BDF data 163
Setting the BDF field delimiter 164
Setting BDF data compression 164
Setting the BDF conversion log level 165
Setting the BDF conversion escape character 166
Assigning data to outage calculation 166
Setting the File Manager log level 167
PF data management 167
Converting DPN-100 accounting raw data to PF 167
Setting PF data encoding 167
Enabling PF backward compatibility 168
Setting PF data data storage format 168
Configuring the switch 169
Configuring a spooling site for a DPN-100 module 169
Setting the PAD daemon 169

Collecting DPN-100 data 171
Configuring outage calculation 171
Prerequisites 171
Setting the BDF field delimiter 172
Calculating combined outages 172
Setting the minimum threshold for outages 172
Setting the maximum threshold for outages 173
Setting the number of days to keep SET alarms 173
Setting the number of days to keep CLEAR alarms 173
Setting the Outage Calculator log level 173

Chapter 5
Configuring MDP for Vector 175
Prerequisites 175
Storing Vector raw data 176
BDF data management 176
Converting Vector raw data to BDF 176
Setting the BDF field delimiter 177
Setting BDF data compression 177
Logging BDF converter warnings 178
Logging File Manager verbose messages 178
Assigning a secondary MDP 178
Collecting Vector data 179

Chapter 6
MDP administration 181
MDP commands 181
Collecting Passport data 182
Converting raw data files to BDF 186
Converting raw files to PF 188
Identifying new Passport performance metrics 191
Launching the MDP Disk Manager and setting the minimum disk space 192
Aggregating Vector call records (legacy billing) 193
Aggregating Vector performance data 194
Correlating Vector call records (legacy billing) 195

Correlating Vector call records (Egress billing) 196
Correlating Vector performance data 197
Processing archived raw data 198
Viewing BDF files with Data Viewer 198
Viewing BDF files with the bdfview command 199
Viewing Published Format files 201

Chapter 7
MDP logs 203
Log format 203
Log file names 204
Log levels 207
MDP Log Viewer 207
Opening the MDP Log Viewer window 208
MDP Log Viewer window 209
Using the MDP Log Viewer window 213
Generating log reports from the command line 217
Log messages 218

Chapter 8
MDP alarms and/or traps 225
Overview 225
MDP events, and alarms and/or traps 226
Retransmission of alarms and/or traps 228

Chapter 9
Value-added data applications 231
Outage calculation overview 232
DPN outage calculation 233
Types of DPN outages 234
Passport outage calculation 235
Types of Passport outages 239
Alarm exceptions file 241
Outage calculation processes 241
Process overview 242
MDP outage controller 243

MDP topology generator 244
Outage calculators 246
Outage calculation file names 251
Outage file names 251
Topology module description file names 252
Unmatched alarm file names 253
Availability calculation 253
Types of reportable outages 255
Accumulated statistics 256
Start life calculation 257
Availability calculator 258
Rollback of availability analysis statistics 260
Availability report generation 264
Availability calculation file names 268
Index **271**

About this document

This document describes how to configure and use the Management Data Provider (MDP). This information includes collecting, converting, and transferring data from DPN-100, Passport, and Vector switches to customer billing and network analysis hosts.

The MDP is installed with the Preside Multiservice Data Manager (MDM).

> ***Note:*** In this document, Passport is used as a generic term that includes all Passports 6400, 7400, 15000, and 20000.

The following topics are discussed in this section:

- "Who should read this document and why" (page 15)
- "What you need to know" (page 16)
- "How this document is organized" (page 16)
- "What's new in this document" (page 17)
- "Text conventions" (page 19)
- "Related documents" (page 20)

Who should read this document and why

This document is intended for network operators, billing administrators, or network performance analysts. Those personnel responsible for configuring or using the Management Data Provider (MDP) will require this document.

What you need to know

You need to have had some exposure to both computers and network concepts. Basic computer literacy is required to operate a Management Data Provider (MDP); you need to know how to use a keyboard and a mouse, what a menu is, and how to start applications from a menu using a mouse.

MDP resides on a UNIX workstation. You should be familiar with a UNIX editting facility (vi, for example) so that you are able to modify files. You should be familiar with SUN workstations, the UNIX operating system, and network communications (IP, FTP, ATM, or frame relay).

Knowledge of network management concepts for Passport, DPN-100 or Vector switches is required.

Knowledge of the Preside Multiservice Data Manager (MDM) software is required. Specifically, knowledge of the MDM Server Management administration (SVM) tools and the Host Group Directory Server (HGDS) and it's administration tool hgadmin.

How this document is organized

This document contains the following sections:

- "Introduction" (page 23) provides an overview of the MDP.
- "Configuration" (page 81) describes how to: identify customer hosts, assign converted data to specific customer hosts, set data file retention periods, archive BDF data, perform surveillance of the MDP host, generate audit reports, archive MDP logs, customize the MDP UNIX directory structure, configure the outage controller, and configure availability calculation and report generation.
- "Configuring MDP for Passport" (page 125) describes how to collect and convert spooled data from Passport switches. The Statistics Retrieval System is also described in detail.
- "Configuring MDP for DPN-100" (page 161) describes how to collect and convert data from DPN-100 switches.
- "Configuring MDP for Vector" (page 175) describes how to collect and convert data from Vector switches.

- “Value-added data applications” (page 231) describes how to use alarm data from switches to calculate and report switch outages and switch availability.
- “MDP administration” (page 181) describes MDP commands and command line parameters.

  This section also describes how to: process archived raw data, view BDF files, and view published format (PF) files.

- “MDP logs” (page 203) describes the logs generated by the MDP. This section also describes how to archive and view MDP logs.
- “MDP alarms and/or traps” (page 225) describes MDP traps, configuring MDP trap generation, and the mapping between significant MDP events and traps. MDP traps can be monitored using the Preside MDM Alarm Viewer.

What’s new in this document

Support for the following feature is added to this document:

- “NM0448 - MDP Administration” (page 17)

NM0448 - MDP Administration

This feature includes the following changes:

- the MDP Administration Client/Server architecture has been removed. The MDP Configuration tool (gmdpconfig) continues to perform MDP customization.

  Some of the common buttons on the configuration tool windows have changed functionality and the message panel has been removed. For more information, see “MDP Configuration tool” (page 85).

  A method of customizing the MDP Configuration tool is provided. For more information, see “Customizing the MDP Configuration tool” (page 86).

- the MDP process administration (mdpadm) has been removed. MDP processes are now controlled by the Multiservice Data Manager (MDM) Server Administration tool (SVM). For more information about SVM, see 241-6001-303 *Preside MDM Administrator Guide*.

  The MDP processes now controlled by SVM are described in 241-6001-310 *Preside MDM Server Reference Guide*.

  The File Prober Manager and MDP Disk Manager command line parameters are described in section "MDP commands" (page 181).

- Passport network information can be obtained from the Multiservice Data Manager (MDM) Host Group Directory Server (HGDS), only. The configuration of Passport network information is performed using the Host Group Administration tool (hgadmin). For more information about defining a Passport network, see "Defining the Passport network" (page 137).
- the DPN-100 Configuration Collector window has been removed. DPN collection processes are now controlled by the Multiservice Data Manager (MDM) Server Administration tool (SVM). For more information about controlling DPN-100 collection processes, see "Collecting DPN-100 data" (page 171).
- The MDP Planning section of this document has been removed. Planning and engineering information can be found in 241-6001-102 *Preside MDM Planning Guide*. MDP host descriptions can be found in the section "Hosts" (page 34).
- A seperate userID (mdpprobe) can no longer be used launch File Probers Passport data collection. The MDP administrator userID is the only userID required to operate the MDP software.
- Nortel Networks recognizes that some customers want to customize their MDP without using the MDP Configuration tool (gmdpconfig). The MDP can be customized by directly editting the MDP configuration files. The configuration files are identified in section "Customizing an MDP configuration" (page 82).
- Configuring Passport and DPN-100 outage calculation involves using different windows.

— Previously, the window Outage Controller was a window tab within the **Value Added** window. Now, Outage Controller configuration is performed using the window Outage Control from the main MDP Configuration tool menu.

— Previously, the Outage Calculator was a window tab within the **Value Added** window and applied to both Passport and DPN-100. Now, Outage Calculator configuration for Passport is performed using the window Passport Outage from the main MDP Configuration tool menu and Outage Calculator configuration for DPN-100 is performed using the window DPN Outage from the main MDP Configuration tool menu.

- It is no longer necessary to specify a workstation port number for Passport Data Model Manager. This port number can now be automatically detected by the Passport File Prober.

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

  Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- **nonproportional spaced bold type**

  Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- `[optional_parameter]`

  Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- `<general_term>`

  Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE,lowercase

  In MDM, uppercase and lowercase letters that appear in UNIX commands and parameters must be matched exactly. The system matches upper and lowercase characters differently.

- |

  This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

  Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

Related documents

This section identifies documents related to the Management Data Provider (MDP):

- “Preside Management Data Provider (MDP)” (page 20)
- “Preside Multiservice Data Manager (MDM)” (page 21)
- “Passport 6400” (page 21)
- “Passport 7400/15000/20000” (page 21)
- “DPN” (page 21)
- “Vector” (page 21)

Preside Management Data Provider (MDP)

A document entitled the Preside MDM Release Supplement is issued with the MDM/MDP software. The Release Supplement describes new features, software compatibility, software patches and known discrepancies. The Release Supplement should be the first point of reference for new information

related to MDP.

241-6001-806 *Preside MDM MDP Data Formats Reference Guide*

Preside Multiservice Data Manager (MDM)

For a list of Preside MDM documents, see 241-6001-000 *Preside MDM Documentation Guide*.

Passport 6400

For a list of Passport 6000 documents, see 241-6401-001 *Passport 6400 Documentation Guide*.

Passport 7400/15000/20000

For a list of Passport 7000/15000/20000 documents, see 241-5701-001 *Passport 7400, 15000, 20000 Documentation Guide*.

DPN

241-1001-100 *DPN-100 Product Overview*
241-1001-115 *DPN-100 Call Redirection System User Guide*
241-1001-320 *DPN-100 Accounting User Guide*
241-2001-332, *DPN-100 Data Spooling Description*

Vector

241-9501-010 *Vector General Description*
241-9501-103 *Vector Site Requirements and Preparation Guide*
241-9501-301 *Vector Operations and Maintenance Using VMI User Guide*
241-9501-302 *Open Management System for Vector (OMS-V) Guide*
241-9501-306 *Open Management System for Vector Error Messages*
241-9501-501 *Vector Hardware Maintenance User Guide*

Chapter 1
Introduction

The Management Data Provider (MDP) is an off-switch component of a data collection system that processes spooled data generated by Nortel Networks switches. The MDP collects spooled data from Passport switches using the file transfer protocol (FTP) to minimize the performance degradation that typically results from constant metric polling. DPN-100 and Vector switches automatically transfer spooled data to the MDP. The raw switch data is reformatted as bulk data format (BDF) or published format (PF) and transferred to down-stream billing and performance analysis applications.

The benefits of the MDP include

- consolidated data collection
- high data integrity
- extensive data content
- scalable solution for all network sizes; performance gains on multi-processor platforms
- ease-of-fit into operational environments

The following topics are discussed in this section:

- “Collecting data” (page 24)
- “Data conversion” (page 24)
- “Archiving” (page 31)
- “Transferring data to down-stream applications” (page 33)

- "Supporting MDP" (page 34)
- "Passport support" (page 42)
- "DPN-100 support" (page 60)
- "Vector support" (page 69)

Collecting data

The Management Data Provider (MDP) collects performance metrics using different methods for each switch type. Only the collection of Passport performance metrics is controlled by the MDP. The transfer of DPN-100 performance metrics to the MDP is controlled by the DPN-100 switch. The transfer of Vector performance metrics to the MDP is controlled by the Vector switch.

Data conversion

The Management Data Provider (MDP) converts performance metrics data to bulk data format (BDF) or published format (PF).

"Supported data conversion formats" (page 24) shows the data conversion format supported for each switch data type.

Table 1
Supported data conversion formats

DataType	DPN	Passport	Vector
accounting	PF/BDF	PF/BDF	BDF
statistics	BDF	BDF	BDF
logs	BDF	BDF	
alarms	BDF	BDF	
state change notification		BDF	
outage	BDF	BDF	
availability	BDF/ASCII	BDF/ASCII	
SRS		BDF	

The following topics are discussed in this section:

- "Converting switch data to bulk data format" (page 25)
- "Converting switch data to published format" (page 29)

Converting switch data to bulk data format

Raw switch data can be converted to bulk data format (BDF) data in an ASCII format. All data-types from all switch-types can be converted to BDF.

The BDF conversion process uses schema files to interpret the binary switch data. A schema file is required for each record type of a data type generated by each switch type. Schema files cannot be modified.

The BDF conversion process uses record description files (RDF) to specify the record format of the converted metric data. RDFs are used to control which fields are converted and their field position in the converted record. The BDF Converter requires an RDF for each datatype generated by each switch-type. Passport RDFs can be modified using the MDP Configuration tool; see "Customizing BDF records" (page 130).

> ***Note:*** Nortel Networks recommends the customization of BDF records. Customizing BDF record content ensures that only those fields required by down-stream processing (billing and performance analysis applications) are converted and transferred. Depending on your requirements, BDF record customatization can provide substantial MDP performance gains.

After the MDP has been configured for BDF conversion, data conversion is automatic and continuous. For testing purposes, the BDF Converter can be manually started from the UNIX command line.

The BDF converter normally reads raw switch data from the spool directory /opt/MagellanMDP/data/mdp/spool. Vector raw data is read from the merge directory /opt/MagellanMDP/data/mdp/merge. Converted files are written to the appropriate sub-directory of the dump directory /opt/MagellanMDP/data/mdp/dump. If BDF archiving is configured, the BDF Converter also writes the BDF records to the appropriate archive directory /opt/MagellanMDP/data/mdp/archive.

For a description of Passport BDF file names, see “BDF data” (page 53).

For details about the bulk data format records, see 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

Interpreting BDF output

The following rules are used to generate BDF records:

- A record can be any length.
- Fields are displayed in the BDF output file in the same order as they are declared in the RDF file. If a field is absent in a record, the field value in the BDF file is NULL (: :).
- The record separator is \n. The \n is stored as a Line Feed 010 (LF).
- A line containing only a \n is a blank line. Blank lines are ignored.
- The default field separator is the DEL (127) character.

  The alphabetic characters [A-Z] [a-z] and numeric characters [0-9] cannot be used as delimiters.

  The following are reserved characters that cannot be used as delimiters by the BDF Convertor: the UNIX pipe command |, the caret ^, the open parentheses (, the close parentheses), blank spaces, the comma ,, the period .,and the forward slash /.

- When a field contains multiple values, such as repeating fields, each value is enclosed in parentheses.
  Elements of a vector, list, and array are also enclosed in parentheses, along with their indexes.
  A comma is used as a delimiter between the index and the value within the parentheses. See the following examples:

  — Repeating field: ...:(3021)(3033)(3034):...

  — List field: ...:(A)(B)(C)(D)(E):...

  — Vector field: ...:(0,A)(1,B)(2,C):...

  — Array field: ...:(0,0,A)(0,1,B)(1,0,C)(1,1,D):...

- A sequence of three, or more, empty fields can be compressed in the output file to save space.
  The start of the compression is indicated by ^<count>.
  For example, ^5 indicates 5 consecutive empty fields.

  The default output format does not use field compression.

- The first 2 fields of all BDF records identify the switch type (pp, dpn, vss, or gen) and the data type (acc, sta, ala, log, scn, otg, or ava). Data type otg applies to switch types pp and dpn, only. Data type ava applies to switch type gen.
- The third field of all BDF records identifies the sub-data type (or record type within data types) for:
  - — DPN statistics and accounting data
  - — Vector statistics and accounting data
- A generic escape character is reserved for masking out characters encountered during input. The escape character is configurable. The default is %.

  If any delimiters, repeating field delimiters, or escape characters (generic or compression) are encountered in any input fields with a type of string, the offending character is replaced with %XX, where XX represents the hexadecimal value of the character.

  The alphabetic characters [A-Z] [a-z] and numeric characters [0-9] cannot be used as escape characters.

  There are 7 reserved characters that cannot be used as escape characters by the BDF Convertor: the UNIX pipe command |, the caret ^, the open parentheses (, the close parentheses), blank spaces, the comma ,, and the forward slash /.

Viewing BDF data

The Data Viewer can be used to verify that converted data matches expected results and to perform cursory to moderate switch performance analysis (troubleshooting).

The Data Viewer displays bulk data format records using three views:

- the record view displays individual BDF records with a field name and the field value
- the spreadsheet view displays all of the records in selected BDF files in spreadsheet tabular format
- the component view displays data values from selected attributes for selected components in a tree format. You can also graph selected component data, and view summary and detailed information.

See the Data Viewer section in 241-6001-031 *Preside MDM Performance Management User Guide*. For more information specific to MDP, see “Viewing BDF files with Data Viewer” (page 198).

BDF data can also be displayed using the command bdfview. For more information, see “Viewing BDF files with the bdfview command” (page 199).

MDP audit reports

The Management Data Provider (MDP generates audit reports which summarize the processing of bulk data format (BDF) records.

These audit reports indicate the following:

- originating switch and datatype for raw data
- possible missing raw data files (raw files out of sequence)
- raw data file size
- number of records successfully converted to BDF
- instances of corrupt data
- successful delivery of BDF files to down-stream application sites

MDP audit reports are generated every 24 hours at 0005 hours. The reports are generated in ASCII format and contain fields that are delimited by a colon, with the exception of field 10 that can contain a maximum of 3 hostnames or IP addresses separated by commas.

To configure audit report generation, see "Configuring MDP file processing audits" (page 101).

Converting switch data to published format

Passport and DPN-100 raw accounting data can be converted to published format (PF).

> ***Note:*** Published format data is used primarily by customers with down-stream billing applications on IBM or VAX mainframes.

PF data can be data encoded to either EBCDIC or ASCII. IBM customer hosts usually use EBCDIC and VAX customer hosts usually use ASCII.

PF data can be stored in one of two formats, big-endian or small-endian. IBM customer hosts usually use big-endian and VAX customer hosts usually use small-endian.

The conversion of Passport or DPN accounting data to published format can be performed using one of two methods:

- with the published format backward compatibility option enabled the PF converter reverts to a legacy method of processing PF data.
- with the published format backward compatibility option disabled, the PF converter optimizes performance gains from advances in hardware technology and accelerates delivery of PF converted data to down-stream billing applications. This method of PF conversion is the default.

Conversion of accounting records to published format, with the published format backward compatibility option disabled, consists of the following steps:

1 If the MDP is configured to convert Passport or DPN accounting data to PF and a raw accounting data file is detected in the spool directory /opt/MagellanMDP/data/mdp/spool, the appropriate published format converter (Passport or DPN) is started.

2 The MDP transfers the converted file, containing Passport or DPN published format accounting records, to the customer billing host.

Conversion of accounting records to published format, with the published format backward compatibility option enabled, consists of the following steps:

1 If the MDP is configured to convert Passport or DPN accounting data to PF and a raw accounting data file is detected in the spool directory /opt/MagellanMDP/data/mdp/spool, the appropriate published format converter (Passport or DPN) is started.

2 All Passport published format files processed within a single hour are concatenated into a single hourly file. All DPN published format files processed within a single hour are concatenated into a single hourly file.

3 At the end of each hour, the data from the Passport hourly file and the data from the DPN hourly file are concatenated into a single hourly file containing Passport and DPN published format accounting records.

4 The MDP transfers the hourly file containing Passport and DPN published format accounting records to the customer billing host.

5 At the end of each day, all of the hourly files, containing Passport and DPN published format accounting records, are concatenated into a single daily file.

6 The MDP File Mover Manager can backup the daily PF files.

After the MDP has been configured for PF conversion, data conversion is automatic and continuous. The PF Converters can also be started manually from the UNIX command line.

For details about the published format accounting records, see 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

Viewing published format data

The published format viewer translates published format (PF) binary records to ASCII format. The published format viewer does not support field selection or filtering.

The published format viewer is used to ensure that the PF files are consistent with the raw accounting data from Passport and DPN-100 switches.

For more information about the published format viewer, see “Viewing Published Format files” (page 201).

Archiving

The Management Data Provider (MDP) can automatically backup raw switch data files, bulk data format (BDF) records, and MDP logs.

Raw data

The MDP can be configured to archive raw switch data from Passport, DPN-100, and Vector switches. Use the appropriate switch data management window of the MDP Configuration tool to configure archiving.

Raw switch data is archived in sub-directories of the directory /opt/MagellanMDP/data/mdp/backup. The sub-directory structure is organized by datatype (accounting, alarm, statistics, scn, log, srs, debug, and outage). This directory structure cannot be customized.

For the naming conventions applied to archived raw data files on the MDP, see

- for Passport raw data files, “Raw data” (page 52)
- for DPN-100 raw data files, “Raw data” (page 64)
- for Vector raw data files, “Raw data” (page 75)

Bulk data format files

The MDP software can be configured to archive bulk data format (BDF) data for Passport and DPN-100 switch-types. A single raw data file can be split into multiple files in multiple directories according to the specified date field and written to a split file that contains the records for one nodeID, one datatype and one day.

Individual BDF records are stored in sub-directories of the archive directory /opt/MagellanMDP/data/mdp/archive. The sub-directory structure is configured using the MDP Configuration tool. For more information about customizing the archive directories, see “Configuring BDF archiving” (page 96).

A BDF archive directory can contain patterns for the year, month and day formats of the output directories. For example,

```
/opt/MagellanMDP/data/mdp/archive/pp/acc/%YYYY/%M%D
```

This example is intended to contain Passport accounting records. If the specified directory structure does not exist, bdfconv creates the structure. Directories with four characters for the year %YYYY, two characters for the month %M and two characters for the day %D are created when records with new dates are encountered during BDF conversion.

A single raw data file can be split into many files according to the specified date field and written to a split file that contains the records for one nodeID, one datatype, and one day.

The following indicates the date fields used:

Product	Datatype	Field
Passport	accounting	startTime
Passport	statistics	timeOfRecord
Passport	alarm	timeOfRecord
Passport	log	timeOfRecord
Passport	scn	timeOfRecord
DPN	accounting	startDateTime
DPN	statistics	dateTime
DPN	alarm	dateTime
DPN	log	dateTime

For a description of BDF archive file names, see “Archived BDF data” (page 55).

MDP logs

The MDP can be configured to archive log messages generated by the following MDP processes: the Passport File Manager, the DPN File Manager, and the Passport File Prober.

Individual MDP logs are stored in sub-directories of the archive directory /opt/MagellanMDP/data/mdp/admin/archive. The sub-directory structure is configured using the MDP Configuration tool. Once a directory structure is configured, the same directory structure is applied to logs from any of the MDP processes identified above. For more information about customizing the archive directories, see “Configuring log archiving” (page 103).

For a description of MDP log archive file names, see “Log file names” (page 204).

Transferring data to down-stream applications

After configuration, the Management Data Provider (MDP) File Mover Manager continually checks for the arrival of converted switch data files in sub-directories of the MDP dump directory /opt/MagellanMDP/data/mdp/dump. If converted switch data files are found, the MDP transfers the files to designated customer hosts.

Also transferred to customer hosts from the MDP are data files from these MDP applications: Statistics Retrieval System (SRS), outage calculation, availability calculation, and file processing audits.

The File Mover Manager controls multiple File Mover processes. Each MDP file type (a combination of switch type and datatype) has a dedicated File Mover process. This dedicated File Mover can transfer multiple instances of a specific file type and can use a maximum of three concurrent FTP sessions to transfer files to a maximum of three customer hosts.

For more information about customer hosts, see “Customer host” (page 36).

Supporting MDP

The following topics are discussed in this section

- "Hosts" (page 34)
- "MDP workstations" (page 37)
- "Configuring MDP" (page 37)
- "Controlling MDP processes" (page 38)
- "MDP logs" (page 38)
- "MDP directory structure" (page 39)

Hosts

The following hosts are discussed in this section:

- "Primary MDP" (page 34)
- "Backup MDP" (page 35)
- "Secondary MDP (Vector, only)" (page 35)
- "Customer host" (page 36)

For information about MDP and customer host security access requirements, see 241-6001-100 *Preside MDM Installer Guide*.

For information about network bandwidth requirements, see 241-6001-102 *Preside MDM Planning Guide*.

Primary MDP

The primary Management Data Provider (MDP)

- receives spooled data from designated switches
- converts spooled data to bulk data format (BDF) or published format (PF)

  Note: Published format data converstion applies to Passport and DPN-100 accounting data, only.

- transfers converted spooled data to designated customer hosts
- can also be a backup MDP

- is responsible for the generation of switch outage and availability statistics

  For Passport and DPN-100 support,
  the raw switch data for outage calculation (alarm and state change notification) can be collected by either the primary or backup MDP, but the outage and availability calculations are performed on the primary MDP.

Backup MDP

A backup Management Data Provider (MDP) performs the role of the primary MDP if the primary MDP is unreachable. The backup MDP

- must be configured as a clone of the primary MDP.

  The MDP administrator userID must be identical on both the primary and backup MDPs.

  The customer host userIDs and passwords configured on the backup MDP must be identical to the customer host userIDs and passwords configured on the primary MDP.

- requires that the switch data collection system be configured to redirect data to the backup MDP host if the primary MDP host is unavailable

  — for Passports, this requires that the MDP File Prober be configured to use the backup MDP; see “Selecting the backup MDP” (page 141)

  — for DPN-100s, this requires that the switches, themselves, be configured to use the backup MDP

  — for Vectors, the mandatory secondary MDP acts as the backup MDP

  Note: Nortel Networks recommends using a backup MDP host.

Secondary MDP (Vector, only)

The secondary Management Data Provider (MDP)

- applies to Vector switches, only
- can be the primary MDP for switches other than those assigned to the primary MDP

- can assume the role of the primary MDP if the primary MDP is unreachable
- must be configured as a clone of the primary MDP.

  The customer host userIDs and passwords configured on the secondary MDP must be identical to the customer host userIDs and passwords configured on the primary MDP.

- can collect switch data from switches other than those assigned to the primary MDP. This raw switch data is then automatically retrieved from the secondary MDP by the primary MDP over a network file system (NFS) connection for subsequent processing.

Customer host

A customer host

- can be a UNIX server, an IBM mainframe, or a VAX mainframe

  IBM customer hosts usually use EBCDIC data encoding and VAX customer hosts usually use ASCII data encoding. This distinction is important when configuring the MDP to convert raw data to published format data.

  IBM customer hosts usually use big-endian and VAX customer hosts usually use small-endian. This distinction is important when configuring the MDP to convert raw data to published format data.

  Note: If the MDP is configured to transfer accounting data to IBM customer hosts in bulk data format (BDF), use short BDF filenames. For information about configuring the MDP to use short BDF filenames, see “Using short BDF file names” (page 89).

- processes data received from a Mangement Data Provider (MDP) host. For information about configuring the MDP to transfer data to customer hosts, see “Transferring files to customer hosts” (page 90).
- a maximum of three customer hosts per datatype is allowed
- configured as a billing host, uses switch accounting data to generate accounting reports for network resource usage analysis, financial planning, budgeting, and billing purposes

- configured as a network performance host, uses switch performance metrics for network engineering and planning analysis
- receives file processing audit reports (if this MDP feature is configured). For information about configuring the MDP to generate file processing audit reports, see “Configuring MDP file processing audits” (page 101).
- receives Statistics Retrieval System (SRS) data in bulk data format (if this feature is configured). For information about configuring the SRS, see “Configuring SRS” (page 145).
- receives outage calculation data in bulk data format (if this feature is configured).

MDP workstations

The Management Data Provider (MDP) software is installed on workstations from Sun Microsystems and uses Solaris, Sun’s UNIX operating system. For more information about MDP workstations, see 241-6001-102 *Preside MDM Planning Guide*.

Installation tools are provided by Nortel Networks to simplify the installation and upgrading of the MDP software. For more information about the software required for MDP, see 241-6001-102 *Preside MDM Planning Guide*.

Configuring MDP

Initial configuration of the Management Data Provider (MDP) for Passport data collection is performed by the Preside Multiservice Data Manager (MDM) QuickStart wizard. For details about this initial configuration, see section “Configuration” (page 81) and 241-6001-100 *Preside MDM Installer Guide*.

The MDP is customized using the MDP Configuration tool. This tool is a graphical user interface (GUI) that is launched from the UNIX command line (gmdpconfig) or using the MDM menu item **Accounting**. For more information, see “Configuration” (page 81).

The MDP can also be customized by performing manual updates to MDP configuration files. The applicable configuration files are identified in section “Customizing an MDP configuration” (page 82).

The MDM Server Administration tool (SVM) is used to start MDP processes after MDP configuration. The MDP Configuration tool can restart MDP processes that have been previously started by SVM.

Controlling MDP processes

Management Data Provider (MDP) processes are controlled using the Preside Multiservice Data Manager (MDM) Server Administation tool (SVM). SVM starts, stops, and monitors MDP processes.

When the MDP software is installed, the MDM software required to use SVM is also installed. For information about starting SVM and registering MDP processes with SVM, see 241-6001-303 *Preside MDM Administrator Guide*.

When upgrading the MDP software, MDP processes registered with SVM are automatically restarted after software installation.

When re-configuring the MDP software features using the MDP Configuration tool, SVM-registered MDP processes are automatically restarted.

MDP logs

All Management Data Provider (MDP) processes generate log messages. These messages are written to log files associated with the MDP process.

MDP log files contain information such as:

- processing start time
- processing end time
- errors encountered
- warnings
- identification of files read
- number of records read
- identification of files created
- identification of files deleted

MDP logs can be selected and viewed using the MDP Log Viewer. This application generates log reports in a tabular format.

For more information about using MDP logs, see “MDP logs” (page 203).

MDP directory structure

The table “MDP directories” (page 39) describes the contents of each Management Data Provider (MDP) directory. The directory names cannot be changed.

Table 2
MDP directories

Directory	Contents of directory
/opt/MagellanMDP/data/mdp/spool	• Passport accounting and performance raw data files transferred by the File Prober • DPN-100 accounting and performance raw data files collected by the File Collector. • Vector accounting and performance raw data files transferred by a Vector switch.
/opt/MagellanMDP/data/mdp/spool/received	The names of DPN files successfully received by the MDP host (the file size is zero).
/opt/MagellanMDP/data/mdp/spool/restore	Vector raw data files deposited by the secondary MDP host; this only occurs when a delivery failure to the primary MDP host occurs.
/opt/MagellanMDP/data/mdp/spool/secondary	Mounting point for the secondary MDP host. Vector, only.
/opt/MagellanMDP/data/mdp/merge	Vector raw data files transferred by the File Manager for aggregation and correlation.
/opt/MagellanMDP/data/mdp/admin	Log files generated by MDP processes.
/opt/MagellanMDP/data/mdp/admin/archive	Archived MDP logs.
/opt/MagellanMDP/data/mdp/admin/mdprober	File Prober logs.
/opt/MagellanMDP/data/mdp/admin/tmp	Temporary log files generated by a File Manager.
(Sheet 1 of 3)	

Table 2 (continued)
MDP directories

Directory	Contents of directory
/opt/MagellanMDP/data/mdp/dump/accounting	bulk data format (BDF) and published format (PF) accounting files.
/opt/MagellanMDP/data/mdp/dump/statistics	BDF statistics files.
/opt/MagellanMDP/data/mdp/dump/alarm	BDF alarm files.
/opt/MagellanMDP/data/mdp/dump/log	BDF log files.
/opt/MagellanMDP/data/mdp/dump/scn	BDF state change notification files.
/opt/MagellanMDP/data/mdp/dump/outage	BDF outage files.
/opt/MagellanMDP/data/mdp/dump/avail	BDF availability report files.
/opt/MagellanMDP/data/mdp/dump/srs	BDF polled statistics files.
/opt/MagellanMDP/data/mdp/backup/...	Copies of raw data files, if the backup option was specified.
/opt/MagellanMDP/data/mdp/db/...	Binary database for DPN-100 and Vector.
/opt/MagellanMDP/data/mdp/avail	Availability calculator accumulated statistics.
/opt/MagellanMDP/data/mdp/oc/dpn/	DPN outage calculation directories. DPN-100 alarm files (BDF) on the primary MDP host are stored in directories oc/dpn/primary and oc/dpn/secondary (which is actually a mount point for oc/dpn/primary on the backup MDP host). oc/dpn/process is used as a working directory. DPN outage files, for use by MDP applications, are stored in oc/dpn/outage. Unmatched DPN alarm files are stored in oc/dpn/unmatched.
/opt/MagellanMDP/data/mdp/oc/pp/	Passport outage calculation directories. Passport alarm and scn files (BDF) on the primary MDP host are stored in oc/pp/primary and oc/pp/secondary (which is actually a mount point for oc/pp/primary on the backup MDP host). oc/pp/process is used as a working directory. Passport outage files for use by MDP applications are stored in oc/pp/outage. Unmatched Passport alarm and scn files are stored in oc/pp/unmatched.
(Sheet 2 of 3)	

Table 2 (continued)
MDP directories

Directory	Contents of directory
/opt/MagellanMDP/data/mdp/oc/model/	Network Topology description files.
/opt/MagellanMDP/data/mdp/archive	Archived Passport and DPN-100 BDF records.
/opt/MagellanMDP/lib/mdp/rdf/pp/<datatype>	Default Passport RDF files, supplied by Nortel Networks. <datatype> is one of: account, stats, alarm, scn, or log. DO NOT EDIT.
/opt/MagellanMDP/lib/mdp/rdf/<dpn|vss>/ <datatype>	Default DPN and Vector RDF files, supplied by Nortel Networks. <datatype> is one of: account, stats, alarm, or log. DO NOT EDIT.
/opt/MagellanMDP/lib/mdp/schema/ <pp|dpn|vss>/<data_type>	Default schema files, supplied by Nortel Networks, for Passport, DPN and Vector switches. data_type is one of: account, stats, alarm, scn, or log.
/opt/MagellanMDP/bin	MDP software executables and scripts.
/opt/MagellanMDP/3rdparty	2nd or 3rd party software libraries.
/opt/MagellanMDP/lib	MDP software libraries.
/opt/MagellanMDP/system	MDP software configuration, initialization, and installation specific files.
/opt/MagellanMDP/cfg/mdp	MDP customer configuration files.
/opt/MagellanMDP/cfg/mdp/pp/<DMId>	Passport data model files. <DMId> is the data model identifier.
/opt/MagellanMDP/cfg/mdp/pp/rdf/<datatype>	Custom Passport RDFs. <datatype> is one of: account, stats, alarm, log, or scn.
/opt/MagellanMDP/cfg/mdp/rdf/<dpn|vss>/ <datatype>	Custom DPN and Vector RDFs. <datatype> is one of: account, stats, alarm, or log.
/opt/MagellanMDP/cfg/mdp/rcf/pp/srs	Record content files (RCF) for Passport switches. RCFs are required by SRS.
(Sheet 3 of 3)	

Passport support

The Management Data Provider (MDP) provides applications to automatically collect, convert, archive, and transfer Passport data.

The following topics are discussed in this section:

- "Passport data flow" (page 42)
- "Datatypes" (page 45)
- "Data models" (page 46)
- "Data collection - Passport" (page 48)
- "Data collection - MDP" (page 51)
- "Passport data file names" (page 52)
- "Value-added applications" (page 58)

Passport data flow

The basic flow of Passport data through the Management Data Provider (MDP) is as follows:

1 The Passport performance metrics are collected in spool files on the switch in FMIP format. FMIP is Nortel Network's proprietary interface protocol on Passport switches. This binary data is referred to as raw switch data in the context of the MDP.

For a description of the Passport Data Collection System (DCS), see "Data collection - Passport" (page 48).

For a description of the types of spooled data collected from Passports, see "Datatypes" (page 45).

2 The MDP File Prober periodically logs into each Passport and initiates a file transfer protocol (FTP) connection from each Passport to the MDP. An FTP transfer is initiated for each Passport datatype.

The File Prober can be configured to close open spool files on the Passport before transferring them to the MDP.

The File Prober interogates each node to determine the Passport data model.

— If the data model exists on the MDP, the File Prober affixes a data model identifier (DMid) to the Passport raw data file name during the data transfer.

— If the data model does not exist on the MDP, the Data Model Manager downloads the Passport data model to the MDP. The Data Model Manager also checks the available MDP disk space to ensure adequate disk space is available for data collection.

New performance metrics introduced with the Passport data model are available for BDF records. The MDP administrator can easily customize the BDF record to include the new performance metrics.

The File Prober completes the transfer of the performance metrics, using the new data model identifier (DMid) in the raw data file name.

The MDP Disk Manager continually monitors MDP data disk space. A minimum disk space threshold is set and if this threshold is exceeded the MDP halts data conversion.

For a complete description of Passport data collection by the MDP, see “Data collection - MDP” (page 51).

3 The raw data file is transferred to the MDP spool directory /opt/MagellanMDP/data/mdp/spool.

The raw data file name is described in “Raw data” (page 52).

4 The MDP Passport File Manager detects the raw data file in the spool directory.

If the MDP is configured to convert Passport accounting data to published format (PF) and the Passport File Manager detects Passport accounting files in the spool directory, the Passport PF Converter is launched. Converting Passport accounting files to PF is described in section “Converting switch data to published format” (page 29).

If the MDP is configured to convert Passport accounting data to bulk data format (BDF), the MDP BDF Converter is launched.

For all other Passport datatypes, the BDF converter can be configured to launch. For more information, see “Datatypes” (page 45).

The PF data file name is described in “PF with the backward compatibility option enabled” (page 55) and “PF with the backward compatibility option disabled” (page 56).

If the BDF Converter is launched, the data model identifier in the raw data file name determines the appropriate schema to use during data conversion. Configure the record layout of the BDF file using the procedures “Retaining backwards compatibility for BDF records” (page 129) and “Customizing BDF records” (page 130). The alternative to configuring the BDF output files is to use the default record layout provided with the MDP software. Converting raw data to BDF is described in section “Converting switch data to bulk data format” (page 25)

The converted data is written to the appropriate sub-directories of the MDP dump directory /opt/MagellanMDP/data/mdp/dump.

If the MDP is configured to archive BDF data, the individual BDF records are archived in the appropriate sub-directories of the MDP archive directory /opt/MagellanMDP/data/mdp/archive.

The BDF data file name is described in “BDF data” (page 53) and “Short BDF file names” (page 54).

5 The Passport File Manager copies the raw data file from the spool directory to the backup directory /opt/MagellanMDP/data/mdp/backup.

6 The MDP File Mover Manager detects the converted data file in the dump directory and transfers the data file to a customer host.

The File Mover Manager can also send the converted data file to a local directory on the MDP host. This feature can be used to create backups of PF files.

7 If outage calculation is configured, successfully converted alarm and SCN BDF files are placed in the directory /opt/MagellanMDP/data/mdp/oc/pp/primary for post processing by the Outage Calculator. Outage calculation is described in section “Outage calculation overview” (page 232).

Datatypes

The following Passport datatypes are processed by the Management Data Provider (MDP):

- accounting (account, acc)
  including (but not limited to) records for ATM, frame relay, FR-ATM, peak water mark (PWM), Time Change, Voice Networking, and IP-VPN.

  By default, accounting data collection is turned on at the switch.

  Passport accounting data (bulk data format (BDF) and published format (PF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

- statistics (stats, sta)
  or performance data, including (but not limited to) trunk, LP, VoiceRoute, CAS, PCU, and ATM port.

  By default, statistics data collection is turned off at the switch.

  Passport statistics data (bulk data format (BDF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

- alarm (ala)
  data is used for analysis of switch and network down-time and other service-affecting problems.

  By default, alarm data collection is turned on at the switch.

  Refer to the Passport documentation for descriptions of Passport alarm data.

- log
  data is used to monitor the operator command activity on a node.

  By default, log data collection is turned on at the switch.

  Refer to the Passport documentation for descriptions of Passport log data.

- state change notifications (scn)
  are used for analysis of switch and network down-time and other service-affecting problems.

  By default, SCN data collection is turned on at the switch.

  Passport SCN data (bulk data format (BDF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

Data models

The Management Data Provider (MDP) stores a data model for each unique Passport data model available in the network. When a new Passport data model is introduced into the network, a new MDP data model is automatically generated. Multiple data models can exist on the MDP. The data models are controlled by the Data Model Manager (mdpdmm).

The Data Model Manager is started by, and registered with, the Preside Multiservice Data Manager (MDM) Server Administration tool when the MDM QuickStart configuration tool is used to configure a new MDP host.

As discussed in section “Converting switch data to bulk data format” (page 25), you, the customer, determine the content of bulk data format (BDF) files. When a new data model is created on the MDP, any new performance metrics for the spooled datatypes collected by the MDP are

identified to you. The MDP administrator has the option of using the MDP Configuration tool to add the new performance metrics to the converted data files. By default, if you do not customize the BDF record, the default data model supplied with the MDP software is used to determine the BDF record layout. To customize BDF records, see “Customizing BDF records” (page 130).

Using the tool **rdfreport**, new Passport data models can be obtained without waiting for the data models to be detected by the MDP. You can also use this tool to obtain data models from Passports not currently integrated into the network. For more information about rdfreport, see “Identifying new Passport performance metrics” (page 191).

New schemas and RDFs are delivered with each MDP software release. These new data models reflect the latest Passport performance metrics. The default RDFs are located in the sub-directories of directory /opt/MagellanMDP/lib/mdp/rdf/pp/<datatype>. No reconfiguration is required to use the default data model for BDF conversion.

Note: Do not modify the default RDFs.

The MDP is configured to maintain backwards compatibility with the default data model. Backwards compatibility ensures that: the fields included in previous BDF records are always included in new BDF records and the fields in previous BDF records are always in the same order. New fields are appended to existing BDF records. This functionality exists for the customer whose down-stream applications require consistent field order. To see how this option is configured, see “Retaining backwards compatibility for BDF records” (page 129). Backwards compatibility can be disabled.

The Data Model Manager uses an information file /opt/MagellanMDP/cfg/mdp/pp/<DMId>/<DMId>.info to record information about each generated data model. This information includes: the Passport node from which the data model was obtained, the date the data model was generated on the MDP, and any warnings or errors generated.

Note: If Passport switch software is rolled-back after the MDP has begun collecting data using a previous data model, the BDF Converter may generate warning messages indicating that some components or attributes are not recognized and cannot be converted.

Data collection - Passport

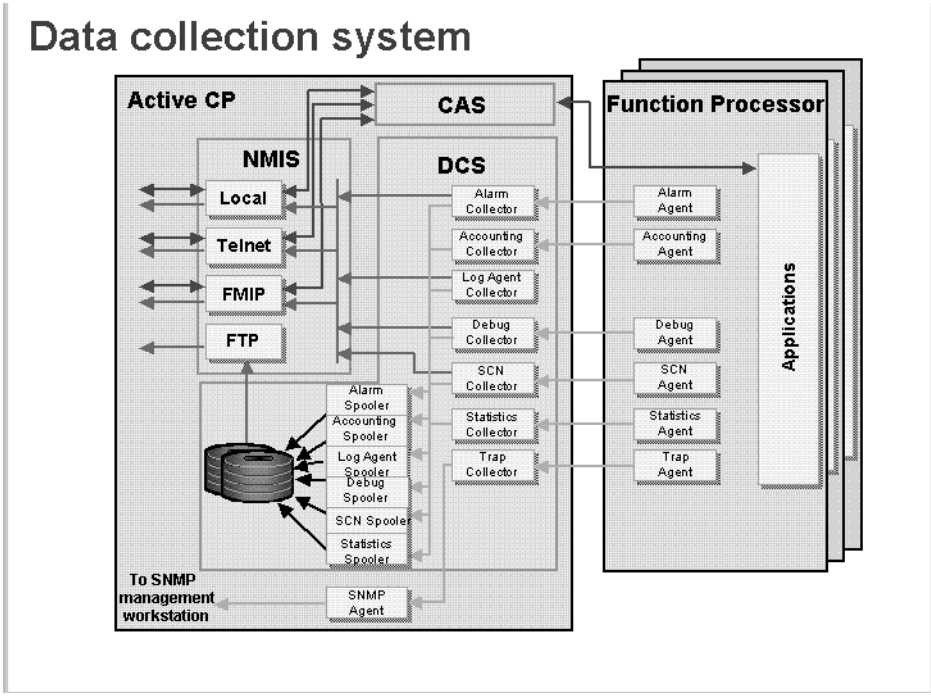
The Passport Data Collection System (DCS) consists of agents, collectors, and spoolers. Agents reside on each processor card to gather data records from the active services. On each processor card there is one agent for each datatype. The datatype agent sends its records to a collector that resides on the active control processor (CP).

The collectors send the data records to the spoolers. The spoolers (one per datatype) format the data and save it on the local Passport file system.

Each collector, agent, and spooler has a queue to hold data records until the data can be processed. If a queue reaches maximum capacity, the DCS begins to disgard data.

The figure “Passport data collection system” (page 49) shows the Passport Data Collection System.

Figure 1
Passport data collection system



Spooled data files

Data spooling can be be turned on or off by setting the spooling attribute of the datatype Spooler component. The spooling of real-time statistics (rtstats) and trap data cannot be turned off. Spooled data files are located in the following Passport file system directories:

```
/spooled/opened/<datatype>
/spooled/closed/<datatype>
```

where:
<datatype> is one of account, stats, alarm, log, or scn. For a description of the Passport datatypes collected by the MDP, see “Datatypes” (page 45).

The spool files on the Passport have the following naming format:

```
<pp|ppc>_<datatype>.<date>.<seq>.<nodeID>
```

For a description of the file name parameters, see “Raw data” (page 52).

When a spool file in the directory opened/<datatype> reaches maximum capacity, the Passport closes the file and moves it to the directory closed/<datatype>. A new file is opened in the directory opened/<datatype>.

Spool files are also closed

- each day at 0000 hours.
- when the Passport spooler receives a newFile command. The MDP File Prober can generate this command.
- when the active control processor (CP) is reset, restarted, or rebooted
- when the Passport file system is disrupted

The Passport DCS is described in the Passport documents 241-5701-611 *Passport 7400, 15000, 20000 Data Collection Guide* and 241-5701-650 *Passport 7400, 15000, 20000 Accounting Fundamentals*.

Data collection - MDP

Passport spooled data is collected by the Management Data Provider (MDP) using the File Prober. The File Prober establishes a proxy file transfer protocol (FTP) connection from a Passport switch to an MDP and transfers closed spool data files. An FTP session is initiated for each Passport datatype.

The File Probers are automatically launched at scheduled intervals.

The File Probers are controlled by the File Prober Manager. The File Prober Manager provides

- ease of configuration using the MDP Configuration tool
- improved error recovery
- confirmation of Passport and MDP host connectivity before attempting data collection
- security protection using encrypted passwords

Before the File Prober begins the transfer of spooled data from a Passport to an MDP, the File Prober interrogates the Passport to determine the Passport data model. The File Prober then sends the Passport data model information to the MDP Data Model Manager.

- If the data model exists on the MDP, the File Prober affixes a data model identifier (DMid) to the Passport raw data file name during the data transfer.
- If the data model does not exist on the MDP, the Data Model Manager downloads the Passport data model to the MDP.

  The File Prober completes the transfer of the spooled data, using the new data model identifier (DMid) in the raw data file name.

  New metrics introduced with the Passport data model are available for BDF records. The MDP administrator can easily customize the BDF record to include them.

Passport data models are described in section “Data models” (page 46).

The File Prober Manager obtains Passport network information from the Preside Multiservice Data Manager (MDM) Host Group Directory Server (HGDS). For more information about the HGDS, see 241-6001-310 *Preside MDM Server Reference Guide*.

Passport data file names

This section describes the formats of the Passport data file names on the Management Data Provider (MDP).

- "Raw data" (page 52)
- "BDF data" (page 53)
- "Short BDF file names" (page 54)
- "Archived BDF data" (page 55)
- "PF with the backward compatibility option enabled" (page 55)
- "PF with the backward compatibility option disabled" (page 56)
- "Passport SRS file names" (page 57)

Raw data

The raw data files on the MDP have the following naming format:

```
pp_<DMid>_<datatype>.<date>.<seq>.<nodeID>
.<status>
```

where:

pp is all types of Passports. On Passport 6000 the spool file prefix is pp and on Passport 7000/15000/20000 the spool file prefix is ppc.

<DMid> is the Data Model Identifier obtained from the MDP Data Model Manager.

<datatype> is account for account, stats, alarm, log, and scn.

<date> is one of <MMDDhhmm> or <YYYYMMDDThhmmss>. <MMDDhhmm> is the date and time the file was opened on the Passport 6000 node (where MM=month, DD=day, hh=hour, and mm=minutes) or <YYYYMMDDThhmmss> is the date and time the file was opened on the Passport 7000/15000/20000 node (where YYYY=year, MM=month, DD=day, T=date/time delimiter, hh=hour, mm=minutes, and ss=seconds)

<seq> is the file sequence number assigned by the Passport node.

<nodeID|nodename> the Passport nodeID is an integer between 1 and 65536 and is as provisioned on the switch. The Passport nodename is an uppercase character string of 1 to 12 characters in length and is as defined in the Host Group Directory Server (HGDS).

> ***Note 1:*** Do not use any special characters in either the nodeID or the nodename when the Passport is provisioned. Use of special characters will cause failure of MDP processes.
>
> ***Note 2:*** MDP value-added processes, such as the Outage and Availability Calculators, are unable to correlate Passport nodeIDs with Passport nodenames. Ensure that the MDP does not generate raw data file names with nodeIDs and raw data filenames with nodenames. If the MDP is generating raw data file names with one format (eg. nodeIDs) and you need to generate raw data file names from the same Passport using the alternate file name format (eg. nodenames), complete all value-added processing before retrieving Passport raw data files with the new file name format.

<status> is a two-letter code indicating the file transfer status. The letters co indicate a file that is currently open and being transferred. The letters cc indicate a file that is closed and has been successfully transferred.

> **Example**
> ```
> pp_BE0123A_account.11072345.003.2121.co
> (open Passport 6000 accounting file with a DMid)
>
> pp_CB03S2C_stats.19990926T141438.044.2001.cc
> (closed Passport 7000/15000/20000 statistics file)
> ```

BDF data

Bulk data format (BDF) files have the following naming format:

```
pp_<DMid>_<datatype>_<date>_<nodeID|nodename>_<seq>
.<ext>
```

where:

<DMid> is the Data Model Identifier obtained from the raw data file name. This qualifier is optional.

<datatype> is acc for acc, sta, ala, log, and scn.

<date> is one of <MMDDhhmm> or <YYYYMMDDThhmmss>. <MMDDhhmm> is the date and time the file was opened on the Passport 6000 node (where MM=month, DD=day, hh=hour, and mm=minutes) or <YYYYMMDDThhmmss> is the date and time the file was opened on the Passport 7000/15000/20000 node (where YYYY=year, MM=month, DD=day, T=date/time delimiter, hh=hour, mm=minutes, and ss=seconds)

<nodeID|nodename> the Passport nodeID is an integer between 1 and 65536. The Passport nodename is an uppercase character string of 1 to 12 characters in length.

<seq> is the file sequence number assigned by the Passport node.

<ext> is bdf if the raw data was successfully converted to BDF. This extension is err if the raw data could not be successfully converted.

Note: If the file name includes the .err extension, this file contains raw records that could not be converted.

Example

```
pp_BE0123A_acc_11072345_2121_003.bdf
(converted Passport 6000 accounting BDF records)

pp_GA0123A_sta_19990926T141438_2001_044.err
(errored Passport 7000/15000/20000 statistics raw
records)
```

Short BDF file names

A file name limitation exists for transferring BDF files to an IBM customer host; a maximum of 16 characters can be used. If the standard BDF file name format is used, the transfer of files to IBM customer hosts will fail. To use the short BDF file name format, see “Using short BDF file names” (page 89).

Note: The File Mover process truncates the nodeID or nodename to the first 4 characters. The MDP does not check for unique naming. If short file names are used, it is your responsibility to ensure that the first 4 characters of the nodeID are unique.

The short file naming convention for BDF files is

```
<p><t><mmddhh.MM><seq#><nodeID|nodename>
```

where:

<p> is p for Passport 6000 and r for Passport 7000/15000/20000.

<t> is datatype. a for accounting, s for statistics, l for logs, m for alarms, and n for state change notifications.

<mmddhh.MM> is the date the file was opened on the Passport (where mm=month, dd=day, hh=hour, and MM=minutes).

<seq> is the 2nd and 3rd digits of the Passport assigned file sequence number.

<nodeID|nodename> is the first 4 characters of the Passport nodeID or nodename.

Archived BDF data

BDF archive files use the same file name format as BDF files except that the date of the records is appended to the end of the filename, before the extension.

```
pp_<datatype>_<date>_<nodeID|nodename>_<seq>_<split-
by-date>.bdf
```

where:

<split-by-date> is the date on the data records, not the date of the raw data file.

PF with the backward compatibility option enabled

The published format (PF) backward compatibility option is described in section “Converting switch data to published format” (page 29).

If the PF backward compatibility option is enabled, PF file names have the following format:

```
Pp_TPACT<?>.mmddHHO (open file)
Pp_TPACT<?>.mmddHH (closed file)
```

the daily file

```
TPACT<?>.mmdd
```

Note: The daily published format file contains both Passport and DPN accounting records if both DPN and Passport switches exist in the network and if both DPN and Passport PF converters are configured with the backward compatibility option enabled.

where:

mm indicates the month the file was received

dd indicates the day the file was received

? is a variable indicating one of

- N a non-duplicate file—the accounting record is unique. This typically occurs for single-ended accounting.
- D a duplicate file—a matching accounting record exists from both ends of the call. This typically occurs for double-ended accounting.
- F a file containing corrupted raw accounting records. These files contain records that cannot be processed further.

PF with the backward compatibility option disabled

The published format (PF) backward compatibility option is described in section “Converting switch data to published format” (page 29).

If the PF backward compatibility option is disabled, PF file names have the following format:

```
pp_<datatype>_<date>_<nodeID>_<seq>_<?>.<ext>
```

where:

<datatype> is acc for accounting.

<date> is one of <MMDDhhmm> or <YYYYMMDDThhmmss>. <MMDDhhmm> is the date and time the file was opened on the Passport 6000 node (where MM=month, DD=day, hh=hour, and mm=minutes) or <YYYYMMDDThhmmss> is the date and time the file was opened on the Passport 7000/15000/20000 node (where YYYY=year, MM=month, DD=day, T=date/time delimiter, hh=hour, mm=minutes, and ss=seconds)

<nodeID|nodename> the Passport nodeID is an integer between 1 and 65536. The Passport nodename is an uppercase character string of 1 to 12 characters in length.

<seq> is the file sequence number assigned by the Passport node.

? is a variable indicating one of

- N a non-duplicate file—the accounting record is unique. This typically occurs for single-ended accounting.
- D a duplicate file—a matching accounting record exists from both ends of the call. This typically occurs for double-ended accounting.
- F a file containing corrupted raw accounting records. These files contain records that cannot be processed further.

<ext> is pf if the raw data was successfully converted to PF. This extension is pf_err if the raw data could not be successfully converted.

Passport SRS file names

Passport SRS data is written directly to directory /opt/MagellanMDP/data/mdp/dump/srs and the file name convention is

```
pp_srs_<YYYYMMDDThhmmss>_<nodename>
```

where:

<YYYYMMDDThhmmss> is the date and time the file was opened on the MDP (where YYYY=year, MM=month, DD=day, T=date/time delimiter, hh=hour, mm=minutes, and ss=seconds)

<nodename> is the Passport nodename.

.bdf is appended to the file name when a file is closed.

Example

```
pp_srs_19990926T141438_TOR32A
(open Passport SRS file)

pp_srs_19990926T141438_TOR32A.bdf
(closed Passport SRS file)
```

Statistics Retrieval System

The Statistics Retrieval System (SRS) polls Passport switches for non-spooled real-time statistical information. SRS formats the polled data values as bulk data format (BDF) and transfers the closed files to a performance or billing host for down-stream processing.

Valid statistics are limited to the operational attributes of a Passport component. Two types of statistics can be reported, raw attributes and delta values. Raw attributes are retrieved from the Passport and written to the BDF file. Delta values indicate the difference between the value of a raw attribute from the previous poll and the value of the raw attribute from the current poll.

A BDF file is created in the directory /opt/MagellanMDP/data/mdp/dump/srs for each Passport node. The BDF file is closed when the BDF file reaches a configurable maximum BDF record threshold or when a configurable time limitation is attained. The closed SRS BDF file can then be transferred to a customer host for downstream processing. For information about the naming convention of SRS data files, see “Passport SRS file names” (page 57).

You select the Passport components and attributes to poll using the MDP Configuration tool.

SRS can be used with Passport Enterprise software release 5.0, or higher, or any software release for Passport Carrier/Wireless.

To use the SRS, see

- “Configuring SRS” (page 145)
- “Selecting Passport components and attributes” (page 152)

Value-added applications

In addition to the standard features provided by the Management Data Provider (MDP), Passport customers can obtain licenses to use the following applications:

- Passport Outage Calculator
  uses alarm and state change notification (SCN) data collected from Passport switches. The Passport outage calculator determines which

components have experienced service interruptions, calculates the outages and generates a bulk data format (BDF) file with the resulting calculations.

A license, separate from the MDP license, is required to use the Passport Outage Calculator.

The Passport Outage Calculator is described in section "Passport outage calculation" (page 235).

- Availability Calculator
  calculates network availability statistics for switch components. Outage records generated by the Passport Outage Calculator and the DPN Outage Calculator can be used as input.

  A license, separate from the MDP license, is required to use the Passport Availability Calculator.

  The Availability Calculator is described in section "Availability calculation" (page 253).

- Availability Report Generator
  converts a BDF Availability Report file into formatted ASCII text output. This process is used to report availability statistics for customers that do not use a performance analysis application down-stream from the MDP.

  The Availability Report Generator is described in section "Availability report generation" (page 264).

DPN-100 support

The Management Data Provider (MDP) provides applications to automatically convert, archive, and transfer DPN-100 data.

The following topics are discussed in this section:

- "DPN-100 data flow" (page 60)
- "Datatypes" (page 62)
- "Data collection" (page 63)
- "DPN-100 data file names" (page 63)
- "Value-added applications" (page 68)

DPN-100 data flow

The basic flow of DPN-100 data through the Management Data Provider (MDP) is as follows:

1 The DPN performance metrics are collected on-switch and written to either a local disk or to a remote disk, if remote spooling is configured. This data is referred to as raw switch data in the context of the MDP.

2 The DPN data files are automatically transferred to the MDP over an X.25 network connection according to the accounting mode (TODA, 12-hour, or frame relay).

The MDP Disk Manager continually monitors MDP data disk space. A minimum disk space threshold is set and if this threshold is exceeded the MDP halts data collection and data conversion.

3 The raw data file is transferred to the MDP spool directory /opt/MagellanMDP/data/mdp/spool.

The raw data file name is described in "Raw data" (page 64).

4 The MDP DPN File Manager detects the raw data file in the spool directory.

If the MDP is configured to convert DPN-100 accounting data to published format (PF) and the DPN File Manager detects DPN accounting files in the spool directory, the DPN PF Converter is launched. For more information about converting DPN-100 accounting files to PF, see “Converting switch data to published format” (page 29).

The PF file names are described in “PF with the backward compatibility option enabled” (page 66) and “PF with the backward compatibility option disabled” (page 67).

If the MDP is configured to convert DPN-100 accounting data to bulk data format (BDF), the BDF Converter is launched.

For all other DPN datatypes, the BDF converter can be configured to launch. For more information about DPN datatypes, see “Datatypes” (page 62).

If the BDF Converter is launched, it obtains the appropriate schema and record description file (RDF) for the current raw data file and converts the data. For more information about converting raw data to BDF, see “Converting switch data to bulk data format” (page 25).

The BDF file names are described in “BDF data” (page 64) and “Short BDF file names” (page 65).

The converted data is written to the appropriate sub-directories of the MDP dump directory /opt/MagellanMDP/data/mdp/dump.

If the MDP is configured to archive BDF data, the individual BDF records are archived in the appropriate sub-directories of the MDP archive directory /opt/MagellanMDP/data/mdp/archive.

The BDF archive file name is described in “Archived BDF data” (page 66).

5 The DPN File Manager copies the raw data file from the spool directory to the MDP backup directory /opt/MagellanMDP/data/mdp/backup.

6 The MDP File Mover Manager detects the converted data file in the dump directory and transfers the data file to a customer host.

The File Mover Manager can also send the converted data file to a local directory on the MDP host. This feature can be used to create backups of PF files.

7 If outage calculation is configured, successfully converted alarm BDF files are placed in the directory /opt/MagellanMDP/data/mdp/oc/pp/primary for post processing by the Outage Calculator. Outage calculation is described in section "Outage calculation overview" (page 232).

Datatypes

The following DPN-100 datatypes are processed by the Management Data Provider (MDP):

- accounting (account, acc)
  including (but not limited to) records for frame relay and peak water mark (PWM), NUI option, inter-network option

  DPN accounting data (bulk data format (BDF) and published format (PF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

- statistics (stats, sta)
  or performance data, including (but not limited to) RM servers, AM/RM servers, API service, asynchronous service

  DPN statistics data (bulk data format (BDF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

- alarm (ala)
  data is used for analysis of switch and network down-time and other service-affecting problems.

  Refer to the DPN-100 documentation for descriptions of DPN alarm data.

- log
  data is used to monitor the operator command activity on a node.

  Refer to the DPN-100 documentation for descriptions of DPN log data.

Data collection

The Management Data Provider (MDP) File Collector process (mdpcol) collects DPN-100 accounting and performance data; it runs on the MDP host as a UNIX daemon waiting for an X.25 call with specific call user data (CUD) or a protocol ID to arrive. When the call request is received, the File Collector process transfers the DPN-100 files to the MDP spool directory /opt/MagellanMDP/data/mdp/spool. Successfully transferred files are automatically removed from the DPN-100 switch.

The File Collector is the front-end process to the DPN-100 network and provides the X.25 interface to the network for data transfer to the MDP host. DPN-100 switches place calls with a specific protocol ID (configurable, but unique) to the MDP File Collector process. The SunNet X.25 software listens for incoming X.25 calls based on a specific priority criteria.

Users who decide to control the transfer of files from a DPN-100 switch using the password option need to create the password file /opt/MagellanMDP/cfg/mdp/MDPCol.passwd on the MDP host; valid passwords must be on separate lines within the file.

DPN-100 records specify the year as two-digits in the date field. This format requires that the MDP apply an algorithm in each of its data conversion processes to determine the appropriate century (19xx or 20xx). This algorithm is as follows:

```
year = YY
YY >= 50 (indicates 20th century)
YY < 50 (indicates 21st century)
```

DPN-100 data file names

This section describes the formats of the DPN-100 data file names on the Management Data Provider (MDP).

- “Raw data” (page 64)
- “BDF data” (page 64)
- “Short BDF file names” (page 65)
- “Archived BDF data” (page 66)
- “PF with the backward compatibility option enabled” (page 66)

- "PF with the backward compatibility option disabled" (page 67)

Raw data

```
OAM_<type>_<YYMMDDhhmmss><seq>.<namsID>
```

where:

<type> is ACC for accounting, STA for statistics, ALA for alarms, or LOG for command logs.

<YYMMDDhhmmss> is the date and time that the file was created on the switch (where YY=year, MM=month, DD=day, hh=hour, mm=minutes, and ss=seconds). See "Data collection" (page 63) for century determination information.

<seq> is a two-digit file sequence number assigned by the DPN-100 switch.

<namsID> is the namsID of the DPN-100 switch that collected the record. The namsID is appended to the filename to indicate that the file is closed.

Example

```
OAM_ACC_94110115490519 (open accounting file)
OAM_ACC_94110115490519.2700 (closed accounting file)
```

BDF data

Bulk data format (BDF) files have the following naming format:

```
dpn_<datatype>_<date>_<namsID>_<seq>.<ext>
```

where:

<datatype> is acc for accounting, sta for statistics, ala for alarms, and log for logs.

<date> is the date and time the file was opened; uses the format <YYMMDDhhmmss> (where YY=year, MM=month, DD=day, hh=hour, mm=minutes, and ss=seconds). See "Data collection" (page 63) for century determination information.

<namsID> the namsID of the DPN-100 that generated this file.

<seq> is the file sequence number assigned by the DPN-100.

<ext> is bdf if the raw data was successfully converted to BDF. This extension is err if the raw data could not be successfully converted.

> ***Note:*** If the file name includes the .err extension, this file contains raw records that could not be converted.

Example

```
dpn_acc_941001154908_2750_33.bdf
(converted accounting BDF records)

dpn_acc_941101154905_2700_19.err
(errored statistics raw records)
```

Short BDF file names

A file name limitation exists for transferring BDF files to an IBM customer host; a maximum of 16 characters can be used. If the standard BDF file name format is used, the transfer of files to IBM customer hosts will fail. To use the short BDF file name format, see “Using short BDF file names” (page 89).

> ***Note:*** The File Mover process truncates the namsID to the first 4 characters. These first 4 characters must be numeric. The MDP does not check for unique naming. If short file names are used, it is your responsibility to ensure that the first 4 characters of the namsID are unique.

The short file naming convention for BDF files is

```
d<t><mmddhh.MM><seq#><namsID>
```

where:

d is for DPN-100.

<t> is datatype. a for accounting, s for statistics, l for logs, and m for alarms.

<mmddhh.MM> is the date the file was opened on the DPN-100 (where mm=month, dd=day, hh=hour, and MM=minutes).

<seq> is the 2 digits of the DPN-100 assigned file sequence number.

<namsID> is the first 4 digits of the DPN-100 namsID.

Archived BDF data

BDF archive files use the same file name format as BDF files except that the date of the records is appended to the end of the filename, before the extension.

```
dpn_<datatype>_<date>_<namsID>_<seq>_<split-by-
date>.BDF
```

where:

<split-by-date> is the date on the data records, not the date of the raw data file.

PF with the backward compatibility option enabled

The published format (PF) backward compatibility option is described in section “Converting switch data to published format” (page 29).

If the PF backward compatibility option is enabled, PF file names have the following format:

```
Dpn_TPACT<?>.mmddHHMM (open file)
Dpn_TPACT<?>.mmddHH (closed file)
```

the daily file

```
TPACT<?>.mmdd
```

Note: The daily published format file contains both Passport and DPN accounting records if both DPN and Passport switches exist in the network and if both DPN and Passport PF converters are configured with the backward compatibility option enabled.

where:

mm indicates the month the file was received

dd indicates the day the file was received

? is a variable indicating one of

- N a non-duplicate file—the accounting record is unique. This typically occurs for single-ended accounting.
- D a duplicate file—a matching accounting record exists from both ends of the call. This typically occurs for double-ended accounting.

- E a file containing published format records from a DPN accounting file that can only be partially converted. View this file using PF File Viewer; see “Viewing Published Format files” (page 201).
- G a file containing corrupted raw accounting records. These files contain records that cannot be processed further.

PF with the backward compatibility option disabled

The published format (PF) backward compatibility option is described in section “Converting switch data to published format” (page 29).

If the PF backward compatibility option is disabled, PF file names have the following format:

```
dpn_<datatype>_<date>_<namsID>_<seq>_<?>.<ext>
```

where:

<datatype> is acc for accounting.

<date> is <YYMMDDhhmmss>. <YYMMDDhhmmss> is the date and time the file was opened on the DPN-100 (where YY=year, MM=month, DD=day, hh=hour, mm=minutes, and ss=seconds)

<namsID> the namsID of the DPN-100 that generated this file.

<seq> is the file sequence number assigned by the DPN-100.

? is a variable indicating one of

- N a non-duplicate file—the accounting record is unique. This typically occurs for single-ended accounting.
- D a duplicate file—a matching accounting record exists from both ends of the call. This typically occurs for double-ended accounting.
- E a file containing published format records from a DPN accounting file that can only be partially converted. View this file using PF File Viewer; see “Viewing Published Format files” (page 201).
- G a file containing corrupted raw accounting records. These files contain records that cannot be processed further.

<ext> is pf if the raw data was successfully converted to PF. This extension is pf_err if the raw data could not be successfully converted.

Value-added applications

In addition to the standard features provided by the Management Data Provider (MDP), DPN-100 customers can obtain licenses to use the following applications:

- DPN Outage Calculator
  uses alarm data collected from DPNs and converted to bulk data format (BDF) by the MDP. The DPN outage calculator determines which components have experienced service interruptions, calculates the outages, and generates a bulk data format (BDF) file with the resulting calculations.

  A license, separate from the MDP license, is required to use the DPN Outage Calculator.

  For more information about the DPN Outage Calculator, see "Outage calculation overview" (page 232).

- Availability Calculator
  calculates network availability statistics for switch components. Outage records generated by the DPN Outage Calculator and Passport Outage Calculator can used as input.

  A license, separate from the MDP license, is required to use the Availability Calculator.

  For more information about the Availability Calculator, see "Availability calculation" (page 253).

- Availability Report Generator
  converts a BDF Availability Report file into formatted ASCII text output. This process is used to report availability statistics for customers that do not use a performance analysis application down-stream from the MDP.

  For more information about the Availability Report Generator, see "Availability report generation" (page 264).

Vector support

The Management Data Provider (MDP) provides applications to automatically collect, convert, archive, and transfer Vector data.

The following topics are discussed in this section:

- "Vector data flow" (page 69)
- "Datatypes" (page 71)
- "Vector data conversion" (page 71)
- "Vector data file names" (page 75)

Vector data flow

The basic flow of Vector data through the Management Data Provider (MDP) is as follows:

1 The Vector data is collected on the switch and transferred to the MDP every 5 minutes using the file transfer protocol (FTP). This data is referred to as raw switch data in the context of the MDP.

Vector accounting data is transferred separately from Vector statistics.

2 The MDP collects Vector records for a one hour period in the MDP spool directory /opt/MagellanMDP/data/mdp/spool.

The MDP Disk Manager continually monitors MDP data disk space. A minimum disk space threshold is set and if this threshold is exceeded the MDP halts data collection and data conversion.

3 The Vector File Manager detects the closed raw data file in the spool directory and moves the file to the MDP merge directory /opt/MagellanMDP/data/mdp/merge.

For accounting records, the Vector File Manager determines the billing record file type (legacy billing records or Egress billing records). This is determined by the file name.

Note: The Vector call accounting records must be either legacy or Egress billing records. The Vector File Manager will not accept a combination of both record types from one switch.

For legacy billing records, the Vector File Manager launches an aggregator process to produce aggregated files that contain data associated with individual fabrics within a Vector switch.

After producing the aggregated billing files, the Vector File Manager launches a correlator process to combine the aggregated files associated with individual fabrics on the same Vector switch, which in turn is used to produce a correlated file that contains hourly data for each Vector switch.

For Egress billing records, the Vector File Manager launches a process which combines the aggregation and correlation processes, described above, for Egress billing records.

For performance records, the Vector File Manager launches an aggregator process to produce aggregated files that contain data associated with individual fabrics within a Vector switch. The Vector File Manager then launches another process to combine the aggregated files associated with individual fabrics on the same Vector switch, which in turn is used to produce a correlated file that contains hourly data for each Vector switch.

4 The BDF Converter is launched. It obtains the appropriate schema and record description file (RDF) for the current raw data file and converts the data. For more information about converting raw data to BDF, see “Converting switch data to bulk data format” (page 25).

The converted data is written to the appropriate sub-directories of the MDP dump directory /opt/MagellanMDP/data/mdp/dump.

For information about the Vector datatypes, see “Datatypes” (page 71).

5 The Vector File Manager copies the raw data file from the spool directory to the MDP backup directory /opt/MagellanMDP/data/mdp/backup.

6 The MDP File Mover Manager detects the converted data file in the dump directory and transfers the data file to a customer host.

The File Mover Manager can also send the converted data file to a local directory on the MDP host. This feature can be used to create backups of converted data files.

Datatypes

The following Vector datatypes are processed by the Management Data Provider (MDP):

- accounting (account, acc)
  only one record type is generated

  Vector accounting data (bulk data format (BDF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

- statistics (stats, sta)
  or performance data, including (but not limited to) board, netmod, PSM, DS1, E1, OC3, OC12

  Vector statistics data (bulk data format (BDF)) is described in detail in 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

Vector data conversion

The Management Data Provider (MDP) converts Vector accounting and performance data using a process different than that used by Passport or DPN.

Vector File Manager

The Vector File Manager (*mdpvssmgr*) handles data differently than either the DPN-100 or Passport File Managers. This process aggregates and correlates data differently for different Vector billing types: legacy and egress.

This process moves Vector data files to the merge directory when there is 60 minutes worth of data.

For billing data files, the Vector File Manager performs a check on each fabric to ensure the billing type is consistent across all fabrics. If the billing type is consistent across all fabrics, the File Manager determines the billing type; legacy or Egress. If the billing type is not consistent across all fabrics (that is, a mixed billing configuration exists on the Vector switch) the File Manager will invoke the combined Aggregator/Correlator used for Egress billing records, raise an alarm to indicate that a mixed billing configuration was encountered, and all legacy billing files are moved to error status.

If the billing type is determined to be legacy, or the data files contain performance data, the File Manager starts an Aggregator process. These processes (*accaggregator* or *pmaggregator*) produce aggregated files containing data associated with individual fabrics within a Vector switch. The File Manager process then starts a Correlator process (*acccorrelator* or *pmcorrelator*) to produce files combining the aggregated files associated with individual fabrics on the same Vector switch, and to produce a correlated file containing the hourly billing data for each Vector switch.

If the billing type is determined to be Egress, or in the case of inconsistent billing types, the File Manager starts a combined Aggregator/Correlator process to: aggregate files containing data associated with individual fabrics within a Vector switch; combine the aggregated files associated with individual fabrics on the same Vector switch; and produce a correlated file containing the hourly billing data for each Vector switch.

Vector File Manager and missing Vector data

The Vector File Manager (*mdpvssmgr*) is responsible for retrieving data files from a secondary MDP host. The File Manager, on the primary MDP host, retrieves any data files found in the restore directory on the secondary MDP host. The retrieval of data files by the File Manager has the following constraints:

- It only processes files from switches that are configured as part of the data collection system.
- If the initial retrieval of files from the secondary MDP host fails, the error is logged and a second attempt is made to retrieve the files.
- If files are not found on the primary or secondary MDP host, the File Manager logs the error and proceeds with the files that are present. Aggregation and correlation only takes place on the files that are present.
- Data files that are retrieved from the secondary MDP host are placed in the spool directory of the primary MDP host for normal MDP processing.

Aggregating Vector call records (legacy billing)

For Vector switches which employ the legacy billing method, you can execute the call record aggregator without executing the call record correlator.

Aggregation combines records associated with individual Vector switch fabrics (identified by their call connection identifier). An aggregated file contains only data associated with one Vector switch fabric. By default, raw data files are retrieved from the merge directory and aggregated files are stored in the merge directory. Successfully processed input files are automatically deleted from the merge directory.

Under normal operation, the call record aggregator is invoked by the Vector File Manager. The aggregator can also be run manually to process files outside the normal operating process. If the aggregator is run manually, it is recommended that you provide a different directory location for the files using the `-r` option to avoid interference with any other aggregator processes using the default merge directory.

Aggregating Vector performance data

Aggregation combines records associated with individual Vector switch fabrics (identified by the equipment type). An aggregated file contains only data associated with one Vector switch fabric. By default, raw data files are retrieved from the merge directory and aggregated files are stored in the merge directory. Successfully processed raw input files are automatically deleted from the merge directory.

Under normal operation, the performance record aggregator is started by the Vector File Manager. The aggregator can also be run manually to process files outside the normal operating process. If the aggregator is run manually, it is recommended that you provide a different directory location for the files using the `-r` option to avoid interference with any other aggregator processes using the default merge directory.

Correlating Vector call records (legacy billing)

For Vector switches that employ the legacy billing method, You can execute the call record correlator without executing the call record aggregator. You must have previously executed the call record aggregator.

Correlation combines the aggregated files associated with individual fabrics on the same Vector switch into one correlated file for each Vector switch. By default, aggregated files are retrieved from the merge directory and the correlated files are stored in the merge directory. Successfully processed input files are automatically deleted from the merge directory.

Under normal operation, the call record correlator is started by the Vector File Manager. The correlator can also be run manually to process files outside the normal operating process. If the call record correlator is run manually, you need to provide a different directory location for the files using the `-r` option to avoid interfering with any other correlator processes using the default merge directory.

Correlating Vector call records (Egress billing)

For Vector switches that use the Egress billing method, there is no separation of the aggregator and correlator processes.

Aggregation combines records associated with individual Vector switch fabrics (identified by their call connection identifier). An aggregated file contains only data associated with one Vector switch fabric. By default, raw data files are retrieved from the merge directory and aggregated files are stored in the merge directory. Successfully processed input files are automatically deleted from the merge directory.

Correlation combines the aggregated files associated with individual fabrics on the same Vector switch into one correlated file for each Vector switch. By default, aggregated files are retrieved from the merge directory and the correlated files are stored in the merge directory. Successfully processed input files are automatically deleted from the merge directory.

Under normal operation, the Egress call record correlator is started by the Vector File Manager. The correlator can also be run manually to process files outside the normal operating process. If the call record correlator is run manually, you need to provide a different directory location for the files using the `-dir` option to avoid interfering with any other correlator processes using the default merge directory.

Correlating Vector performance data

Correlation combines the aggregated files associated with individual fabrics on the same Vector switch into one correlated file for each Vector switch. By default, aggregated files are retrieved from the merge directory and the correlated files are stored in the merge directory. Successfully processed input files are automatically deleted from the merge directory.

Under normal operation, the performance record correlator is started by the Vector File Manager. The correlator can also be run manually to process files outside the normal operating process. If the correlator is run manually, you need to provide a different directory location for the files using the `-r` option in order to avoid interference with any other correlator processes using the default merge directory.

Vector data file names

This section describes the formats of the Vector data file names on the Management Data Provider (MDP).

- "Raw data" (page 75)
- "Aggregated file names" (page 77)
- "Correlated file names" (page 77)
- "BDF data" (page 78)
- "Short BDF file names" (page 79)

Raw data

For those Vector switches using legacy billing, the following is the raw data file name format:

```
vss_<datatype>.<date>.<interval>.<switchID>.
<fabricID>.<co|cc>
```

For those Vector switches using Egress billing, the following is the raw data file name format:

```
vss_<datatype>.<date>.<interval>.<swact_seq>.
<switchID>.<fabricID>.<co|cc>
```

where:

vss indicates Vector switch data.

<datatype> is account for billing data or statistics for performance data.

<date> is the start date and time of the data collection interval. The format is YYYYMMDDhhmm (year, month, day, hour, minute). All values are subject to the following constraints:

hhmm=hh+I*(interval), where interval is usually 5 and I is a positive integer. This formula allows the MDP to determine if any files are missing.

The next hh00 partition must not be missed.

<interval> is the amount of time (in minutes) of the billing interval. This value is usually 5 minutes.

<swact_seq> is the SWACT sequence, used to detect a restart or fabric SWACT. This file name attribute is only used by Egress billing raw data files and has the following format fssrr where:

- f represents the fabricID
- ss represents a SWACT sequence number. This counter wraps around from 00 to 99 and increments each time a fabric SWACT occurs. This value is absolute and includes all fabric SWACTs from time of fabric initialization.
- rr represents a restart sequence number. This counter wraps around from 00 to 99 and increments each time a fabric restart occurs. This value is absolute and includes all fabric restarts from time of fabric initialization.

<switchID> is the six-digit numeric switch identifier of the Vector switch.

<fabricID> is the one-digit numeric identifier for the slot into which the fabric is inserted; it can have a value from 0 to 3.

<co | cc> is a two-digit letter code used to identify if the file is open or closed. Closed is indicated by cc and open is indicated by co.

> ***Note:*** The PAMS board in a Vector switch contains the switchID for the switch and is used to name the data files from the switch. When the board is changed, the switch data collection system has to be reconfigured.

Aggregated file names

The aggregation process applies to legacy billing and aggregates unprocessed raw Vector files found in the merge directory within one hour. Aggregated files are also stored in the merge directory. Records that cannot be aggregated are placed in an error file in the merge directory. The naming convention for aggregated files is

```
vss_<datatype>_<date>_<switchID>_<fabricID>.ext
```

where:

vss indicates Vector switch data.

<datatype> is account for billing data and stats for performance data.

<date> is a date in the format YYYYMMddhhmm where YYYY=year, MM=month, dd=day, hh=hour, and mm=minutes.

<switchID> is the six-digit numeric switch identifier of the Vector switch.

<fabricID> is the one-digit numeric identifier for the slot into which the fabric is inserted; it can have a value from 0 to 3.

<ext> is agg for an aggregated file and err for an error file.

Example

```
vss_account.199612252330.345.2.agg
```

is the file name of an aggregated Vector billing file with a switchID of 345 and a fabricID of 2.

Correlated file names

The correlation process correlates unprocessed aggregated Vector files found in the merge directory. Correlated files are stored in the merge directory. If an error occurs while a file is being correlated, it is renamed with a suffix of err. The naming convection for a correlated file is

```
vss_<datatype>_<date>_<switchID>_<fabricID>.ext
```

where:

vss indicates Vector switch data.

<datatype> is account for billing data and stats for performance data.

<date> is a date in the format YYYYMMddhhmm where YYYY=year, MM=month, dd=day, hh=hour, and mm=minutes.

<switchID> is the six-digit numeric switch identifier of the Vector switch.

<fabricID> is the one-digit numeric identifier for the slot into which the fabric is inserted; it can have a value from 0 to 3.

<ext> is corr for an aggregated file and err for an error file.

Example
`vss_stats_199612252330_345_2_corr`

is the file name of an correlated Vector statistics file with a switchID of 345 and a fabricID of 2.

BDF data

Bulk data format (BDF) files have the following naming format:

```
vss_<datatype>_<date>_<switchID>_0.<ext>
```

where:

<datatype> is acc for accounting, sta for statistics, ala for alarms, and log for logs.

<date> is the date and time the file was opened; uses the format <YYYYMMDDhhmm> (where YYYY=year, MM=month, DD=day, hh=hour, and mm=minutes).

<switchID> the switchID of the Vector that generated this file.

<ext> is bdf if the raw data was successfully converted to BDF. This extension is err if the raw data could not be successfully converted.

Note: If the file name includes the .err extension, this file contains raw records that could not be converted.

Example

```
vss_acc_199410011549_2750_0.bdf
(converted accounting BDF records)

vss_acc_199411011549_2700_0.err
(errored statistics raw records)
```

Short BDF file names

A file name limitation exists for transferring BDF files to an IBM customer host; a maximum of 16 characters can be used. If the standard BDF file name format is used, the transfer of files to IBM customer hosts will fail. To use the short BDF file name format, see “Using short BDF file names” (page 89).

The short file naming convention for BDF files is

```
v<t><mmddhh.MM><switchID>
```

where:

v is for Vector.

<t> is datatype. a for accounting or s for statistics.

<mmddhh.MM> is the date the file was opened on the Vector (where mm=month, dd=day, hh=hour, and MM=minutes).

<switchID> is the Vector switchID.

Chapter 2
Configuration

This section describes the customization of the Management Data Provider (MDP) configuration.

To install MDP software and to configure a new MDP host to collect Passport performance metrics, see 241-6001-100 *Preside MDM Installer Guide*.

Initial configuration of the Management Data Provider (MDP) is performed by the Preside Multiservice Data Manager (MDM) QuickStart wizard. This basic configuration applies to Passport data collection, only. Initial configuration includes:

- license registration
- network connectivity
- validation of a UNIX userID for the MDP administrator
- Passsport network configuration
- starting Passport data collection at midnight each day
- data conversion of Passport data to BDF using the supplied default data model
- starting the Passport Data Model Manager (mdpdmm)
- starting the MDP Disk Manager (mdpdiskmgr)

Customizing an MDP configuration

This section provides instructions for customizing a Management Data Provider (MDP) configuration.

Prerequisites

Before configuring the Management Data Provider (MDP) software, ensure that you have:

- reviewed 241-6001-102 *Preside MDM Planning Guide*.
- reviewed the Preside Multiservice Data Manager (MDM) Release Supplement for this release.
- installed the MDM and MDP software; see 241-6001-100 *Preside MDM Installer Guide*.
- read the section about the "MDP Configuration tool" (page 85).
- launched the MDP Configuration tool; see "Launching the MDP Configuration tool" (page 87).

  Experienced MDP administrators can manually edit the MDP configuration files instead of using the MDP Configuration tool. The applicable MDP configuration files are identified in each of the steps in the following procedure.

Configuring MDP features

MDP features can be configured using the MDP Configuration tool or by manually changing the configuration files.

1 Select **File Mover**.

To identify customer hosts, supply login information, and assign the transfer of converted data files to customer hosts, see "Configuring file transfers to customer hosts" (page 87).

This configuration can be performed manually using the file /opt/MagellanMDP/cfg/mdp/MDPMover.cfg.

2 Select **Disk Manager**.

To configure data file retention, see "Configuring data file retention" (page 94).

To configure the minimum MDP disk space requirements and the Disk Manager log level, see “Launching the MDP Disk Manager and setting the minimum disk space” (page 192).

This configuration can be performed manually using the file /opt/MagellanMDP/cfg/mdp/MDPClean.cfg.

3 To configure Passport data collection and data conversion, see “Configuring MDP for Passport” (page 125).
This configuration can be performed manually using the files: /opt/MagellanMDP/cfg/mdp/MDPFPSched.cfg, and /opt/MagellanMDP/cfg/mdp/MDPPPMgr.cfg.

To configure DPN-100 data collection and data conversion, see “Configuring MDP for DPN-100” (page 161).
This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPDPNMgr.cfg.

To configure Vector data collection and data conversion, see “Configuring MDP for Vector” (page 175).
This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPVSSMgr.cfg.

4 To sort bulk data format (BDF) data using dates and nodeIDs, select **BDF Archiving**. This selection applies to Passport or DPN switch data, only.

Archiving BDF data is described in section “Configuring BDF archiving” (page 96).

This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPBDFArch.cfg.

5 To generate audit reports, select **Audits**.

MDP audit reports and how to generate them is described in section “Configuring MDP file processing audits” (page 101).

This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPAudit.cfg.

6 To configure MDP SNMP trap and/or alarm generation, select **Surveillance**.

For more information, see “Configuring MDP surveillance” (page 105).

This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPTG.cfg.

7 To archive MDP logs, select **Log Archiving**.

For more information, see “Configuring log archiving” (page 103).

This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPLogArch.cfg.

8 To customize the MDP data directories, see “Customizing MDP data directories” (page 106).

9 To configure the Passport Statistic Retrieval System (SRS), see “Configuring SRS” (page 145).

This configuration can be performed manually using the file: /opt/MagellanMDP/cfg/mdp/MDPSRS.cfg.

10 To configure Passport outage calculation, see “Configuring the Outage Controller” (page 115) and “Configuring outage calculation” (page 156).

This configuration can be performed manually using the files: /opt/MagellanMDP/cfg/mdp/MDPOCtrl.cfg. and /opt/MagellanMDP/cfg/mdp/MDPPPOC.cfg.

11 To configure DPN-100 outage calculation, see “Configuring the Outage Controller” (page 115) and “Configuring outage calculation” (page 171).

This configuration can be performed manually using the files: /opt/MagellanMDP/cfg/mdp/MDPOCtrl.cfg. and /opt/MagellanMDP/cfg/mdp/MDPDPNOC.cfg.

12 To configure availability calculation, see “Configuring availability calculation” (page 118).

13 If the following MDP processes were configured but are not currently controlled by the Server Administration (SVM) tool, configure the SVM tool to control them:

- Passport Data Model Manager (mdpdmm)
- File Mover Manager (mdpfmmgr)
- DPN-100 Data Collector (mdpcol)
- Disk Manager (mdpdiskmgr)
- Passport Statistics Retrieval System (mdpsrs)
- Passport File Prober Manager (mdpfpmgr)
- Passport File Manager (mdpppmgr)
- DPN-100 File Manager (mdpdpnmgr)
- Vector File Manager (mdpvssmgr)

MDP Configuration tool

This section describes the MDP Configuration tool.

Common buttons

Each MDP Configuration tool window includes four buttons common to all MDP Configuration tool windows. These buttons are consistently located at the bottom of each window.

- **Save <window>**
  saves the values in the current window to the configuration file.

  You are prompted for confirmation to save the indicated configuration file.

  If an MDP server uses the indicated configuration file and this MDP server is currently running, you are prompted for confirmation to restart the MDP server (for example, mdpppmgr).

  Note: The **Save** button saves the configuration settings from the current MDP Configuration tool window, only.

- **Refresh <window>**
  resets the values in the current window to the values in the configuration file.

  A dialog box requests that you confirm the refresh.

- **Exit**
  terminates the MDP Configuration tool.

  A dialog box is displayed requesting that configuration updates not previously applied be saved.

- **Help**
  displays a dialog box that describes the current MDP Configuration tool window.

Window status

The status of each MDP Configuration tool window can be visually determined using the tabs in the panel on the left side of each window. See the table “Window status by tab icon” (page 86) for a description of the shape and color of a tab icon.

Table 3
Window status by tab icon

Icon shape	Icon color	Description
circle	grey	values have not changed
triangle	yellow	values have changed
diamond	red	error in values

Logs

All information related to MDP configuration, including error and warning messages, is recorded in the configuration log file. The configuration log file is described in section “Log file names” (page 204).

Customizing the MDP Configuration tool

The MDP Configuration tool can be customized to display only those MDP configuration windows that you require. The default is that all MDP configuration windows are displayed.

1. Exit from the MDP Configuration tool.
2. Copy the tool configuration file using the command

   ```
   cp /opt/MagellanMDP/lib/mdp/cfg/MDPCfgGuiPanels.cfg
      /opt/MagellanMDP/cfg/mdp/MDPCfgGuiPanels.cfg
   ```

3. Edit the file /opt/MagellanMDP/cfg/mdp/MDPCfgGuiPanels.cfg.

   Each configuration tool window is indicated with a **Y** or an **N**. **Y** indicates that the configuration tool window is displayed. **N** indicates that the configuration tool window is not displayed.
4. Launch the MDP Configuration tool.

Launching the MDP Configuration tool

Launch the Management Data Provider (MDP) Configuration tool using one of the following methods.

Access from the Preside MDM window

1 From the Preside MDM window, as the MDP administrator userID, select **Accounting -> Management Data Provider Administration**.

The MDP Configuration tool opens.

The contents of the MDP configuration files are retrieved.

Access from the UNIX command line

1 From a UNIX xterm, as the MDP administrator userID, type

```
/opt/MagellanMDP/bin/gmdpconfig &
```

The MDP Configuration tool opens.

The contents of the MDP configuration files are retrieved.

Configuring file transfers to customer hosts

The Management Data Provider (MDP) automatically transfers converted switch data files to customer hosts for billing or performance analysis. Other file types can also be automatically transferred. File transfer to customer hosts is described in section “Transferring data to down-stream applications” (page 33).

Use the **File Mover** window for

- “Configuring customer host connections” (page 88)
- “Transferring files to customer hosts” (page 90)
- “Checking file type destinations” (page 91)
- “Backing up converted files” (page 91)
- “Transferring files to multiple directories on the same host” (page 92)
- “Setting the File Mover Manager log level” (page 92)
- “Scheduling customized data analysis programs” (page 93)
- “Backing up daily published format files” (page 93)

For a description of how the MDP handles file transfer failures, see “File transfer failures” (page 94).

Configuring customer host connections

The Management Data Provider (MDP) transfers converted billing and performance data to selected customer hosts. Before the MDP can perform these file transfers, access to the customer hosts must be configured.

Note: If you reconfigure your customer hosts, ensure that any remaining data files are sent to the intended customer host.

Adding a customer host

1. Using the MDP Configuration tool, select **File Mover**.
2. Click **Edit Host**.

   The Edit Host window is displayed.
3. Type the following information in the data entry boxes:

   a. In the data entry box **Hostname**, type the hostname or IP address of the customer host.

   b. In the data entry box **Userid**, type a userID for accessing the customer host.

   c. In the data entry box **Password**, type the password for the customer host userID.

   The password is stored in an encrypted format.
4. To transfer BDF files to this customer host with short file names, click **Use Shortened Names**.

   A check mark is displayed in the button box.

   The default is this button is unchecked.
5. Click **Save Host**.

   The new entry is added to the configuration file /opt/MagellanMDP/cfg/mdp/MDPMover.cfg.
6. Click **Cancel**.

   The Edit Host window closes.
7. To use the new customer host, follow the instructions in section “Transferring files to customer hosts” (page 90).

Changing the password for a customer host

1. Using the MDP Configuration tool, select **File Mover**.
2. Click **Edit Host**.

   The Edit Host window is displayed.
3. Click the pull-down button beside **Select Host** and select the customer host:userID to change.
4. Type the new password in the data entry box **Password**.

   The password is stored in an encrypted format.
5. Click **Save Host**.

   The entry is updated in the configuration file /opt/MagellanMDP/cfg/mdp/MDPMover.cfg.
6. Click **Cancel**.

   The Edit Host window closes.
7. Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Using short BDF file names

To accommodate IBM customer hosts, bulk data format (BDF) files can be transferred with short file names. Passport short BDF file names are described in section "Short BDF file names" (page 54). DPN short BDF file names are described in section "Short BDF file names" (page 65). Vector short BDF file names are described in section "Short BDF file names" (page 79).

Note: Passport Statistics Retrieval System BDF file names, Passport and DPN Outage and Availability Report BDF file names are not shortened using this procedure.

1. Using the MDP Configuration tool, select **File Mover**.
2. Click **Edit Host**.

   The Edit Host window is displayed.
3. Click the pull-down button beside **Select Host** and select the customer host:userID to change.
4. To shorten BDF filenames when files are transferred to this customer host, click **Use Shortened Names**.

If MDP was previously configured to shorten BDF filenames for this customer host and you now want to halt this file name conversion, click **Use Shortened Names**.

5 Click **Save Host**.

The entry is updated in the configuration file /opt/MagellanMDP/cfg/mdp/MDPMover.cfg.

6 Click **Cancel**.

The Edit Host window closes.

7 Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Transferring files to customer hosts

Configure the File Mover Manager to transfer files from the Management Data Provider (MDP) to a maximum of 3 customer hosts for each file type.

Note 1: Before configuring the File Mover Manager, configure access to customer hosts using the File Mover button **Edit Host** "Configuring customer host connections" (page 88).

Note 2: If Availability Reports are transferred to a customer host, the reports are no longer available to the Management Data Provider (MDP) for further processing (by the MDP Report Generator, for example). If the Availability Reports are required for further MDP processing, see "Backing up converted files" (page 91).

1 Using the MDP Configuration tool, select **File Mover**.

2 The **File Type** is a pull-down list. Select the file type to be transferred (for example, Passport Accounting BDF).

3 Click **enabled** in the **Customer Host 1** panel.

A check mark is displayed.

4 **hostname** in the **Customer Host 1** panel is a pull-down list. Select the customer host:userID for the selected File Type from the **hostname** list.

5 To specify a directory on **Customer Host 1** where the selected file type will be transferred, click **Set destination ftp directory** and type the directory pathname in the data entry box.

A check mark is displayed.

The default is this option is not selected and the files are transferred to the default directory determined by the FTP server.

6 To transfer the selected file type to other customer hosts (or the same customer host using a different userID and destination directory), repeat steps 3, 4 and 5 for **Customer Host 2** and **Customer Host 3**.

7 Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Checking file type destinations

You can verify the destination customer host(s) for each Management Data Provider (MDP) file type.

1 Using the MDP Configuration tool, select **File Mover**.

2 Click **Summary**.

A pop-up window displays a list of the possible file types. If a file type is configured for transfer to a customer host, the hostname (or IP address) and a userID is displayed beside the file type.

Backing up converted files

After transferring a converted data file (bulk data format (BDF) and published format (PF)) to a customer host, the File Mover Manager deletes the file from the Management Data Provider (MDP) host. Use the File Mover Manager to copy the converted data file to a local MDP directory before the file is removed.

1 Using the MDP Configuration tool, select **File Mover**.

2 Use the procedure “Adding a customer host” (page 88) to add the following host information:

- host name or IP address of the local MDP
- a userID and password for the local MDP

3 Use the procedure “Configuring file transfers to customer hosts” (page 87) to specify the local MDP as a customer host.

4 Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Transferring files to multiple directories on the same host

Converted data files can be transferred to multiple directories on the same customer host.

1. Configure file transfers to the first directory location using the procedure “Transferring files to customer hosts” (page 90).
2. On the MDP, as userID **root**, open an xterm.
3. Add an alias to an existing host in the file /etc/hosts.

   `<IP_address> <hostname> <alias1> <alias...>`
4. Using the MDP Configuration tool, as the MDP Administrator, select **File Mover**.
5. Use the procedure “Adding a customer host” (page 88) to add the following host information:
   - the alias created in step 3 as the **Hostname**
   - a userID and password on the host
6. Use the procedure “Transferring files to customer hosts” (page 90) to add the following file transfer information:
   - the alias created in step 3 and added to the MDP in step 5 as the **hostname**
   - the second directory on the host
7. Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Setting the File Mover Manager log level

The File Mover Manager logs error messages to a daily log file in directory /opt/MagellanMDP/data/mdp/admin. The File Mover Manager logs are described in section “MDP logs” (page 203).

1. Using the MDP Configuration tool, select **File Mover**.
2. Click the button box beside **Process Log Level**.

   The log levels are indicated (0 - 4).
3. Click the appropriate log level.

   Log levels are described in section “Log levels” (page 207).

   The default level is 3.

Note: To report the filenames of files successfully transferred to customer hosts , set the log level to 4.

4 Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Scheduling customized data analysis programs

Use the File Mover Manager to execute a single user-defined data analysis program daily, at midnight. This program uses available daily published format (PF) accounting files as input. Only those PF files generated before the current date are read.

Note: This option is only applicable if the published format backward compatibility option is enabled for DPN-100 or Passport; see section "Converting switch data to published format" (page 29).

1 Using the MDP Configuration tool, select **File Mover**.

2 Click **Perform additional processing on daily PF file** in the **Published Format Details** panel.

A check mark is displayed.

The default is this option is not selected.

3 Type the absolute path for the program in the text entry box **Program to execute**.

The default for this field is a blank entry.

4 Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

Backing up daily published format files

Use the File Mover Manager to archive the daily published format (PF) file.

Note: This option is only applicable if the published format backward compatibility option is enabled for DPN-100 or Passport; see section "Converting switch data to published format" (page 29).

1 Using the MDP Configuration tool, select **File Mover**.

2 Click **Perform backup of daily PF file** in the **Published Format Details** panel.

A check mark is displayed.

The default is this option is not selected.

3 Click **Save File Mover** to save the configuration change and to restart the File Mover Manager.

File transfer failures

If the File Mover fails to successfully transfer a data file

- the File Mover logs an error message that indicates the affected file and customer host. The Management Data Provider (MDP) continues to attempt the data transfer every 5 minutes until the problem is corrected or until the customer host configuration is changed.
- the File Mover does not resend a file to a host if the file has been successfully transferred to the host previously,

If the File Mover Manager fails, any File Mover processes running at that time will continue to run. If the File Mover Manager and File Mover processes fail at the same time (for example, complete workstation shutdown), the File Mover Manager ensures that the appropriate File Mover processes are restarted.

Configuring data file retention

The Management Data Provider (MDP) Disk Manager

- can be configured to retain data files for any length of time.
- coordinates the removal of data files. Data files are automatically removed at 0100 hours on the day that they reach their configured threshold.
- continually monitors MDP data file disk space. A minimum disk space threshold can be configured using a procedure in this section and when this threshold is exceeded the MDP halts data conversion. If data file disk space usage exceeds 90% of the configured threshold, SNMP traps and MDP logs are generated to alert you of this condition.

CAUTION
The Passport Statistics Retrieval System (SRS) does not stop polling when the minimum disk space threshold is exceeded. This can cause spooled data collection to fail due to a lack of disk space.

Use the MDP Disk Manager Configuration window for

- "Setting the data file retention time" (page 95)
- "Setting the minimum available disk space" (page 96)
- "Setting the Disk Manager log level" (page 96)

Setting the data file retention time

Configure the retention time for each indicated data directory.

1. Using the MDP Configuration tool, select **Disk Manager**.
2. Review each of the indicated MDP directories under the label **Location**.
3. Confirm that the retention time, specified under the label **number of days to keep files**, is acceptable. Retention time is specified in units of days. The default for most data directories is 7 days, except for the directories
   - /opt/MagellanMDP/data/mdp/spool/received - default is 2 days
   - /opt/MagellanMDP/data/mdp/merge - default is 30 days
   - /opt/MagellanMDP/data/mdp/admin - default is 30 days
   - /opt/MagellanMDP/data/mdp/report - default is 90 days
4. To change the file retention time, double-click the retention time using the right-mouse button and replace the existing number of days with a new number of days.
5. Repeat step 4 for each indicated MDP directory.
6. Click **Save** to save the configuration change.
7. Click **Save Disk Cleaner** to save the configuration change and to restart the Disk Manager.

Setting the minimum available disk space

The MDP Disk Manager monitors the available MDP disk space.

1 When MDP disk space reaches 90% of the minimum available disk space requirement, traps and alarms are generated.

2 When MDP disk space reaches the minimum available disk space threshold, data conversion is halted.

Note: If MDP disk space regularly approaches the minimum disk space threshold, reduce the retention time of data files or add more disk space.

To change the minimum available disk space threshold, the MDP Disk Manager (mdpdiskmgr) must be restarted using the new setting. For more information, see "Launching the MDP Disk Manager and setting the minimum disk space" (page 192).

Setting the Disk Manager log level

Configure the information level of logs generated by the MDP Disk Manager. For more information, see "Launching the MDP Disk Manager and setting the minimum disk space" (page 192).

Configuring BDF archiving

BDF archiving sorts individual bulk data format (BDF) records into files in sub-directories of directory /opt/MagellanMDP/data/mdp/archive. This sub-directory structure is determined by the order of the selections made using the procedures in this section.

Note: The MDP Disk Manager does not maintain archived data. The Disk Manager is described in section "Configuring data file retention" (page 94).

For more information, see "Bulk data format files" (page 31).

For information about the BDF archive file name format, see "Archived BDF data" (page 55).

Configuring BDF archiving

1. If you are configuring BDF archiving for the first time, follow the procedure “Configuring the initial BDF archival directory structure” (page 97).

   If you are re-configuring BDF archiving, follow the procedure “Changing an existing BDF archival directory structure” (page 98).

2. Configure the disk space threshold for halting BDF archiving, see “Configuring the disk space threshold for halting BDF archiving” (page 99).

3. Configure the disk space threshold for generating SNMP warnings, see “Configuring the disk space threshold for SNMP warnings” (page 99).

4. Click **Save** to save the new configuration.

5. If you are configuring BDF archiving for Passports, select **Passport** from the MDP Configuration tool window and follow the procedure “Archiving BDF records” (page 133).

   If you are configuring BDF archiving for DPNs, select **DPN** from the MDP Configuration tool window and follow the procedure “Archiving BDF data” (page 163).

Configuring the initial BDF archival directory structure

1. Using the MDP Configuration tool, select **BDF Archiving**.

2. Select the first level of the structure by clicking on the button box beside one of the options under **Format**.

   Note: You cannot select one of the formats containing **DD** until you have selected one of the formats containing **YYYY**.

   The selected level name is displayed at the top of the panel beside the list of optional format names and the button box contains a check mark.

   For example, if the first level selected is **DATATYPE** and if you have selected Passport accounting BDF data to be archived, the new archive directory structure is /opt/MagellanMDP/data/mdp/archive/acc.

3. Select the next level of the structure by clicking on the button box beside one of the options under **Format**.

   The next level name is displayed below the previously selected level name in the panel beside the list of optional format names and the button box contains a check mark.

For example, if the next level selected is **NODEID**, the new archive directory structure is /opt/MagellanMDP/data/mdp/archive/acc/<nodeID>.

where
<nodeID> will be an actual nodeID obtained from the data filename when the data is archived.

4 Repeat step 3 until you have completed the selection of directory levels.

5 If you are configuring BDF archiving for Passports, select **Passport** from the MDP Configuration tool window and follow the procedure “Archiving BDF records” (page 133).

If you are configuring BDF archiving for DPNs, select **DPN** from the MDP Configuration tool window and follow the procedure “Archiving BDF data” (page 163).

Changing an existing BDF archival directory structure

1 Using the MDP Configuration tool, select **BDF Archiving**.

2 Click **Unlock**.

A confirmation pop-up window is displayed. To confirm your intention to change the BDF archival directory structure, click **Ok**.

3 Click **Clear**.

The level names in the panel beside the list of optional format names are removed and the check marks in the button boxes beside the previously selected level names are removed.

4 Select the first level of the structure by clicking on the button box beside one of the options under Format.

Note: You cannot select one of the formats containing **DD** until you have selected one of the formats containing **YYYY**.

The selected level name is displayed at the top of the panel beside the list of optional format names and the button box contains a check mark.

For example, if the first level selected is **DATATYPE** and if you have selected Passport accounting BDF data to be archived, the new archive directory structure is /opt/MagellanMDP/data/mdp/archive/acc.

5 Select the next level of the structure by clicking on the button box beside one of the options under **Format**.

The next level name is displayed below the previously selected level name in the panel beside the list of optional format names and the button box contains a check mark.

For example, if the next level selected is **NODEID**, the new archive directory structure is /opt/MagellanMDP/data/mdp/archive/acc/<nodeID>.

where
<nodeID> will be an actual nodeID obtained from the data filename when the data is archived.

6 Repeat step 5 until you have completed the selection of directory levels.

7 If you are configuring BDF archiving for Passports, select **Passport** from the MDP Configuration tool window and follow the procedure “Archiving BDF records” (page 133).

If you are configuring BDF archiving for DPNs, select **DPN** from the MDP Configuration tool window and follow the procedure “Archiving BDF data” (page 163).

Configuring the disk space threshold for halting BDF archiving

To halt BDF archiving if the disk space threshold is exceeded for directory /opt/MagellanMDP/data/mdp/archive

1 Using the MDP Configuration tool, select **BDF Archiving**.

2 Type the amount of disk space in the box **Disk space threshold to halt processing**. Disk space is specified in units of megabytes (MB).

The default is 100MB.

3 Click **Save** to save the new configuration.

Configuring the disk space threshold for SNMP warnings

To generate SNMP warnings when the disk space threshold for directory /opt/MagellanMDP/data/mdp/archive is exceeded

1 Using the MDP Configuration tool, select **BDF Archival**.

2 Type the amount of disk space in the box **Disk space threshold for SNMP warnings**. Disk space is specified in units of megabytes (MB).

The default is 300MB.

3 Click **Save** to save the new configuration.

Configuring MDP file processing audits

Management Data Provider (MDP) file processing audit reports

- are generated every 24 hours at 0005 hours each morning (24 hours is the reporting period);
- are in ASCII text format;
- contain fields that are delimited by a colon, with the exception of field 10 that can contain a maximum of 3 hostnames or IP addresses separated by commas;
- header records can be included to identify field names (omit these records if the reports are to be processed downstream);
- track raw and bulk data format (BDF) data files being processed by MDP;
- detect missing raw data files using file sequence numbers;
- indicate raw data file size, number of records processed per file and instances of corrupt data;
- indicate delivery status of BDF data files and the customer host receiving the BDF files; and
- provide a summary of processed files by datatype and node.

For more information, see “MDP audit reports” (page 28).

For audit report field descriptions, see 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

Use the **Configure File Processing Audits** window for

- “Configuring the audit of MDP file processing” (page 101)
- “Configuring the File Processing Audit log level” (page 102)

Configuring the audit of MDP file processing

1. Using the MDP Configuration tool, select **Audits**.
2. To configure auditing of Passport BDF file processing, click on the button box **Enable Passport file process auditing**.

To configure auditing of DPN BDF file processing, click on the button box **Enable DPN file process auditing**.

A check mark is displayed in the selected button box.

The default is these options are not selected.

3 Select the report options.

To include the field names in the report, click on the button box **Print header records in report**.

To include detailed records in the report, click on the button box **Print detail records in report**.

To include summary records in the report, click on the button box **Print summary records in report**.

A check mark is displayed in the selected button box.

By default, only the summary records are reported.

4 Click **Save** to save the configuration change.

5 Use the **File Mover Manager** to configure the transfer of audit reports (filetype Audit Report) to customer hosts; see “Transferring files to customer hosts” (page 90).

Configuring the File Processing Audit log level

1 Using the MDP Configuration tool, select **Audits**.

2 To change the current File Processing Audit log level, click on the button box **auditing log level**.

The log levels are indicated (0 - 4).

3 Click on the appropriate log level. The default level is 3.

Log levels are described in section “Log levels” (page 207).

4 Click **Save** to save the configuration change.

Configuring log archiving

Log messages for the following Management Data Provider (MDP) processes are archived using an identical directory structure: Passport File Manager, DPN File Manager, and Passport File Prober Manager.

Log archiving stores MDP logs in sub-directories of the directory /opt/MagellanMDP/data/mdp/admin/archive. The sub-directory structure is determined by the order of the selections made using the procedures in this section.

For more information about logs, see “MDP logs” (page 32).

For information about the log archive file name format, see “Archived log files” (page 206).

Configuring log archiving

1. If you are configuring log archiving for the first time, follow the procedure “Configuring the initial log archival directory structure” (page 103).

   If you are reconfiguring log archiving, follow the procedure “Changing an existing log archival directory structure” (page 104).

2. Click on the **Save** button to save the new configuration.

   Log messages for the following MDP processes are archived using the specified directory structure: Passport File Manager, DPN File Manager, and Passport File Prober Manager.

Configuring the initial log archival directory structure

1. Using the MDP Configuration tool, select **Log Archival**.

2. Select the first level of the structure by clicking on the button box beside one of the options under **Format**.

   Note: You cannot select one of the formats containing **DD** until you have selected one of the formats containing **YYYY**.

   The selected level name is displayed at the top of the panel beside the list of optional format names and the button box contains a check mark.

   For example, if the first level selected is **DATATYPE** the archive directory structure created is /opt/MagellanMDP/data/mdp/admin/archive/acc.

3. Select the next level of the structure by clicking on the button box beside one of the options under **Format**. You cannot select one of the formats

containing DD until you have selected one of the formats containing YYYY.

The next level name is displayed below the previously selected level name in the panel beside the list of optional format names and the button box contains a check mark.

For example, if the next level selected is **NODEID**, the archive directory structure created is /opt/MagellanMDP/data/mdp/admin/archive/acc/<nodeID>.

4 Repeat step 3 until you have completed the selection of directory levels.

Changing an existing log archival directory structure

1 Using the MDP Configuration tool, select **Log Archival**.

2 Click **Unlock**.

A confirmation pop-up window is displayed. To confirm your intention to change the format of the log archival directory structure, click the **Ok** button.

3 Click **Clear**.

The level names in the panel beside the list of optional format names are removed and the check marks in the button boxes beside the previously selected level names are removed.

4 Select the first level of the structure by clicking on the button box beside one of the options under **Format**.

Note: You cannot select one of the formats containing **DD** until you have selected one of the formats containing **YYYY**.

The selected level name is displayed at the top of the panel beside the list of optional format names and the button box contains a check mark.

For example, if the first level selected is **DATATYPE** the archive directory structure created is /opt/MagellanMDP/data/mdp/admin/archive/acc.

5 Select the next level of the structure by clicking on the button box beside one of the options under **Format**.

Note: You cannot select one of the formats containing **DD** until you have selected one of the formats containing **YYYY**.

The next level name is displayed below the previously selected level name in the panel beside the list of optional format names and the button box contains a check mark.

For example, if the next level selected is **NODEID**, the archive directory structure created is /opt/MagellanMDP/data/mdp/admin/archive/acc/<nodeID>.

6 Repeat step 5 until you have completed the selection of directory levels.

Configuring MDP surveillance

The Management Data Provider (MDP) can generate traps and alarms for all MDP processes.

To generate alarms, the MDP workstation is configured with an Injected Management Data Router (IMDR) and a General Management Data Router (GMDR).

To monitor MDP alarms, activate the MDM **Fault->Alarm Display**. For more information about IMDR and GMDR, see 241-6001-303 *Preside MDM Administrator Guide*. For more information about fault monitoring, see 241-6001-011 *Preside MDM Fault Management User Guide*.

If the MDP is unable to connect to or send alarms to an active IMDR, log message 10174 is generated.

To view traps, you are required to configure a workstation as an SNMP Management Station. For more information about MDP SNMP trap generation, see “MDP alarms and/or traps” (page 225).

Configuring MDP surveillance

1 Using the MDP Configuration tool, select **Surveillance**.

2 To generate MDP alarms

a. Click **Enable MDP to send MDM Alarms**.

A check mark is displayed in the button box.

The default is not to have this option selected.

b. Type the hostname or IP address of an MDM workstation in the data entry box **IMDR Host**. This is an MDM with an active Injected Management Data Router (IMDR).

This option is only required if **Enable MDP to send MDM Alarms** is selected.

The default is **local host**.

3 To generate MDP traps

a. Click **Enable MDP to send SNMP traps**.

A check mark is displayed in the button box.

The default is this option is not selected.

b. In the data entry box **SNMP Community string variable**, type the community string variable for MDP SNMP traps. This option is only required if **Enable MDP to send SNMP traps** is selected.

The default community string is **public**.

c. Type the following information in the data entry boxes beside **SNMP Management Stations #1**:

In the first column **Hostname / IP Address**, type the hostname, or IP address, of an SNMP management station.

In the second column **Port#**, type the port number on the SNMP management station.

The default SNMP management station port number is port 162.

Repeat this step to configure another SNMP management station. A maximum of three SNMP management stations can be configured.

4 Click **Save** to save the new configuration.

The new configuration is saved on the MDP.

You are prompted to restart all of the MDP processes currently controlled by the Server Administration (SVM) tool.

Customizing MDP data directories

The directories used to store switch data on the Management Data Provider (MDP) can be directed to disks, or disk partitions, other than the disk and partition where the default directory /opt is located. This capability adds flexibility to MDP processing. Disks, or disk partitions, that have reached maximum disk space capacity need not prevent MDP processing for all MDP data types. For a list of the MDP data directories and their default pathnames, refer to “MDP directory structure” (page 39).

Note: Customization of MDP directories applies to MDP data directories, only. These directories include any sub-directory of directory /opt/MagellanMDP/data/mdp. MDP software and configuration directories are not customizable.

Use the following procedures to manage MDP directories:

- “Opening the MDP Flexible Directory Installation window” (page 107)
- “Customizing data directory location” (page 107)
- “Returning a customized directory to a standard MDP directory” (page 109)

These sections describe the MDP Flexible Directory Installation window, constraints on directory customization, and process logging.

- “Flexible Directory Installation window” (page 110)
- “Restrictions on directory customization” (page 112)
- “Recording directory customization” (page 113)
- “Setting a secondary MDP mount point (Vector, only)” (page 114)

Opening the MDP Flexible Directory Installation window

CAUTION
All MDP processing must be stopped before customizing the MDP data storage directories.

1. Stop switch data collection.
2. Halt all MDP processes using the Server Administration tool (SVM).
3. Using the userID root, from the UNIX command line, type

   `/opt/MagellanMDP/bin/gmdpinst &`

   A window opens with two tabs, the Directory Install tab and the Flexible Install tab.
4. Select **Flexible Install**.

   The Flexible Directory Installation window opens.

Customizing data directory location

1. Click the **Custom** radio button beside the MDP directory to be relocated.

   The **Physical Path Root** data entry box is enabled.

The **Check** button is enabled.

The **Space(MB)** field is made blank.

The **Status** field indicates UNKNOWN.

2 Do one of the following

a. Type the new mount point into the **Physical Path Root** data entry box.

b. From an xterm, copy a selected mount point and paste the mount point into the **Clipboard** data entry box. Paste the mount point from the **Clipboard** in to the **Physcial Path Root** data entry box using the middle mouse button.

3 Click **Check** to validate the new physical path. To understand the restrictions placed on custom physical paths, see “Restrictions on directory customization” (page 112).

If no errors are detected by the validity check, the **Status** field indicates VALID. The **Space(MB)** field indicates the amount of space available in units of megabytes.

If an error is detected by the validity check, a new window opens and indicates the cause of the error.

If the specified physical path root is invalid, a new window opens and indicates the reason for invalidation.

If there is insufficient space for the specified physcial path root, or if detailed activation information is available, the **Status** field indicates WARNING. The **Space(MB)** field indicates the amount of space available in units of megabytes.

4 Click **Activate Configuration** to activate the new custom directory mapping.

If the custom physical path does not exist, it is created.

If this is a standard MDP directory being customized, all data in the standard directory is moved to the custom physical path and links are created from the standard MDP path to the custom physical path.

If this is a previously customized physical path, all data in the old custom physical path is moved to the new custom physical path and links are created from the standard MDP path to the new custom physical path.

The Flexible Install Activation Log window opens. This window reports the progress of the directory mapping changes.

If an error is detected during activation, a new window opens and indicates the cause of the error. The error must be corrected before clicking the **Activate Configuration** button.

If no errors are detected by the activation, a new window opens with the following message:

```
Finished activation with no errors.
```

If no errors are detected by the activation, the **Status** field indicates READY.

5 If the MDP directory being customized is directory /opt/MagellanMDP/data/mdp/spool/secondary, see “Setting a secondary MDP mount point (Vector, only)” (page 114).

6 Select **File -> Exit**.

Returning a customized directory to a standard MDP directory

1 Click the **Default** radio button beside the MDP directory to be relocated.

The **Check** button is enabled.

The **Space(MB)** field is made blank.

The **Status** field indicates UNKNOWN.

2 Click **Check** to validate the new physical path. To understand the restrictions placed on new physcial paths, see “Restrictions on directory customization” (page 112).

If no errors are detected by the validity check, the **Status** field indicates DEFAULT. The **Space(MB)** field indicates the amount of space available in units of megabytes.

If an error is detected by the validity check, a new window opens and indicates the cause of the error.

3 Click **Activate Configuration** to return the directoy mapping to the standard MDP directory.

If the standard MDP physical path does not exist, it is created.

All data in the custom physical path is moved to the standard MDP directory and the custom mapping links are deleted.

The Flexible Install Activation Log window opens. This window reports the progress of the directory mapping changes.

If an error is detected during activation, a new window opens and indicates the cause of the error. The error must be corrected before clicking **Activate Configuration**.

If no errors are detected, a new window opens with the following message:

```
Finished activation with no errors.
```

If no errors are detected by the activation, the **Status** field indicates DEFAULT.

4 Select **File -> Exit**.

Flexible Directory Installation window

The Management Data Provider (MDP) Flexible Directory Installation window includes the following components.

Pull-down menu

The Flexible Directory Installation window includes the pull-down menu item **File -> Exit**. This option exits the gmdpinst application and closes all associated open windows.

Main panel

The main panel of the Flexible Directory Installation window displays all of the MDP data directories. The main panel includes:

- **Logical Path**
  is the standard MDP directory path located under directory /opt/MagellanMDP/data/mdp. The logical path always starts with /opt. This path is the default physical path for new MDP installations. An example of an MDP logical path is

  ```
  /opt/MagellanMDP/data/mdp/dump/alarm
  ```

- **Default**
  radio button. Click this button for any standard MDP directory path to make the logical path equal to the actual physical path.

- **Custom**
  radio button. Click this button for any standard MDP directory path to indicate that you want to specify a physical path other than the specified logical path.

- **Physical Path Root**
  is the UNIX mount point for the custom physical path. You must have previously added the physical path root to the /etc/vfstab file and mounted this path root before the configuration is activated. Examples of physical path roots are

  `/raid_mdpdata`

  `/mounts/datastore1`

  This data entry box is only available if the Custom radio button has been selected.

  Data can be typed directly into this data entry box or data can be pasted from the Clipboard.

- **Physical Path ext.**
  is the MDP defined extension to the custom physical path. There is a physical path extension for each MDP data logical path. This extension cannot be changed.

- **Space(MB)**
  indicates the amount of disk space, in megabytes, for the specified physical path.

- **Check**
  button. Click this button to validate accessibility and size of the disk, or disk partition, of the physical path.

- **Status**
  indicates the current status of the mapping between the logical path and the physical path. The possible values for the Status field are

  — UNKNOWN - the mapping cannot be determined

  — DEFAULT - the default mapping for this directory is active. The logical path equals the physical path.

  — VALID - the specified change in mapping is valid.

  — INVALID - the specified change in mapping is not valid.

  — READY - the specified change in customized mapping is complete.

  — ERROR - the specified physical path cannot be used.

— WARNING - there is a low amount of disk space in the specified physical path or directories and files will be moved by this action.

Directory management actions bar

The Flexible Directory Installation window includes a directory management actions bar located at the bottom of the window:

- **Clear**
  button. Click this button to remove the contents of the Clipboard data entry box.
- **Clipboard**
  a physical path root can be cut and pasted into this data entry box from an xterm and then transferred to the physical path root data entry box. A physical path root can also be typed in this data entry box.
- **Show Log**
  button. Click this button to display the MDP Flexible Install Activation Log window that reports activity related to MDP data directory customization. This button label changes to Hide Log when the MDP Flexible Install Activation Log window is open.
- **Activate Configuration**
  button. Click this button to activate the new directory mapping specified in the Flexible Directory Installation window.
- **Refresh Space**
  button. Click this button to redisplay the space available for each MDP data directory. The Space(MB) value is updated with the actual current space available.
- **Check All**
  button. Click this button to activate the Check button for those directories that have an indicated status of: UNKNOWN, ERROR, or INVALID.

Restrictions on directory customization

The following restrictions are placed on customized MDP data paths:

- a logical path cannot contain an embedded symbolic link above level /opt/MagellanMDP/data/mdp. For example, the logical path cannot be /localdisk/data/mdp or /localdisk/data.

- a logical path cannot be a shared mount point. For example, the logical path cannot be an exported directory in file /etc/dfs/dfstab.
- a custom physical path cannot contain an embedded symbolic link. For example

  ```
  /opt/MagellanMDP/data/mdp/dump/statistics ->
  /localdisk/mdp_dump/statistics
  /localdisk/mdp_dump/statistics -> /var/statistics
  ```

- a custom physical path cannot be a sub-directory of any of the following directories:

  ```
  /
  /dev
  /opt
  /usr
  /etc
  /tmp
  /bin
  /sbin
  /lib
  /devices
  /proc
  ```

- a custom physical path cannot be mounted on a partition equivalent to the root ‘/ ‘ partition.
- a custom physical path cannot be an NFS mounted filesystem, with the following exceptions:

  ```
  /opt/MagellanMDP/data/mdp/spool/secondary
  /opt/MagellanMDP/data/mdp/oc/dpn/secondary
  /opt/MagellanMDP/data/mdp/oc/pp/secondary
  ```

- a custom physical path must have the minimum required disk space as specified by the MDP Disk Manager. For more information, see “Setting the minimum available disk space” (page 96).

Recording directory customization

Customization of the MDP data directory structure is recorded in log file /opt/MagellanMDP/data/mdp/admin/ MDPFID<Sun|Mon|Tue|Wed|Thu|Fri|Sat>_<YYYYMMDD>.log.

Setting a secondary MDP mount point (Vector, only)

If you customize the physical path for the data directory /opt/MagellanMDP/data/mdp/spool/secondary on the primary MDP, perform the following procedures.

In this example, the directory /opt/MagellanMDP/data/mdp/spool/restore on the secondary MDP host was mounted at the /opt/MagellanMDP/data/mdp/spool/secondary directory mount point on the primary MDP host. If the directory /opt/MagellanMDP/data/mdp/spool is customized to map to the physical path /var/mdp_spool on the primary MDP, the spool/secondary directory is now physically located at /var/mdp_spool/secondary.

Configuring the secondary MDP

1 Add the following information to file /etc/dfs/dfstab on the secondary MDP.

```
share -F nfs -o rw=<primary_hostname>
/opt/MagellanMDP/data/mdp/spool/restore
```

2 Using the UNIX userID root, type the following at the command line:

```
/usr/sbin/shareall
```

Configuring the primary MDP

1 Add the following information to file /etc/vfstab on the primary MDP.

```
<secondary_hostname>:/opt/MagellanMDP/data/mdp/spool/
restore - /var/mdp_spool/secondary nfs - yes rw
```

2 Using the UNIX userID root, type the following at the command line:

```
/usr/sbin/mount /var/mdp_spool/secondary
```

Configuring the Outage Controller

This section describes how to configure the Management Data Provider (MDP) Outage Controller for outage calculation.

The MDP value-added applications are described in detail in section "Value-added data applications" (page 231).

The following topics are discussed in this section:

- "Setting the local MDP host as primary or secondary" (page 115)
- "Identifying the secondary MDP host" (page 116)
- "Scheduling the Outage Calculator" (page 116)
- "Identifying the MDM host" (page 116)
- "Setting the Outage Controller log level" (page 117)
- "Enabling outage calculation" (page 117)
- "Launching the MDP Topology Generator" (page 117)
- "Archiving outage files" (page 118)
- "Transferring outage files to customer hosts" (page 118)

After the Outage Controller is configured

- for Passport outages, see "Configuring outage calculation" (page 156).
- for DPN-100 outages, see "Configuring outage calculation" (page 171).

Setting the local MDP host as primary or secondary

For more information about MDP hosts, see "Hosts" (page 34).

1. Using the MDP Configuration tool, select **Outage Control**.
2. Click one of the radio buttons for **Is this MDP server?**.
   - To select primary, click **primary**.
   - To select secondary, click **secondary**.

   The default is neither option is selected.

Note: If a backup MDP host has been configured, the backup MDP host is configured as a secondary MDP host with an NFS mount connection between the primary and backup hosts.

3 Click **Save** to save the configuration change.

Identifying the secondary MDP host

For more information about MDP hosts, see "Hosts" (page 34).

1 Using the MDP Configuration tool, select **Outage Control**.

2 Type the hostname or IP address of the secondary host in the data entry box **Hostname or IP address of secondary server**.

The default is this data entry box is empty.

Note: If you have set the local MDP host as the secondary MDP host, this option is not available.

3 Click **Save** to save the configuration change.

Scheduling the Outage Calculator

1 Using the MDP Configuration tool, select **Outage Control**.

2 Click **Invoke Outage Calculator daily**.

A check mark is displayed in the button box.

The default is this option is not selected.

3 Type the time to launch the Outage Calculator in the data entry box **Time of day to start Outage Calculator (hh:mm)**. Use the 24 hour clock standard (for example, 5:00 PM is 17:00).

The default is 00:00.

Note: If you have not enabled the daily execution of the Outage Calculator, this option is not available.

An entry is added to the UNIX crontab to invoke the Outage Controller every day at this time.

4 Click **Save** to save the configuration change.

Identifying the MDM host

For DPN outage calculation, only.

1 Using the MDP Configuration tool, select **Outage Control**.

2 Type the hostname of the MDM host in the data entry box **Hostname of DPN Network Model Server**.

The default is this data entry box is empty.

3 Click **Save** to save the configuration change.

Setting the Outage Controller log level

1 Using the MDP Configuration tool, select **Outage Control**.

2 To change the current Outage Controller log level, click the button box **Outage Controller log level**.

The log levels are indicated (0 - 4).

3 Click on the appropriate log level.

The default is level 3.

For more information about log levels, see “Log levels” (page 207).

4 Click **Save** to save the configuration change.

Enabling outage calculation

1 Using the MDP Configuration tool, select **Outage Control**.

2 Select a switch type: Passport or DPN; click a button box beside **Enable outage calculation**. For example, to enable outage calculation for Passport, click the button box below **Passport**.

A check mark is displayed in the button box.

The default is this option is not selected.

3 Repeat, as necessary, for each switch type.

4 Click **Save** to save the configuration change.

Launching the MDP Topology Generator

For DPN outage calculation, only.

To launch the MDP Topology Generator before the DPN Outage Calculator

1 Using the MDP Configuration tool, select **Outage Control**.

2 Click **Run topology generator before outage calculator**.

A check mark is displayed in the button box.

The default is this option is not selected.

3 Click **Save** to save the configuration change.

Archiving outage files

1 Using the MDP Configuration tool, select **Outage Control**.

2 Select a switch type: Passport or DPN; click a button box beside **Archive outage files**. For example, to archive outage files for Passport, click the button box below **Passport**.

A check mark is displayed in the button box.

The default is this option is not selected.

3 Repeat, as necessary, for each switch type.

4 Click **Save** to save the configuration change.

Transferring outage files to customer hosts

1 Using the MDP Configuration tool, select **Outage Control**.

2 Select a switch type: Passport or DPN; click a button box beside **Copy outage files to dump directory**. For example, to transfer outage files to customer hosts for Passport, click the button box below **Passport**.

A check mark is displayed in the button box.

The default is this option is not selected.

3 Repeat, as necessary, for each switch type.

4 Click **Save** to save the configuration change.

Configuring availability calculation

Configuring availability calculation potentially involves the three manual tasks described in the following sections:

- "Availability calculator configuration" (page 119)
- "Service window configuration" (page 120)
- "Start life configuration" (page 121)
- "Availability report generation" (page 122)

Availability calculator configuration

Availability calculator options can be specified using command line options. For more information, see “Availability calculation” (page 253).

The Availability Calculator can be manually configured by editing the configuration file /opt/MagellanMDP/cfg/mdp/MDPAVCALC.cfg. This file contains records, separated by line feeds, of parameter identifier and value pairs. The following parameters are valid:

`OLD_LOGS_TO_RETAIN`

The number of logs from previous runs to retain. The range is from 0 to 9; defaults to 3.

`ACCUMULATED_STATS`

To specify processing and update of the accumulated statistics file. The options are [Y|N]; defaults to N.

`GEN_AVA_DELIMITER`

The character to use as the field delimiter in the Availability Report BDF output file; defaults to DEL.

`DPN_OTG_DELIMITER`

The character to interpret as the field delimiter in the DPN Outage BDF input files; defaults to DEL.

`PP_OTG_DELIMITER`

The character to interpret as the field delimiter in the Passport Outage BDF input files; defaults to DEL.

For example:

```
OLD_LOGS_TO_RETAIN: 3
ACCUMULATED_STATS: Y
GEN_AVA_DELIMITER: :
DPN_OTG_DELIMITER: :
PP_OTG_DELIMITER: :
```

Service window configuration

If required, an exceptions file /opt/MagellanMDP/cfg/mdp/MDPSERVWIN.cfg can be created to exclude periods of known component down-time from the availability statistics. When performing availability analysis, periods of outage for a component, and subcomponents, that occur during the defined network service window are ignored. The time period identified by the network service window is not included in availability calculations.

> ***Note:*** Service window entries must be retained for at least one subsequent availability analysis sample period following that sample period during which the component was out-of-service for maintenance.

This exceptions file can be created and edited using any text editor (for example, `vi`). If this file exists, the Availability Calculator process reads it on startup. This file can contain multiple records separated by line feeds. This file contains fields that identify components and the start and end times of a network service window. The exceptions file has the following format:

```
<module_id>[<component_id>]:<start_time>-<end_time>
```

where:

`<module_id>` is an integer corresponding to the nodeID or namsID of the module.

`<component_id>` is the component identifier and consists of a string of <category>/<value> pairs.

`<start_time>` is the start of the exclusion period: YYYYMMDD[hh[mm[ss]]], for year, month, day, hours (optional), minutes (optional) and seconds (optional).

`<end_time>` is the end of the exclusion period: YYYYMMDD[hh[mm[ss]]], for year, month, day, hours (optional), minutes (optional) and seconds (optional).

For example:

1041 : 19970112 - 19970116
1041 PE/2 : 199702070000 - 199702070030
3034 PE/4 : 19970628174800 - 19970630073030

Start life configuration

If required, a component start life file /opt/MagellanMDP/cfg/mdp/MDPSTLIFE.cfg can be created to specify the date and time at which a component becomes available for availability calculation purposes.

If the start life is not defined by the user, a start life is automatically established as the beginning date/time of the sample period in which an outage for the component is first encountered. The start life of each component is recorded in the Availability Calculator administration log file /opt/MagellanMDP/data/mdp/admin/MDPAC<date>.log (where <date> is the date the log file was generated). An indication of whether the start life was user defined or automatically generated is included in the log file.

A user-defined component start life also applies to the components subcomponents, unless a start life is specifically defined for those subcomponents.

The start life file can be created and edited using any text editor (for example, vi). If this file exists, the Availability Calculator process reads it on startup. This file can contain multiple records separated by line feeds with fields that identify a component and its start life in the following format:

```
<moduleID>[<componentID>]:<start_life_date_time>
```

where:

<moduleID> is an integer corresponding to the nodeID/namsID of the module.

<componentID> is a string of <category>/<value> pairs.

<start_life_date_time> is the start life setting: YYYYMMDD[hh[mm[ss]]], for year, month, day, hours (optional, default 00), minutes (optional, default 00), and seconds (optional, default 00).

For example:

```
1041 : 19970112
1041 PE/2 : 199702070000
3034 PE/4 : 19970628174800
2023 EM/PASSNODE2 LogicalProcessor/7 :199706190000
```

Availability report generation

Report Generator options can be specified using command line options. See "Availability report generation" (page 264).

The Report Generator can be manually configured by editing the configuration file /opt/MagellanMDP/cfg/mdp/MDPREPGEN.cfg. This file contains records (separated by a line feed character) of parameter identifier and value pairs. The following records are valid:

`GEN_AVA_DELIMITER`

The character to interpret as the field delimiter of the Availability Report BDF input file; defaults to DEL.

`DEFAULT_INPUT_DIR`

The default directory for Availability Report BDF input files; defaults to /opt/MagellanMDP/data/mdp/dump/avail.

`REPORT_TYPE`

The type of report selected. The possible options are:

MODLINK (modules, links, trunks, and Gateways)
SUBCOMP (module subcomponents)
BACKBONE (cards, processors, Logical Processors, and Gateways)
TOPOLOGY (trunks, links, and Gateways)
LOGPROC (Passport Logical Processors)
ALL (all component types)

`MODULE_ID`

Limit the report to a particular module. Enter an integer value or an asterik * to select all modules.

`ACCUMULATED_STATS`

Report accumulated statistics, not statistics from the last sample period. Options are [Y|N]; defaults to N.

`AVAILABILITY_THRESHOLD`

Components with availability above this threshold are not be included in the report. The range is from 0.00 to 100.00; defaults to 100.00 (all components included).

`SHOW_CP_SWITCHOVER`

Display Passport module Control Processor switchover counts. Options are [Y|N]; defaults to N. Specify this option for Passports using a pre-5.1 software release.

CP switchover counts are reported in a separate section at the end of the Availability Report. To generate this type of report, you must use REPORT_TYPE_ALL and you must include the -cpsw option.

For Passports using a software release of 5.1, or later, CP switchover counts and durations are included with the Logical Processor/0 component.

`PAGE_WIDTH`

The number of characters on a line before a new line is forced; defaults to no line limit.

Note: For configurable windows (for example, Xterms), it is suggested that this parameter be set to a minimum of 90 characters and the window size adjusted as required.

`PAGE_LENGTH`

The number of lines on a page before a page feed is forced. Enter an integer value; defaults to 66.

Chapter 3
Configuring MDP for Passport

This section describes how to configure the Management Data Provider (MDP) to collect and convert Passport performance metrics data.

The following topics are discussed in this section:

- "Prerequisites" (page 125)
- "Storing Passport raw data" (page 126)
- "BDF data management" (page 126)
- "Assigning data to outage calculation" (page 134)
- "Setting the File Manager log level" (page 134)
- "PF data management" (page 134)
- "Collecting Passport data" (page 136)
- "Configuring SRS" (page 145)
- "Configuring outage calculation" (page 156)

Prerequisites

Before configuring the Management Data Provider (MDP) software to manage Passport data, ensure that you have:

- reviewed 241-6001-102 *Preside MDM Planning Guide*
- reviewed the Preside Multiservice Data Manager (MDM) Release Supplement for this release.

- installed the MDP software - see 241-6001-100 *Preside MDM Installer Guide*.
- configured data file retention and the minimum MDP disk space requirements - see “Configuring data file retention” (page 94).
- launched the MDP Configuration tool - see “Launching the MDP Configuration tool” (page 87).

Storing Passport raw data

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **Backup raw files**. For example, to backup accounting raw data, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.

   The raw switch data is stored in sub-directories of the directory /opt/MagellanMDP/data/mdp/backup.
3. Repeat, as necessary, for each datatype.
4. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

BDF data management

An introduction to converting data to bulk data format (BDF) is provided in section “Converting switch data to bulk data format” (page 25).

A discussion about Passport and MDP data models and how they affect BDF data conversion is provided in section “Data models” (page 46).

The following topics are discussed in this section:

- “Converting Passport raw data to BDF” (page 127)
- “Setting the BDF field delimiter” (page 127)
- “Setting BDF data compression” (page 128)
- “Including the DMId with BDF filenames” (page 128)
- “Including the DMId and RDF version with BDF records” (page 129)

- “Retaining backwards compatibility for BDF records” (page 129)
- “Customizing BDF records” (page 130)
- “Setting the BDF conversion log level” (page 132)
- “Setting the BDF conversion escape character” (page 132)
- “Creating empty BDF files” (page 133)
- “Archiving BDF records” (page 133)

Converting Passport raw data to BDF

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **BDF in dump directories**. For example, to convert accounting raw data to BDF, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.

   The converted data is written to sub-directories of the directory /opt/MagellanMDP/data/mdp/dump.
3. Repeat, as necessary, for each datatype.
4. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Setting the BDF field delimiter

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: aAccount, Stats, Alarm, Log, or SCN; type the hex code representation for the equivalent character in the data entry box beside **BDF field delimiter**. For example, to set the BDF field delimiter for accounting files, type the hex code in the data entry box below **Account**.

   The default is DEL (0x7F) for all datatypes.

   Note: Do not use alpha-numeric characters [Aa-Zz] [0-9] as these can make it difficult to read the output files. Also, do not use the following special characters: "|", "^", "(", ")", " ", ",", “.”, or "/".
3. Repeat, as necessary, for each datatype.
4. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Setting BDF data compression

BDF records with 3, or more, fields containing null values can be compressed to save disk space and transmission bandwidth. In BDF files, the start of the compression is indicated by ^<count> where <count> is the number of empty fields. For example, ^5 indicates 5 consecutive empty fields.

CAUTION
If the Passport Outage Calculator is used, do not apply data compression to alarm or SCN files. The Passport Outage Calculator does not support compressed data.

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **BDF output compression**. For example, to compress accounting data, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.
3. Repeat, as necessary, for each datatype.
4. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Including the DMId with BDF filenames

The Data Model Identifier (DMId) can be included with the BDF file names. For more information, see “Data models” (page 46) and “Passport data file names” (page 52).

Note 1: The DMId is not included in the file name of files containing archived BDF records.

Note 2: If short BDF file names are used to transfer BDF files to IBM mainframe customer hosts, do not include the DMId in BDF file names.

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **DMID in BDF filename**. For example, to include the Data Model Identifier with accounting filenames, click the button box below **Account**.

The default is this option is not selected.

3 Repeat, as necessary, for each datatype.

4 Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Including the DMId and RDF version with BDF records

The Data Model Identifier (DMId) and RDF version can be included with BDF records. This information is added to the datatype field; for more information see 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

Note: Including the record description file (RDF) version in the BDF records enables the **Data Viewer** application to select the correct RDF for BDF file viewing.

1 Using the MDP Configuration tool, select **Passport**.

2 Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **DMID in dataType field**. For example, to include the DMId and RDF version with accounting records, click the button box below **Account**.

The default is this option is not selected.

3 Repeat, as necessary, for each datatype.

4 Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Retaining backwards compatibility for BDF records

The MDP is configured to maintain backwards compatibility with the default data model for all BDF records. Backwards compatibility can be removed to allow the customization of BDF records. If you use this setting, do not use the instructions in procedure "Customizing BDF records" (page 130).

1 Using the MDP Configuration tool, select **Passport**.

2 Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **RDF Backwards Compatibility**. For example, to maintain backwards compatibility for accounting files, click the button box below **Account**.

The default is this option is selected. New performance metrics are appended to BDF records and the field order cannot be changed.

3 Repeat, as necessary, for each datatype.

4 Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Customizing BDF records

BDF records for each Passport datatype can be customized to include or exclude Passport performance metrics. The field order in BDF records can also be customized.

Note: If the Passport Outage Calculator is used, do not customize Passport alarm or state change notification (SCN) records.

1 Using the MDP Configuration tool, select **Passport**.

2 Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click **Edit** beside **Configure RDF**. For example, to customize BDF accounting records, click **Edit** below **Account**.

The **Passport <datatype> RDF Configuration** window opens.

The panel **Configured RDF fields** lists the fields currently included in the BDF records.

Note: If backwards compatibility has been configured for the selected datatype, the fields listed in the **Configured RDF fields** panel cannot be removed or re-ordered.

The panel **New RDF fields** lists the performance metrics identified in Passport data models that have not been selected for BDF record conversion and have not been excluded.

To identify new performance metrics before they are introduced into the network, use the **rdfreport** command. For more information about the **rdfreport** command, see “Identifying new Passport performance metrics” (page 191).

The panel **Excluded RDF fields** lists the performance metrics identified in Passport data models that have not been selected for BDF record conversion. Excluding performance metrics prevents them from being identified as ‘new’ when a new Passport data model is detected.

Only the fields for the selected datatype are listed.

3 To add a field to the BDF record

a. Select the field from the **New RDF fields** panel or the **Excluded RDF fields** panel

b. Click the **Move to Configured** button below the respective panel.

The selected field is placed at the bottom of the **Configured RDF fields** list.

4 To remove a field from the BDF record

a. Select the field from the **Configured RDF fields** panel.

b. Click the **Move to New** or **Move to Excluded** button below the **Configured RDF fields** panel.

The selected field is placed at the bottom of the **New RDF fields** list or **Excluded RDF fields** list.

5 To change the order of fields in the BDF record

a. Select the field in the **Configured RDF fields** panel.

b. Click the **Move Up** button to move the field toward the beginning of the record.

c. Click the **Move Down** button to move the field toward the end of the record.

6 To exclude a new performance metric

a. Select the field from the **New RDF fields** panel.

b. Click the **Move to Excluded** button under the **New RDF fields** panel.

The selected field is placed at the bottom of the **Excluded RDF fields** list.

7 To replace an excluded performance metric for future consideration

a. Select the field from the **Excluded RDF fields** panel.

b. Click the **Move to New** button under the **Excluded RDF fields** panel.

The selected field is placed at the bottom of the **New RDF fields** list.

8 When all of the BDF record changes for the selected datatype are complete, click the **Commit RDF** button.

The new RDF is saved.

You are prompted to confirm the commit action.

The **Passport <datatype> RDF Configuration** window closes.

Note: The Passport File Manager (mdpppmgr) must be restarted to implement the committed BDF record changes.

Setting the BDF conversion log level

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **BDF converter log level**. For example, to set the BDF converter log level for accounting data conversion, click the button box below **Account**.

   The log levels are indicated (0 - 4).
3. Select a log level.

   The default log level is 3 for all datatypes.

   Log levels are described in section “Log levels” (page 207).
4. Repeat, as necessary, for each datatype.
5. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Setting the BDF conversion escape character

A generic escape character can be set to mask characters that cannot be interpreted. If any delimiters, repeating field delimiters, or escape characters (generic or compressed) are encountered in data fields with a type of string, the string is replaced with <escape character><hex code>, where <hex code> is the 2-digit hexadecimal value of the character.

Escape character conversion is only required for Passport datatypes: alarms, logs, and state change notifications (SCN).

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Alarm, Log, or SCN; type the BDF escape character in a data entry box beside **BDF output escape char**. For example, to set the BDF escape character for alarm files, type the escape character in the data entry box below **Alarm**.

   The default is % for all three datatypes.

   Note: Do not use alpha-numeric characters [Aa-Zz] [0-9] as these can make it difficult to read the output files. Also, do not use the following special characters: "|", "^", "(", ")", " ", ",", or "/".
3. Repeat, as necessary, for each datatype.
4. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Creating empty BDF files

To retain the sequence of BDF file names, empty BDF files can be created when zero-length raw data files are collected.

1. Using the MDP Configuration tool, select **Passport**.
2. Click the button box **Process Empty Raw Files**.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Archiving BDF records

Individual BDF records can be stored in a customized directory structure using dates, datatypes, or nodeIDs. DMIds are not included in the file name format.

Note: Use the MDP Configuration tool window **BDF Archiving** to create the archive directory structure before selecting the Passport datatypes to archive. For more information, see "Configuring BDF archiving" (page 96).

1. Using the MDP Configuration tool, select **Passport**.
2. Select a Passport datatype: Account, Stats, Alarm, Log, or SCN; click a button box beside **BDF in archive directories**. For example, to convert accounting raw data to BDF and write the converted records to the archive directory structure, click the button box below **Account**.

   Note: If **BDF in dump directories** has not been enabled, this option is not available.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Assigning data to outage calculation

Passport outage calculation is described in section "Value-added applications" (page 68) and "Value-added data applications" (page 231).

Configure the MDP Outage Controller before performing this procedure. For more information, see "Configuring the Outage Controller" (page 115).

Note: The Passport Outage Calculator cannot use customized Passport alarm or state change notification (SCN) records.

1. Using the MDP Configuration tool, select **Passport**.
2. Click the button box **Collect BDF data for outage calculator**.

   Note: If the MDP configuration option **BDF in dump directories** has not been enabled for datatypes Alarm and scn, this option is not available.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Setting the File Manager log level

1. Using the MDP Configuration tool, select **Passport**.
2. To change the current File Manager log level, click the button box **Passport File Manager log level**.

   The log levels are indicated (0 - 4).
3. Select the appropriate log level. The default is level 3.

   Log levels are described in section "Log levels" (page 207).
4. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

PF data management

For an introduction to converting spooled data to published format (PF), see "Converting switch data to published format" (page 29).

The following topics are discussed in this section:

- "Converting Passport accounting raw data to PF" (page 135)

- “Setting PF data storage format” (page 136)
- “Enabling PF backward compatibility” (page 135)
- “Setting PF data storage format” (page 136)

Converting Passport accounting raw data to PF

1. Using the MDP Configuration tool, select **Passport**.
2. Click the button box **Convert Accounting files to PF**.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Setting PF data encoding

1. Using the MDP Configuration tool, select **Passport**.
2. Click one of the radio buttons beside **PF encoding**.
   - To select ASCII encoding, click the radio button **ASCII**.
   - To select EBCDIC encoding, click the radio button **EBCDIC**.

   IBM customer hosts usually use EBCDIC and VAX customer hosts usually use ASCII.

   Note: If **Convert Accounting files to PF** has not been enabled, you cannot set PF encoding.

   The default is neither option is selected.
3. Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Enabling PF backward compatibility

The published format (PF) backward compatibility mode is described in section “Converting switch data to published format” (page 29).

1. Using the MDP Configuration tool, select **Passport**.
2. Click the button box **PF backward compatibility mode**.

   A check mark is displayed in the button box.

   The default is this option is not selected.

3 Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Setting PF data storage format

1 Using the MDP Configuration tool, select **Passport**.

2 Click one of the radio buttons beside PF storage.

- To select big-endian, click the radio button **Big**.
- To select small-endian, click the radio button **Little**.

Note: If **Convert Accounting files to PF** has not been enabled, you cannot set PF storage.

IBM customer hosts usually use big-endian and VAX customer hosts usually use small-endian.

Note: If **PF encoding** is set to EBCDIC, PF storage must be set to big-endian.

The default is neither option is selected.

3 Click **Save Passport** to save the configuration change and to restart the Passport File Manager.

Collecting Passport data

This section describes how to configure the Mangement Data Provider (MDP) software to collect Passport data.

An introduction to collecting Passport performance metrics on the MDP is provided in section “Data collection - MDP” (page 51) and a description of MDP related hosts is in section “Hosts” (page 34). For information about the File Prober Manager and file prober command line settings, see “Collecting Passport data” (page 182).

The following topics are discussed in this section:

- “Defining the Passport network” (page 137)
- “Managing data collection entries” (page 137)
- “Setting data collection options” (page 140)
- “Scheduling data collection” (page 144)

Defining the Passport network

Passport network information is obtained from the Preside Multiservice Data Manager (MDM) Host Group Directory Server (HGDS). The HGDS can be located on the MDP host or on a remote MDM host.

Use the Host Group Administration tool (hgadmin) to define the Passport network. For information about the Host Group Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

Managing data collection entries

Use this section to create data collection entries for each Passport group and each Passport datatype.

CAUTION

If File Prober crontab entries exist, the File Prober Manager cannot be started. Remove the crontab entries and then use the procedure "Creating a new data collection entry" (page 138) or import the crontab entries using the procedure "Importing File Prober crontab entries" (page 138).

The following topics are discussed in this section:

- "Importing File Prober crontab entries" (page 138)
- "Creating a new data collection entry" (page 138)
- "Activating and deactivating a data collection entry" (page 139)
- "Changing a data collection entry" (page 139)
- "Removing a data collection entry" (page 140)

Importing File Prober crontab entries

Nortel Networks recommends that you use the File Prober Manager to control File Probers. If you choose not to use the File Prober Manager, existing crontab entries created to launch scheduled Passport data collection continue to collect Passport data.

If the File Prober Manager is not used to control File Probers: MDP host and Passport passwords are not secure, connectivity to Passports and MDP disk space availability cannot be confirmed prior to data transfers, the data transfer retry mechanism cannot be used, and data collection cannot be monitored using the Preside Multiservice Data Manager (MDM) Alarm Display.

Use the following procedure to import File Prober crontab entries:

> ***Note:*** This procedure can only be used to import crontab entries created by the MDP administrator userID. If crontab entries were created by another userID (for example, mdpprobe), you must manually remove the crontab entries and then create new data collection entries using the procedure "Creating a new data collection entry" (page 138).

1. Using the MDP Configuration tool, select **File Prober**.
2. Existing File Prober crontab entries are displayed in the **Entries** panel.

   These entries are greyed-out to indicate that they cannot be used by the File Prober Manager to collect Passport data.

   If there are no old File Prober crontab entries for the MDP administrator userID, the **Import Crontab** button is greyed-out.
3. If File Prober crontab entries exist, click the **Import Crontab** button.

   The old File Prober crontab entries become comments in the crontab, but are not deleted. This enables roll-back to the previous method of data collection if problems occur.

   New data collection entries are created for the File Prober Manager using the settings of the old File Prober crontab entries.
4. If a data collection entry requires changes, follow the procedures in section "Changing a data collection entry" (page 139).
5. Click **Save File Prober** to save the configuration change and to restart the Passport File Prober Manager.

Creating a new data collection entry

1. Using the MDP Configuration tool, select **File Prober**.

2 Complete the procedures in section “Setting data collection options” (page 140).

3 Complete the procedure in section “Scheduling data collection” (page 144).

4 Click **Add**.

The new data collection entry is added to the **Entries** panel.

The data collection entry is activated (ready to begin collecting data at the scheduled time).

Activating and deactivating a data collection entry

1 Using the MDP Configuration tool, select **File Prober**.

2 To activate a data collection entry, click the button box beside the data collection entry in the **Entries** panel.

A check mark is placed in the button box and the data collection entry is activated.

3 To deactivate a data collection entry, click the button box beside the data collection entry in the **Entries** panel.

The check mark is removed from the button box and the data collection entry is deactivated.

4 Click **Save File Prober** to save the configuration change and to restart the Passport File Prober Manager.

Changing a data collection entry

1 Using the MDP Configuration tool, select **File Prober**.

2 Select a data collection entry from the list of entries in the **Entries** panel.

The data collection entry parameters are indicated in the Collection Options and Collection Time windows. For example, if specific days of the month were selected using the calendar in the Collection Time window, the days are indicated on the calendar in that window.

3 Complete the procedures in section “Setting data collection options” (page 140).

4 Complete the procedure in section “Scheduling data collection” (page 144).

5 Click **Update**.

The updated data collection entry is replaced in the **Entries** panel.

Removing a data collection entry

1. Using the MDP Configuration tool, select **File Prober**.
2. Select a data collection entry from the list of entries in the **Entries** panel.
3. Click **Delete**.

   The data collection entry is removed from the **Entries** panel.

Setting data collection options

The following topics are discussed in this section:

- "Selecting the Passport datatype to collect" (page 140)
- "Selecting the Passport group" (page 140)
- "Selecting the primary MDP" (page 141)
- "Selecting the backup MDP" (page 141)
- "Using Passport node names or nodeIDs in MDP file names" (page 142)
- "Configuring the Passport spool file rollover setting" (page 142)
- "Configuring the Passport spool file no erase setting" (page 143)
- "Setting the number of spool files to collect" (page 143)
- "Setting the File Prober timeout" (page 144)
- "Setting the File Prober log level" (page 144)

Selecting the Passport datatype to collect

1. Select the **Collection Options** tab.
2. Click the pull-down button box beside **DataType**.

   A list of the Passport datatypes is displayed (acc, sta, log, ala, scn).
3. Select one of the Passport datatypes.

Selecting the Passport group

1. Select the **Collection Options** tab.
2. Click the pull-down button box inside the **Passport Group** panel.

   A list of Passport groups is displayed.

   This list is obtained from the Preside Multiservice Data Manager (MDM) Host Group Directory Server (HGDS) configuration file.

3 Select one of the Passport groups.

4 Type the Passport access userID in the data entry box **User**.

This Passport userID must be configured on all of the Passports within the Passport group.The Passport permissions required by this userID are

- scope of **network**, or greater
- impact of **config**, or greater
- AllowedAccess including **FMIP** and **FTP**

5 Type the password for the Passport access userID in the data entry box **Password**.

Note: The password is stored in an encrypted format.

Selecting the primary MDP

The role of the primary MDP is described in section "Primary MDP" (page 34).

Note: If a primary host is not defined, the File Prober Manager cannot be started.

1 Select the **Collection Options** tab.

2 In the **Primary MDP Host** panel

a. type the name of the primary MDP host in the **Host** data entry box.

b. type the MDP administrator userID in the data entry box **User**.

c. type the password for the MDP administrator userID in the data entry box **Password**

The password is stored in an encrypted format.

Selecting the backup MDP

The role of the backup MDP is described in section "Backup MDP" (page 35).

1 Select the **Collection Options** tab.

2 In the **Backup MDP Host** panel

a. type the name of the backup MDP host in the **Host** data entry box.

b. type the MDP administrator userID in the data entry box **User**.

c. type the password for the MDP administrator userID in the data entry box **Password**

The password is stored in an encrypted format.

Using Passport node names or nodeIDs in MDP file names

CAUTION
If you plan to transfer files to a billing host using shortened file names, ensure that the first 4 characters of the nodeID or node name is unique.

1 Select the **Collection Options** tab.

2 Click one of the radio buttons.

- To include Passport nodeIDs in MDP filenames, click the radio button **Node ID**.
- To include Passport nodenames in MDP filenames, click the radio button **Node name**.

The default is to include Passport nodeIDs in MDP filenames; **Node ID** is selected.

Configuring the Passport spool file rollover setting

The File Prober can close an open Passport spool file before transferring it to the MDP. The spool file is moved to the Passport directory /spooled/closed/<datatype> and a new file is opened in the Passport directory /spooled/opened/<datatype> where <datatype> is one of the Passport datatypes selected for collection.

Note: Passport accounting spool files do not automatically close after 30 minutes.

1 Select the **Collection Options** tab.

2 Click **Rollover**.

A check mark is placed in the button box.

The default is this option is not selected.

Configuring the Passport spool file no erase setting

Using this procedure prevents the removal of closed Passport spool files after data collection. By default, Passport spool files are deleted after data collection.

CAUTION

If Passport accounting files are not deleted after collection by the File Prober, duplicate accounting records can be collected. Use this option for testing purposes only.

1 Select the **Collection Options** tab.

2 Click **No erase on Passport**.

A check mark is placed in the button box.

The default is this option is not selected.

Setting the number of spool files to collect

You can set the maximum number of files collected during a single data collection. Before using this option, carefully calculate the required data collection start times.

1 Select the **Collection Options** tab.

2 Type the number of files in the data entry box **Max. Files to Collect**.

To specify the collection of all closed spool files, type *****.

There is no limitation on the number of spool files to collect.

The default is 60 files.

Setting the File Prober timeout

You can set the number of seconds the File Prober waits before halting execution if a Passport does not respond.

CAUTION

A Passport to MDP FTP connection can time-out when transferring very large amounts of data. If this problem occurs with a frame relay connection and a data transfer cannot be completed, or if very large data transfers on a frame relay connection to the MDP is anticipated, configure the frame relay network-to-network interface (FrNni) data link connection identifier (DLCI) to use a transfer priority (TP) of normal (6).

1 Select the **Collection Options** tab.

2 Type the number of seconds in the data entry box **FTP timeout interval (sec)**.

The default is 300 seconds.

Setting the File Prober log level

1 Select the **Collection Options** tab.

2 Click **log level**.

The log levels are indicated (0 - 4).

3 Select the appropriate log level. The default is level 3.

Log levels are described in section “Log levels” (page 207).

Scheduling data collection

CAUTION

Scheduling data collections that coincide with time of day accounting (TODA) periods on the Passport switch can result in starvation of the FTP process and data collection will be unsuccessful.

1 Select the **Collection Time** tab.

2 Using the buttons in the **Data Collection Start Time** panel, specify the File Prober start times.

To select multiple units, press the control keyboard button and click on individual units. For example, to select multiple days of the week click Monday and then press the control keyboard button and click Wednesday.

To select a range of units, click the first unit in the range, press the shift keyboard button and click the last unit in the range. For example, to select a range of days, click Monday and then press the shift keyboard button and click Wednesday.

A check mark in the **All** box can be used to specify the entire range of a unit. For example, to specify data collection on every day of the week select **All** for **Every day on...**.

For example, to collect the Passport data at 2:00 AM each day, select: 2 for the hour, 0 for the minute, All for the month, and All for the day of the week.

Note: Do not schedule collections for midnight. Conflicts with automatic processes will occur if you do.

a. Select the month (Jan - Dec) or All.

b. Select the hour(hr) (0 - 23) or All.

c. Select the minute(min) (0 - 59) or All.

d. Select the day of the week (Sunday - Saturday) or All.

e. To select specific days of each month, select the days to collect data by clicking the dates on the calendar.

You cannot select specific days of each month using the calendar and select days of the week.

Configuring SRS

If previous versions of the Statistics Retrieval System (SRS) were used on this Management Data Provider (MDP), perform “Consolidating RCFs from previous versions of SRS” (page 145).

If SRS is new to this MDP, perform “Configuring SRS” (page 147) to configure SRS.

Consolidating RCFs from previous versions of SRS

1 If one RCF was used to poll all Passport families, rename the record content file (RCF) to the following filename.

```
/opt/MagellanMDP/cfg/mdp/rcf/pp/
pp_srs_<identifier>.rcf
```

If a different RCF was used to poll each Passport family (multiple RCFs), create the following file.

```
/opt/MagellanMDP/cfg/mdp/rcf/pp/
pp_srs_<identifier>.rcf
```

where <identifier>
is the name for this RCF (for example, Version1).

2 If multiple RCFs were previously used to poll each Passport family, copy-and-paste each unique RCF component and component attribute entry into the new RCF.

3 Use 241-5701-060 *Passport 7400, 15000, 20000 Components* to obtain the maximum value for each component attribute.

The maximum attribute value is added to the raw attribute value to calculate delta values when the attribute value reaches maximum threshold and rolls-over between two polls. The maximum value is appended to raw attribute entries for reference, only.

4 Using a system editor, edit the file created in step 1. Append the maximum value to each component attribute entry in the form

```
Delta: <attribute> <maximum value>
Raw: <attribute> <maximum value>
```

For example,

```
Delta: txCellClp 18446744073709551615
Raw: txDiscardClp 18446744073709551615
```

5 Save the new RCF.

6 To select additional Passport groups to poll, see “Adding a Passport group to poll” (page 152).

7 To select additional Passport components and attributes to poll or to select specific instances of Passport components, see “Selecting Passport components and attributes” (page 152).

8 To use the new RCF to poll Passports, see “Selecting the RCF to commit” (page 148).

The new RCF identifier is now available in the pull-down list of the **Committed RCF Identifier** button.

Configuring SRS

1 Use the Host Group Administration tool hgadmin to configure HGDS with Passport network configuration data. This data is stored in the HGDS configuration file /opt/MagellanNMS/cfg/HGDS.cfg.

For more information about the passport.config command, see 241-6001-303 *Preside MDM Administrator Guide*.

If you are using MDM on another host (Passport access host) to provide network connectivity to the polled Passports, ensure that the content of the HGDS configuration file HGDS.cfg on the MDP host is the same as the content of the HGDS configuration file HGDS.cfg on the MDM host.

2 Use the MDM Server Administration tool to start the HGDS and FDTM servers.

Note: If you are using MDM on another host (Passport access host) to provide network connectivity to the polled Passports, you need not start FDTM on the MDP host.

If the HGDS and FDTM servers are running, use the command /opt/MagellanNMS/bin/passport.kick to update the HGDS with new information without stopping and restarting the HGDS and FDTM servers.

For more information about the Server Administration tool and the passport.kick command, see 241-6001-303 *Preside MDM Administrator Guide*.

3 Log on to the MDP as the MDP administrator.

4 Using the MDP Configuration tool, select the **Passport SRS** tab.

The MDP **Statistics Retrieval System** window opens.

5 To select the Passport components and attributes to poll, see “Selecting Passport components and attributes” (page 152).

6 To configure Passport SRS options, use

- “Selecting the RCF to commit” (page 148)
- “Configuring the SRS polling interval” (page 149)
- “Configuring the maximum SRS BDF file size” (page 150)
- “Configuring the BDF file closure interval” (page 150)
- “Configuring SRS to backup BDF files” (page 151)
- “Setting the compression of BDF data” (page 151)
- “Setting the BDF field delimiter” (page 151)

- "Configuring the SRS log level" (page 151)
- "Configuring a Passport access host" (page 151)
- "Adding a Passport group to poll" (page 152)
- "Removing a Passport group from SRS polling" (page 152)

7 If necessary, edit the SRS RDFs to rearrange statistics. Use a system editor to edit the file

`/opt/MagellanMDP/cfg/mdp/rdf/pp/srs/pp_srs_<identifier>.rdf`

where <identifier> is the name for this RDF (for example, Version1).

Note 1: Fields that contain delta values have Delta appended to the field name. Fields that contain raw attribute values have Raw appended to the field name.

Note 2: Do not delete statistics for attributes that exist in the RCFs. Attributes are then polled but not reported causing unecessary network congestion.

8 Click **Save SRS** to save the SRS configuration updates and commit the RCF.

If this is not the first time SRS is configured, clicking **Save SRS** restarts SRS.

9 If this is the first time SRS is configured, use the MDM Server Administration tool (SVM) to start SRS. For more information about SVM, see 241-6001-303 *Preside MDM Administrator Guide*.

Start SRS using the following command:

`/opt/MagellanMDP/bin/mdpsrs [-ignorenegativedelta | -ind]`

where:
[-ignorenegativedelta | -ind] instructs SRS to ignore negative deltas and not to perform roll-over calculations. Without this parameter the maximum attribute value is added to the raw attribute value to calculate delta values when the attribute value reaches maximum threshold and rolls-over between two polls.

Selecting the RCF to commit

1 Click the button box at the far-right of **Committed RCF Identifier**.

This button box displays the currently committed RCF.

2 Select an RCF.

For more information about RCFs, see “Selecting Passport components and attributes” (page 152).

Note: A record description file (RDF) is created when you select an RCF and save this MDP configuration change. The pathname of the SRS RDF is:

```
/opt/MagellanMDP/cfg/mdp/rdf/pp/srs/
pp_srs_<identifier>.rdf
```

where <identifier> is the name for this RCF and RDF (for example, Version1).

Configuring the SRS polling interval

1 Type the SRS polling interval in the data entry box **Polling Interval**. The polling interval is specified in seconds.

The default polling interval is 900 seconds (15 minutes). The minimum polling interval is 10 seconds and the maximum polling interval is 65535 seconds.

Note: Configure the polling interval as high as possible to avoid network performance degradation, to ensure polling intervals are not skipped, and to ensure delta statistics reflect the configured polling interval.

The first poll occurs when SRS is started. Subsequent polls occur at specified intervals after the first poll.

The time of polling for each Passport component is not guaranteed to occur exactly on the polling interval. For example, component EM/PP303 AtmIf/31 Vcc/0.32 may not be polled exactly 900 seconds after it was polled previously (if the default polling interval was used). Response time can be affected by network activity and Passport traffic load.

If a response is not received from a polling interval before the subsequent polling interval is scheduled, the subsequent polling interval is skipped. Another poll is not attempted until the next polling interval. Missed polling intervals are caused by a polling interval that is too small.

Configuring the maximum SRS BDF file size

Specify the number of records written to the output BDF file in directory /opt/MagellanMDP/data/mdp/dump/srs before SRS closes it.

1 Type the maximum BDF file size in the data entry box **Max number of BDF records in file**.

The default is 500 records.

Note: Configure the maximum number of SRS BDF records or the SRS BDF file closure time interval. Failure to configure one of these configuration settings results in an error message. If both of these configuration settings are configured, SRS closes the BDF file when the criteria for either setting is reached.

Configuring the BDF file closure interval

Specify when SRS is to close the BDF file in the directory /opt/MagellanMDP/data/mdp/dump/srs.

1 Click **File Close Interval**.

The time intervals are indicated (15 or 30).

2 Select the appropriate time interval.

The default is this option is not selected.

If 15 is selected, the SRS BDF file is closed on the hour and every 15 minutes afterwards (for example, 0000hrs, 0015hrs, 0030hrs, and 0100hrs).

If 30 is selected, the SRS BDF file is closed on the hour and every 30 minutes afterwards (for example, 0000hrs, 0030hrs, and 0100hrs).

Note: Configure the maximum number of SRS BDF records or the SRS BDF file closure time interval. Failure to configure one of these configuration settings results in an error message. If both of these configuration settings are configured, SRS closes the BDF file when the criteria for either setting is reached.

Configuring SRS to backup BDF files

Configure SRS to archive closed SRS BDF files to the directory /opt/MagellanMDP/data/mdp/backup/srs

1 Click **Backup BDF file**.

A check mark is displayed in the button box.

The default is this option is not selected.

Setting the compression of BDF data

1 Click **BDF output compression**.

A check mark is displayed in the button box.

The default is this option is not selected.

Setting the BDF field delimiter

1 Type the hex code representation for the equivalent character in the data entry box **BDF delimiter**.

The default is DEL (0x7F).

Note: Do not use alpha-numeric characters as these can make it difficult to read the output files. Do not use the following characters: "|", "^", "(", ")", " ", ",", ".", or "/".

Configuring the SRS log level

1 Click **Passport SRS log level**.

The log levels are indicated (0 - 4).

2 Select the appropriate log level. The default is level 3.

For more information about log levels, see “Log levels” (page 207).

Configuring a Passport access host

Configure SRS to use another MDM host to provide network connectivity to Passports. Both the MDP host and the MDM host can resolve hostnames to IP addresses.

1 Type a hostname or IP address in the data entry box **Passport Access Host**.

The default is the local host.

Adding a Passport group to poll

1 Click **Add empty row** in the **Edit polling groups** panel.

The **groupname** column displays a list of the Passport groups available from HGDS. If SRS is unable to connect to the HGDS server, the following message is displayed:

```
Passport SRS configuration: queryHGDS: Cannot connect
to HGDS server.
SRS group selection is not available.
```

2 Select a Passport group.

3 Type the following information in the data entry boxes:

a. In the **login ID** column, type the userID for the Passport nodes.

b. In the **password** column, type the password for the Passport userIDs.

The password is stored in an encrypted format.

Removing a Passport group from SRS polling

1 In the **Edit polling groups** panel, select the row that contains the Passport group to remove.

2 Click **Delete group**.

The selected row is removed.

Selecting Passport components and attributes

Select Passport components and attributes to poll by using the MDP Configuration tool. Selected Passport component and attribute information is stored in a record content file (RCF).

This section includes the following information:

- "Starting the RCF Editor" (page 152)
- "Selecting Passport components and attributes" (page 153)
- "Selecting Passport component instances" (page 154)

Starting the RCF Editor

1 Using the MDP Configuration tool, select **Passport SRS**.

The **MDP Statistics Retrieval System** window opens.

2 Click **Start RCF editor**.

The **MDP RCF Editor** window opens.

The MDP RCF Editor window has two panels. Select a Passport component in the left panel and the right panel contains configured component instances. Select a Passport component attribute in the left panel and the right panel contains configured component attribute criteria.

3 To create a new RCF, use the current window contents.

To edit an existing RCF, select **File -> Open** to display a list of existing RCFs and to select the RCF to edit.

Note: An RCF cannot be editted and saved using the same identifier as the currently committed RCF.

4 In the MDP RCF Editor window, select one of the following:

- **all**
  to display all Passport components and attributes. Select this option if this is the first configuration of SRS. This option enables you to choose any Passport component and attribute.
- **configured**
  to display those components and attributes configured for SRS polling. Select this option if this is not the first configuration of SRS and you are editing an existing RCF.

The default is **all**.

Selecting Passport components and attributes

1 In the left panel, navigate through the Passport components.

- Click the circled dot to the left of the component to display sub-components.
- Use the slider bar to display additional components and attributes.

2 To select a component attribute, click the button box beside the component attibute.

A check mark is displayed in the button box.

The right panel displays the polling options for component attributes: raw, delta, or both.

3 To select a polling option, click the appropriate radio button: **raw**, **delta**, or **both**.

4 When your selection of component attributes is complete and you do not need to configure any component instances, use

- **File -> New** to clear the window of all updates and return to the original view.
- **File -> Save** to save the updated RCF /opt/MagellanMDP/cfg/mdp/rcf/pp/pp_srs_<identifier>.rcf where <identifier> is the name for this RCF. The previous version of this file is overwritten.
- **File -> Save As** to save the updated RCF /opt/MagellanMDP/cfg/mdp/rcf/pp/pp_srs_<identifier>.rcf where <identifier> is the name for this RCF. A new file is created.
- **File -> Exit** to leave the RCF Editor without saving your updates.

To configure polling of component instances, see “Selecting Passport component instances” (page 154).

Selecting Passport component instances

Failure to specify any components instances results in polling of all instances of the previously selected component. Otherwise, only the selected component instances are polled.

1 In the left panel, navigate through the Passport components.

- Click the circled dot to the left of the component to display sub-components.
- Use the slider bar to display additional components.

2 To select a component, click the component.

If this is the first configuration of SRS, the right panel **Polling Instances** is empty.

If this is not the first configuration of SRS, the right panel **Polling Instances** lists existing configurations for polling Passport components using this RCF.

3 To add a new polling instance, click **add** in the right panel.

To edit an existing polling instance, click the polling instance to be editted and then click **edit**.

The **Polling Instance details** dialog window opens.

4 To use the **Polling Instance details** dialog, perform the following:

a. In the **Polling Instance** panel specify the instances of components to poll.

The component, and all parent components, are indicated by the column headings in the Polling Instance panel.

If the current settings for this component are not suitable, click **Add** to create a new polling instance for the selected component.

The next available row in the Polling Instance panel is highlighted.

Enter: a range of components to poll, in the form [x - x]; or a specific component instance, in the form or a string or decimal identifier; or an asterisk "*" to indicate all the components at this component level. The valid ranges and suggested entries are indicated in the header row for each component level.

If an asterisk at is used at one component level, an asterisk must be used at all selected sub-component levels for that component instance. For example, atmif/* vcc/3 is not acceptable.

Using an asterisk to specify all instances of a component is an efficient use of MDP resources. Specifying every instance of a component can slow the performance of this application.

The maximum number of component instances per polling instance is 1000.

b. In the **Use the configured SRS polling interval** section, select the polling interval configured in the Statistics Retrieval System Configuration window (see "Configuring the SRS polling interval" (page 149)) or select **Override** to override the configured polling interval by typing a new polling interval to be used for this polling instance, only.

The default is the polling interval configured by the Statistics Retrieval System window.

c. In the **Groups/Nodes** section, select the Passport groups or individual Passport nodes to poll for the selected component.

The default is that all Passport groups, and all Passport nodes within the groups, as configured using the Statistics Retrieval System Configuration window, are polled.

If a Passport group is selected to poll, all Passport nodes in that group are polled.

If you click one of the Passport groups listed in the left panel of the **Groups/Nodes** section, the individual Passport nodes are listed in

the right panel. Select a Passport node by clicking on the nodename. A check mark is displayed beside the Passport nodename. If you select a Passport node you cannot select the group of which this node is a member.

d. Click the **Ok** button to accept the polling instance details and return to the RCF Editor window.

The Polling Instances panel in the RCF Editor window now lists the new configuration by indicating the Passport groups and nodes identified for polling using the new polling instance.

5 When you have completed the configuration of component instances, use

- **File -> New** to clear the window of all updates and return to the original view.
- **File -> Save** to save the updated RCF /opt/MagellanMDP/cfg/mdp/rcf/pp/pp_srs_<identifier>.rcf where <identifier> is the name for this RCF. The previous version of this file is overwritten.
- **File -> Save** As to save the updated RCF /opt/MagellanMDP/cfg/mdp/rcf/pp/pp_srs_<identifier>.rcf where <identifier> is the name for this RCF. A new file is created.
- **File -> Exit** to leave the RCF Editor without saving your updates.

Configuring outage calculation

This section describes how to configure the Management Data Provider (MDP) for Passport outage calculation.

The following topics are discussed in this section:

- "Prerequisites" (page 157)
- "Setting the BDF field delimiter" (page 157)
- "Calculating combined outages" (page 157)
- "Setting the minimum threshold for outages" (page 157)
- "Setting the maximum threshold for outages" (page 158)
- "Setting the number of days to keep unmatched OOS records" (page 158)
- "Setting the Outage Calculator log level" (page 158)

Prerequisites

Before configuring the Management Data Provider (MDP) to calculate Passport outages, ensure that you have:

- configured the MDP Outage Controller. For more information, see “Configuring the Outage Controller” (page 115).
- configured Passport alarm and state change notification (SCN) raw data to be converted to bulk data format (BDF). For more information, see “Converting Passport raw data to BDF” (page 127).
- configured the assignment of Passport alarm and SCN BDF data to outage calculation. For more information, see “Assigning data to outage calculation” (page 134).

Setting the BDF field delimiter

1. Using the MDP Configuration tool, select **Passport Outage**.
2. Type the hex code representation for the equivalent character in the data entry box **Outage Calculator BDF delimiter**.

   The default is DEL (0x7F).

   Note: Do not use alpha-numeric characters as these can make it difficult to read the output files. Do not use the following characters: "|", "^", "(", ")", " ", ",", “.”, or "/".
3. Click **Save** to save the configuration change.

Calculating combined outages

1. Using the MDP Configuration tool, select **Passport Outage**.
2. Click **Calculate combined outages**.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save** to save the configuration change.

Setting the minimum threshold for outages

Outages that exceed this threshold are included in outage calculations.

1. Using the MDP Configuration tool, select **Passport Outage**.
2. Type the minimum threshold value in the data entry box **Minimum threshold value of outages**.

Type the threshold in units of seconds(s), minutes(m), hours(h), or days(d). For example: 15s, 30m, 1h, or 7d.

The default is zero. The maximum is 365d.

3 You can also use supplied values. Click the button box **Minimum threshold value of outages**.

The suggested values are indicated.

4 Click **Save** to save the configuration change.

Setting the maximum threshold for outages

Outages that are less than this threshold are included in outage calculations.

1 Using the MDP Configuration tool, select **Passport Outage**.

2 Type the maximum threshold value in the data entry box **Maximum threshold value of outages**.

Type the threshold in units of seconds(s), minutes(m), hours(h), or days(d). For example: 15s, 30m, 1h, or 7d.

The default is 7d. The maximum is 365d.

3 You can also use supplied values. Click **Maximum threshold value of outages**.

The suggested values are indicated.

4 Click **Save** to save the configuration change.

Setting the number of days to keep unmatched OOS records

1 Using the MDP Configuration tool, select **Passport Outage**.

2 Type the number of days in the data entry box **Number of days to keep unmatched OOS records**.

The default is 100 days.

3 Click **Save** to save the configuration change.

Setting the Outage Calculator log level

1 Using the MDP Configuration tool, select **Passport Outage**.

2 Click **Outage Calculator log level**.

The log levels are indicated (0 - 4).

3 Click on the appropriate log level.

The default is level 3.

For more information about log levels, see “Log levels” (page 207).

4 Click **Save** to save the configuration change.

Chapter 4
Configuring MDP for DPN-100

This section describes how to configure the Management Data Provider (MDP) to collect and convert DPN-100 performance metrics.

The following topics are discussed in this section:

- "Prerequisites" (page 162)
- "Storing DPN-100 raw data" (page 162)
- "BDF data management" (page 163)
- "Assigning data to outage calculation" (page 166)
- "Setting the File Manager log level" (page 167)
- "PF data management" (page 167)
- "Configuring the switch" (page 169)
- "Collecting DPN-100 data" (page 171)
- "Configuring outage calculation" (page 171)

After the MDP software has been configured for DPN-100 data management, follow the instructions in section "Collecting DPN-100 data" (page 171) to begin collecting DPN-100 data.

Prerequisites

Before configuring the Management Data Provider (MDP) software to manage DPN-100 data, ensure that you have:

- reviewed 241-6001-102 *Preside MDM Planning Guide.*
- reviewed the Preside Multiservice Data Manager (MDM) Release Supplement for this release.
- installed the MDP software - see 241-6001-100 *Preside MDM Installer Guide*.
- configured data file retention and the minimum MDP disk space requirements - see “Configuring data file retention” (page 94).
- launched the MDP Configuration tool - see “Launching the MDP Configuration tool” (page 87).

Storing DPN-100 raw data

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Account, Stats, Alarm, or Log; click a button box beside **Backup raw files**. For example, to backup accounting raw data, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.

   The raw switch data is stored in sub-directories of the directory /opt/MagellanMDP/data/mdp/backup.
3. Repeat, as necessary, for each datatype.
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

BDF data management

An introduction to converting data to bulk data format (BDF) is provided in section “Converting switch data to bulk data format” (page 25).

The following topics are discussed in this section:

- “Converting DPN-100 raw data to BDF” (page 163)
- “Archiving BDF data” (page 163)
- “Setting the BDF field delimiter” (page 164)
- “Setting BDF data compression” (page 164)
- “Setting the BDF conversion log level” (page 165)
- “Setting the BDF conversion escape character” (page 166)

Converting DPN-100 raw data to BDF

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Account, Stats, Alarm, or Log; click a button box beside **Convert raw files to BDF in dump directories**. For example, to convert accounting raw data to BDF, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.

   The converted data is written to sub-directories of the directory /opt/MagellanMDP/data/mdp/dump.
3. Repeat, as necessary, for each datatype.
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Archiving BDF data

Individual BDF records can be stored in a customized directory structure using dates, datatypes, or namsIDs.

> ***Note:*** Use the MDP Configuration tool window **BDF Archiving** to create the archive directory structure before selecting the DPN datatypes to archive. For more information, see “Configuring BDF archiving” (page 96).

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Account, Stats, Alarm, or Log; click a button box beside **Convert raw files to BDF in the archive directories**. For example, to convert accounting raw data to BDF and write the converted BDF records to the archive directory structure, click on the button box below **Account**.

   Note: The option **Convert raw files to BDF in the dump directories** must be enabled before this option can be enabled.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Repeat, as necessary, for each datatype.
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting the BDF field delimiter

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Account, Stats, Alarm, or Log; type the hex code representation for the equivalent character in the data entry box beside **BDF field delimiter**. For example, to set the BDF field delimiter for accounting files, type the hex code in the data entry box below **Account**.

   The default is DEL (0x7F) for all datatypes.

   Note: Do not use alpha-numeric characters as these can make it difficult to read the output files. Also, do not use the following special characters: "|", "^", "(", ")", " ", ",", ".", or "/".
3. Repeat, as necessary, for each datatype.
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting BDF data compression

BDF records with 3, or more, fields containing null values can be compressed to save disk space and transmission bandwidth. In BDF files, the start of the compression is indicated by ^<count> where <count> is the number of empty fields. For example, ^5 indicates 5 consecutive empty fields.

CAUTION
If the DPN Outage Calculator is used, do not apply data compression to alarm files. The DPN Outage Calculator does not support compressed data.

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Account, Stats, Alarm, or Log; click a button box beside **BDF output compression**. For example, to compress accounting data, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.
3. Repeat, as necessary, for each datatype.
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting the BDF conversion log level

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Account, Stats, Alarm, or Log; click a button box beside **BDF converter log level**. For example, to set the BDF converter log level for accounting data conversion, click the button box below **Account**.

   The log levels are indicated (0 - 4).
3. Select a log level.

   The default log level is 3 for all datatypes.

   Log levels are described in section “Log levels” (page 207).
4. Repeat, as necessary, for each datatype.
5. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting the BDF conversion escape character

A generic escape character can be set to mask characters that cannot be interpreted. If any delimiters, repeating field delimiters, or escape characters (generic or compressed) are encountered in data fields with a type of string, the string is replaced with <escape character><hex code>, where <hex code> is the 2-digit hexadecimal value of the character.

The escape character is only required for DPN datatypes: alarm and log.

1. Using the MDP Configuration tool, select **DPN**.
2. Select a DPN datatype: Alarm or Log; type the BDF escape character in a data entry box beside **BDF output escape char**. For example, to set the BDF escape character for alarm files, type the escape character in the data entry box below **Alarm**.

   The default is % for all three datatypes.
3. Repeat, as necessary, for each datatype.
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Assigning data to outage calculation

DPN outage calculation is described in section “Value-added applications” (page 68) and “Value-added data applications” (page 231).

Configure the MDP Outage Controller before performing this procedure. For more information, see “Configuring the Outage Controller” (page 115).

1. Using the MDP Configuration tool, select **DPN**.
2. Click **Collect BDF data for outage calculator**.

   Note: If **Convert raw files to BDF in the dump directories** has not been enabled for datatype alarm, this option is not available.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting the File Manager log level

1. Using the MDP Configuration tool, select **DPN**.
2. To change the current File Manager log level, click **DPN File Manager log level**.

   The log levels are indicated (0 - 4).
3. Click the appropriate log level. The default is level 3.

   Log levels are described in section “Log levels” (page 207).
4. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

PF data management

For an introduction to converting data to published format (PF), see “Converting switch data to published format” (page 29).

The following topics are discussed in this section:

- “Converting DPN-100 accounting raw data to PF” (page 167)
- “Setting PF data data storage format” (page 168)
- “Enabling PF backward compatibility” (page 168)
- “Setting PF data data storage format” (page 168)

Converting DPN-100 accounting raw data to PF

1. Using the MDP Configuration tool, select **DPN**.
2. Click the button box **Convert Accounting files to PF**.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting PF data encoding

1. Using the MDP Configuration tool, select **DPN**.
2. Click one of the radio buttons beside **PF encoding**.
   - To select ASCII encoding, click the radio button **ASCII**.

- To select EBCDIC encoding, click the radio button **EBCDIC**.

IBM customer hosts usually use EBCDIC and VAX customer hosts usually use ASCII.

Note: If **Convert Accounting files to PF** has not been enabled, you cannot set PF encoding.

The default is neither option is selected.

3 Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Enabling PF backward compatibility

The published format (PF) backward compatibility mode is described in section "Converting switch data to published format" (page 29).

1 Using the MDP Configuration tool, select **DPN**.

2 Click **PF backward compatibility mode**.

A check mark is displayed in the button box.

The default is this option is not selected.

3 Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Setting PF data data storage format

1 Using the MDP Configuration tool, select **DPN**.

2 Click one of the radio buttons beside PF storage.

- To select big-endian, click the radio button **Big**.
- To select small-endian, click the radio button **Little**.

Note: If **Convert Accounting files to PF** has not been enabled, you cannot set PF storage.

IBM customer hosts usually use big-endian and VAX customer hosts usually use small-endian.

Note: If **PF encoding** is set to EBCDIC, PF storage must be set to big-endian.

The default is neither option is selected.

3 Click **Save DPN** to save the configuration change and to restart the DPN File Manager.

Configuring the switch

This section describes how to configure a DPN-100 to collect and transfer performance metrics to a Management Data Provider (MDP) host:

- "Configuring a spooling site for a DPN-100 module" (page 169) instructs you to configure an MDP spooling site on a DPN-100 module.

  For details on using Preside Multiservice Data Manager (MDM) configuration tools, see 241-6001-012 *Preside MDM Configuration Management for DPN User Guide*.

- "Setting the PAD daemon" (page 169) instructs you to modify the PAD daemon configuration to not interfere with MDP File Collector processes.

Configuring a spooling site for a DPN-100 module

1. Under the PM and Data_Spooling components, provision a new Direct Call to the DNA of an MDP host, with a unique protocol ID. The protocol ID is 12 ASCII characters and is case-sensitive.
2. Under the PM and Data_Spooling components, provision the Dump component to direct the dumpsite of the accounting files to the same MDP host.
3. Use the Network Call Redirection System to redirect the files to a backup MDP host in case the primary MDP host is not functioning. For details about Network Call Redirection, see 241-1001-115 *DPN-100 Call Redirection System User Guide*.

Setting the PAD daemon

When you configure X.25 for Solaris, you need to modify the PAD daemon configuration so that it does not interfere with MDP File Collector processes.

Modifying the PAD daemon configuration

1. From the root user account, run the X25 tool; type

   `/opt/SUNWconn/x25/bin/x25tool &`

   A window is created that includes a series of menu options.
2. Select **Application Configuration** from the menu.
3. Select **PAD**.
4. Select **PAD daemon**.

The PAD Daemon Listen Database window is displayed.

5 Select **Call User Data**.

Three options are displayed.

The following two options are acceptable: **Starts With** and **Matches**. The permitted values are as follows:

a. Starts With 01000000rrrrxxxxxxxxxxxxxxxxxxxx

where:
01000000
is the standard protocol id
rrrr
is a user-definable protocol id (in hex) and must be a value other than the default MDP protocol id (4335).

xxxxxxxxxxxxxxxxxxx
is the call user data, in hex. The length of this field can be truncated.

If the MDP protocol ID has been modified to a value other than the default 4335 values, these modified values cannot be used in the *rrrr* field.

b. Exact Match. The call user data field does not match the following:

010000004335

If the MDP protocol ID has been modified, the value must not conflict with the hex values of the last two bytes of this string.

The selection of a value depends on the manner in which a PAD user logs on. If you do not want the PAD user to enter a Call User Data field in a PAD request, use Exact Match with the value 01000000. However, if Call User Data is wanted, enter an appropriate value (other than 4335 used by the MDP host.).

6 Restart the X.25 connection.

Collecting DPN-100 data

Use the Multiservice Data Manager (MDM) Server Administration tool (SVM) to launch DPN File Collectors. Use the following syntax in the SVM command.

For more information about the DPN File Collector server, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanMDP/bin/mdpcol -pid <PID>
-v /opt/MagellanMDP/data/mdp/spool #<file_collector>
```

where:
<PID> is a unique protocolID for each DPN-100 file collector
<file_collector> is an integer. The first file collector should be numbered 1, the next file collector should be numbered 2, and so on.

Configuring outage calculation

This section describes how to configure the Management Data Provider (MDP) for DPN-100 outage calculation.

The following topics are discussed in this section:

- "Prerequisites" (page 171)
- "Setting the BDF field delimiter" (page 172)
- "Calculating combined outages" (page 172)
- "Setting the minimum threshold for outages" (page 172)
- "Setting the maximum threshold for outages" (page 173)
- "Setting the number of days to keep SET alarms" (page 173)
- "Setting the number of days to keep CLEAR alarms" (page 173)
- "Setting the Outage Calculator log level" (page 173)

Prerequisites

Before configuring the Management Data Provider (MDP) to calculate DPN-100 outages, ensure that you have:

- configured the MDP Outage Controller. For more information, see "Configuring the Outage Controller" (page 115).

- configured DPN-100 alarm raw data to be converted to bulk data format (BDF). For more information, see “Converting DPN-100 raw data to BDF” (page 163).
- configured the assignment of DPN-100 alarm BDF data to outage calculation. For more information, see “Assigning data to outage calculation” (page 166).

Setting the BDF field delimiter

1. Using the MDP Configuration tool, select **DPN Outage**.
2. Type the hex code representation for the equivalent character in the data entry box **Outage Calculator BDF delimiter**.

   The default is DEL (0x7F).

   Note: Do not use alpha-numeric characters as these can make it difficult to read the output files. Do not use the following characters: "|", "^", "(", ")", " ", ",", “.”, or "/".
3. Click **Save** to save the configuration change.

Calculating combined outages

1. Using the MDP Configuration tool, select **DPN Outage**.
2. Click **Calculate combined outages**.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Click **Save** to save the configuration change.

Setting the minimum threshold for outages

Outages that exceed this threshold are included in outage calculations.

1. Using the MDP Configuration tool, select **DPN Outage**.
2. Type the minimum threshold value in the data entry box **Minimum threshold value of outages**.

   Type the threshold in units of seconds(s), minutes(m), hours(h), or days(d). For example: 15s, 30m, 1h, or 7d.

   The default is zero. The maximum is 365d.
3. You can also use supplied values. Click **Minimum threshold value of outages**.

The suggested values are indicated.

4 Click **Save** to save the configuration change.

Setting the maximum threshold for outages

Outages that are less than this threshold are included in outage calculations.

1 Using the MDP Configuration tool, select **DPN Outage**.

2 Type the maximum threshold value in the data entry box **Maximum threshold value of outages**.

Type the threshold in units of seconds(s), minutes(m), hours(h), or days(d). For example: 15s, 30m, 1h, or 7d.

The default is 7d. The maximum is 365d.

3 You can also use supplied values. Click **Maximum threshold value of outages**.

The suggested values are indicated.

4 Click **Save** to save the configuration change.

Setting the number of days to keep SET alarms

1 Using the MDP Configuration tool, select **DPN Outage**.

2 Type the number of days in the data entry box **Number of days to keep SET alarms**.

The default is 100 days.

3 Click **Save** to save the configuration change.

Setting the number of days to keep CLEAR alarms

1 Using the MDP Configuration tool, select **DPN Outage**

2 Type the number of days in the data entry box **Number of days to keep CLEAR alarms**.

The default is 100 days.

3 Click **Save** to save the configuration change.

Setting the Outage Calculator log level

1 Using the MDP Configuration tool, select **DPN Outage**.

2 To change the current Outage Calculator log level, click **Outage Calculator log level**.

The log levels are indicated (0 - 4).

3 Click on the appropriate log level.

The default is level 3.

For more information about log levels, see “Log levels” (page 207).

4 Click **Save** to save the configuration change.

Chapter 5
Configuring MDP for Vector

This section describes how to configure the Management Data Provider (MDP) to collect and convert Vector accounting and performance data. Vector on-switch accounting and performance data collection is also described.

The following topics are discussed in this section:

- "Prerequisites" (page 175)
- "Storing Vector raw data" (page 176)
- "BDF data management" (page 176)
- "Logging File Manager verbose messages" (page 178)
- "Assigning a secondary MDP" (page 178)
- "Collecting Vector data" (page 179)

Prerequisites

Before configuring the Management Data Provider (MDP) software to manage Vector data, ensure that you have:

- reviewed 241-6001-102 *Preside MDM Planning Guide*
- reviewed the Preside Multiservice Data Manager (MDM) Release Supplement for this release.
- installed the MDP software - see 241-6001-100 *Preside MDM Installer Guide*.
- configured data file retention and the minimum MDP disk space requirements - see "Configuring data file retention" (page 94).

- launched the MDP Configuration tool - see “Launching the MDP Configuration tool” (page 87).

Storing Vector raw data

1. Using the MDP Configuration tool, select **Vector**.
2. Select a Vector datatype: Account or Stats; click a button box beside **Backup raw files**. For example, to backup accounting raw data, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.

   The raw switch data is stored in sub-directories of the directory /opt/MagellanMDP/data/mdp/backup.
3. Repeat, as necessary, for each datatype.
4. Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

BDF data management

An introduction to converting data to bulk data format (BDF) is provided in section “Converting switch data to bulk data format” (page 25).

The following topics are discussed in this section:

- “Converting Vector raw data to BDF” (page 176)
- “Setting the BDF field delimiter” (page 177)
- “Setting BDF data compression” (page 177)
- “Logging BDF converter warnings” (page 178)

Converting Vector raw data to BDF

1. Using the MDP Configuration tool, select **Vector**.
2. Select a Vector datatype: Account or Stats; click a button box beside **Convert raw files to BDF**. For example, to convert accounting raw data to BDF, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.

The converted data is written to sub-directories of the directory /opt/MagellanMDP/data/mdp/dump.

3 Repeat, as necessary, for each datatype.

4 Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

Setting the BDF field delimiter

1 Using the MDP Configuration tool, select **Vector**.

2 Select a Vector datatype: Account or Stats; type the hex code representation for the equivalent character in the data entry box beside **BDF field delimiter**. For example, to set the BDF field delimiter for accounting files, type the hex code in the data entry box below **Account**.

The default is DEL (0x7F) for all datatypes.

Note: Do not use alpha-numeric characters as these can make it difficult to read the output files. Also, do not use the following special characters: "|", "^", "(", ")", " ", ",", ".", or "/".

3 Repeat, as necessary, for each datatype.

4 Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

Setting BDF data compression

BDF records with 3, or more, fields containing null values can be compressed to save disk space and transmission bandwidth. In BDF files, the start of the compression is indicated by ^<count> where <count> is the number of empty fields. For example, ^5 indicates 5 consecutive empty fields.

1 Using the MDP Configuration tool, select **Vector**.

2 Select a Vector datatype: Account or Stats; click a button box beside **BDF output compression**. For example, to compress accounting data, click the button box below **Account**.

A check mark is displayed in the button box.

The default is this option is not selected for any datatype.

3 Repeat, as necessary, for each datatype.

4 Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

Logging BDF converter warnings

1. Using the MDP Configuration tool, select **Vector**.
2. Select a Passport datatype: Account or Stats; click a button box beside **Log BDF converter warnings**. For example, to log BDF converter warnings for accounting data conversion, click the button box below **Account**.

   A check mark is displayed in the button box.

   The default is this option is not selected for any datatype.
3. Repeat, as necessary, for each datatype.
4. Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

Logging File Manager verbose messages

1. Using the MDP Configuration tool, select **Vector**.
2. Click **Run Vector Manager in verbose mode**.

   A check mark is displayed in the button box.

   This option generates Vector File Manager logs using a log level of 4.

   Log levels are described in section “Log levels” (page 207).
3. Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

Assigning a secondary MDP

For more information about MDP hosts, see “Hosts” (page 34).

1. Using the MDP Configuration tool, select **Vector**.
2. Click **Is there a secondary host?**.

   A check mark is displayed in the button box.

   The default is this option is not selected.
3. Type the hostname of the secondary MDP host in the data entry box **Secondary hostname**.
4. Click **Save Vector** to save the configuration change and to restart the Vector File Manager.

Collecting Vector data

The two on-switch components of the Vector data collection system are

- call record data collection application
- performance monitoring data collection application

These applications are part of the Vector Switching System (VSS) software. Call record data collection generates call records, and performance monitoring data collection generates performance records.

The Vector data collection applications collect data during five-minute collection intervals. Although the collection interval is configurable, the Vector data collection system only supports five-minute intervals. At the end of each collection interval, the Vector switch transfers the records to a primary or secondary Management Data Provider (MDP) using the file transfer protocol (FTP).

The MDP host collects Vector records for a one hour period. It then aggregates and correlates the data for each Vector switch fabric.

> ***Note:*** Correlation of point-to-multipoint call records between fabrics only occurs if both records originate as point-to-multipoint. Call records with different origination methods are written to an error file.

The performance monitoring data collection application collects performance usage measurements for the following Vector switch fabric resources:

- fabric board data elements
- network module data elements
- port shared memory priority data, facility common data
- DS1 port data elements
- DS3 port data elements
- OC3 port data elements
- OC12 port data elements
- E1 port data elements
- E3 port data elements

- J2 port data elements.

For a description of the call record data collected, see 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

For a description of the performance data collected, see 241-6001-806 *Preside MDM MDP Data Formats Reference Guide*.

The data transfer process requires two data transfer connections to be established between a Vector switch fabric and an MDP host; one to transfer call record data and the other to transfer performance monitoring data.

For each Vector switch running the data collection software, perform the following configuration tasks using either the Vector Management Interface (VMI):

- specify the IP addresses and names of the primary and secondary MDP hosts
- turn the on-switch data generation function to on
- specify a login userID and password

For a detailed description of VMI, see 241-9501-301 *Vector Operations and Maintenance Using VMI User Guide*.

To generate call records, it is also necessary that you:

- allocate an adequate amount of on-switch memory required for call record generation
- specify what action the Vector switch takes when the allocated memory runs out

Chapter 6
MDP administration

This section describes miscellaneous aspects of the Management Data Provider (MDP).

The following topics are discussed in this section:

- "MDP commands" (page 181)
- "Processing archived raw data" (page 198)
- "Viewing BDF files with Data Viewer" (page 198)
- "Viewing BDF files with the bdfview command" (page 199)
- "Viewing Published Format files" (page 201)

MDP commands

This section describes the syntax of the Management Data Provider (MDP) commands that can be manually executed at the UNIX command line.

This section describes the commands for the following MDP processes:

- "Collecting Passport data" (page 182)
- "Converting raw data files to BDF" (page 186)
- "Converting raw files to PF" (page 188)
- "Identifying new Passport performance metrics" (page 191)
- "Launching the MDP Disk Manager and setting the minimum disk space" (page 192)
- "Aggregating Vector call records (legacy billing)" (page 193)

- "Aggregating Vector performance data" (page 194)
- "Correlating Vector call records (legacy billing)" (page 195)
- "Correlating Vector call records (Egress billing)" (page 196)
- "Correlating Vector performance data" (page 197)

Collecting Passport data

MDP file probers (mdprober) are normally controlled by the MDP File Prober Manager. The File Prober Manager is controlled by the MDM Server Administration tool (SVM).

MDP File Prober Manager

```
/opt/MagellanMDP/bin/mdpfpmgr
[-max_concurrent <m>]
[-loglevel <0-4>]
```

where:

[-max_concurrent <m>]

is the maximum number of concurrent probers allowed. The default number is 2. The maximum limit is 128.

[-loglevel <0-4>]

specifies the level of logs reported. The default level is 3.

There are five levels of log reporting. For more information about log levels, see "Log levels" (page 207).

MDP file prober

CAUTION

Nortel Networks recommends that you use the File Prober Manager to control File Probers. If the File Prober Manager is not used to control File Probers: MDP host and Passport passwords are not secure, connectivity to Passports and MDP disk space availability cannot be confirmed prior to data transfers, the data transfer retry mechanism cannot be used, and data collection cannot be monitored using the Preside Multiservice Data Manager (MDM) Alarm Display.

```
/opt/MagellanMDP/bin/mdprober
-host <Hostname>
-hup <HostUserId Password>
-data <Datatype>
-g <PassportName|PassportGroupName>
-up <PassportUserID Password>
[-nnmap | -idmap]
[-b <Backup Hostname>]
[-bup <UserID Password]
[-files <all|number of files to transfer>]
{-noerase]
[-rollover]
[-timeout <file transfer timeout in seconds>]
[-loglevel <0-4>]
```

where:

-host <Hostname>

is the name of the primary MDP to which the Passport data is sent.

-hup <HostUserID Password>

is the userID and password of a UNIX account on the MDP host to which the data is sent. This is the MDP administrator userID created during MDP installation.

-data <DataType>

is one of the following data types: acc for files that contain accounting information, sta for files that contain statistics information, ala for files that contain alarm information, log for files that contain switch command log information, and scn for files that contain state change notification information.

-g <PassportNodeName|PassportGroupName>

is either the group name of the Passport switches from which the data is collected or the name of the individual Passport switch from which the data is collected. The PassportGroupName exists only in the Host Group Directory Server (HGDS); the data stored on Passport switches does not include a group name.

If a PassportGroupName is provided, spooled data files for all Passport members within the Passport group are collected. The PassportGroupName is a valid group name, as defined in the HGDS.

If a PassportNodeName is provided, only spooled data files from the specified Passport switch are collected.

-up <PassportUserID Password>

is the userID and password of the Passport group or Passport switch. The userID is provisioned on the Passport switch before File Prober can be used.

[-nnmap | idmap]

-nnmap indicates that files transferred from Passport switches include the Passport nodename in the raw data file names.

-idmap indicates that files transferred from Passport switches include the Passport nodeID in the raw data file names.

Note: If you plan to transfer bulk data format (BDF) files to a billing host using shortened BDF file names, do not use the -nnmap option because unique file names cannot be guaranteed.

[-b <Backup Hostname>]

is the name of the backup MDP, used when a connection to the primary MDP fails. Use this optional parameter, only if a backup MDP is installed.

[-bup <UserID Password>]

is the userID and password of a UNIX account on the backup MDP. This is the MDP administrator userID created during MDP installation. This option is only required if the userID and password are different from the userID and password used for the primary MDP.

[-files <all|number of files to transfer>]

is the maximum number of files transferred at any one time from a Passport switch. All indicates that all files found, at the time the File Prober is started, are transferred. Before using this option, determine the required data transfer start times for the File Prober.

Note: Do not schedule transfers to coincide with Time of Day Accounting (TODA) periods on the Passport switch, because these transfers result in starvation of the FTP process and data collection can fail.

[-noerase]

ensures that the File Prober does not remove the Passport spool files after the files have been copied to the MDP. The default is for the File Prober to remove Passport spool files after successful transfer.

CAUTION
Use this option for testing purposes only.

Using the -noerase option does not remove accounting files from the Passport after they are transferred to the MDP. Failure to remove these accounting files by other means can cause duplicated records.

[-rollover]

if this option is specified and the spool file for -data <datatype> is open on the Passport, the File Prober closes the open spool file and opens a new spool file before transferring the closed spool file to the MDP.

[-timeout <file transfer timeout in seconds>]

is the number of seconds the File Prober waits before halting execution when the Passport being probed is not responding. The default is 300 seconds.

[-loglevel <0-4>]

specifies the level of logs reported. The default level is 3.

There are five levels of log reporting. For more information about log levels, see “Log levels” (page 207).

Converting raw data files to BDF

Use the MDP administrator userID to execute the bdfconv command.

```
/opt/MagellanMDP/bin/bdfconv
-i <data_file>
[-rdf <RDFversion>]
[-o <output_file>]
[-d <delimiter>]
[-esc <escape character>]
[-compressed]
[-loglevel n]
[-force]
[-help]
[-splitdir <split_directory>]
[-split <split_method>]
[-dmidname]
[-dmidrecord]
```

where:

-i <data_file>

the only mandatory command line input that specifies the absolute pathname of the input file. The data file name must be a valid raw data file name as described in section “Introduction” (page 23) for each of the MDP supported products.

[-rdf <RDFversion>]

an optional parameter that specifies the version of RDF. For example,

```
-rdf 14
```

[-o <output_file_name>]

an optional parameter that specifies the absolute pathname of the output file. The data file name must be a valid BDF file name as described in section “Introduction” (page 23) for each of the MDP supported products.The default directory is /opt/MagellanMDP/data/mdp/dump/<datatype>.

[-d <delimiter>]

an optional command line parameter that specifies a single character that can be used as field delimiter (for example, a separator) in the BDF output file.

The default field delimiter is the ASCII <DEL> character.

[-esc <escape character>]

an optional character used to define an escape character.

The default escape character is %.

[-compressed]

an optional parameter that specifies that three, or more, consecutive blank, or empty, fields in the BDF output are compressed (replaced by one field that indicates how many fields are empty).

[-loglevel <0|1|2|3|4>]

an optional parameter that specifies the level of BDF conversion logs to be reported. The default level is 3.

[-force]

an optional parameter that forces any database used by the BDF Converter to be parsed again from the source files.

[-help]

an optional parameter that lists the bdfconv command line options.

[-splitdir <split_directory>]

an optional parameter that must be used with the -split option. This option specifies where bdfconv is to write the split BDF records. For more information, see “Bulk data format files” (page 31).

[-split <split_method>]

an optional parameter that must be used with the -splitdir option. This option specifies the method used to extract BDF records for output to an archive directory. For more information, see “Bulk data format files” (page 31).

[-dmidname]

an optional parameter that specifies that the Data Model Identifier (DMId) be specified on the BDF filename.

[-dmidrecord]

an optional command line parameter that specifies that the Data Model Identifier (DMId) and the RDF version be included in the datatype field of the BDF records.

Converting raw files to PF

Use the MDP administrator userID to execute the fpconv and amconv commands.

CAUTION
Using SVM, halt the appropriate File Manager (mdpppmgr or mdpdpnmgr) before you run the PF converter (fpconv or amconv).

Ensure that other instances of the PF converter (fpconv or amconv) are not executing and that the PF converter is not scheduled to execute.

The syntax of the Passport Published Format Converter is

```
/opt/MagellanMDP/bin/fpconv
[-big] [-ebcdic] raw_filename
[output_directory]
[-help | -h] [-loglevel <0-4>]
```

The syntax of the DPN Published Format Converter is

```
/opt/MagellanMDP/bin/amconv
[-big] [-ebcdic] [-x <suffix>] raw_filename
[output_directory]
[-c [customer_id] | -n [nams_id] | -s [service_type]]
[-help | -h]
[-recover] [-loglevel <0-4>]
```

where:

<raw_filename>

is the only mandatory command line input. It is the full pathname of the input file that is to be converted to Published Format.

[-big]

this option specifies that big endian encoding is used for numeric fields. If this flag is not specified, small endian encoding is used.

[-ebcdic]

this option specifies that EBCDIC encoding is used for text fields. If this flag is not specified, ASCII encoding is used.

[-x <suffix>]

this option directs the converter to use the specified output filename suffix.

[output directory]

The directory in which the output files are placed. If no directory is specified, the output files are placed in the current directory. If the converter is invoked by one of the File Managers, the output files are created in /opt/MagellanMDP/data/mdp/dump/accounting.

[-c [customer_id]]

this option directs the converter to create more than one output file.

If a customerID is specified with this option, 2 files are created; one file that contains only those accounting records for the specified customerID and another file that contains the accounting records for all other customerIDs.

If a customerID is not specified with this option, an output file is created for each customerID.

If the -c option is used, you cannot use the -n or -s options.

[-n [nams_id]]

this option directs the converter to create more than one output file.

If a namsID is specified with this option, 2 files are created; one file that contains only those accounting records for the specified namsID and another file that contains the accounting records for all other namsIDs.

If a namsID is not specified with this option, an output file is created for each namsID.

If the -n option is used, you cannot use the -c or -s options.

[-s [service_type]]

this option directs the converter to create more than one output file.

If a service type is specified with this option, 2 files are created; one file that contains only those accounting records for the specified service type and another file that contains the accounting records for all other service types.

If a service type is not specified with this option, an output file is created for each service type.

If the -s option is used, you cannot use the -c or -n options.

[-recover]

This option is only available for published format conversion of DPN accounting files.

When data corruption is encountered in a DPN accounting record, the default behaviour of MDP is to halt processing of the file and store the corrupted record and all other records in an error file. Selecting this option indicates that MDP must attempt to recover any valid records that can be present in the file beyond the data corruption. The error file is still created, but all recovered records are stored in the Published Format output files.

[-help | -h]

an optional parameter that lists command options.

[-loglevel <0-4>]

an optional parameter. This parameter specifies the level of PF conversion logs to be reported. The default level is 3.

Identifying new Passport performance metrics

Use the command **rdfreport** to identify Passport performance metrics before they are introduced into the network. This command obtains a new Passport data model from a specified Passport, creates a schema for each Passport record and compares the new schemas to the current record description files (RDFs) to detect new performance metrics.

New Passport performance metrics are indicated as **New** fields in the **Passport <datatype> RDF Configuration** window, where <datatype> is the datatype selected from the **Passport** window of the Management Data Provider (MDP) Configuration tool. For information about identifying, and using, new performance metrics, see “Customizing BDF records” (page 130).

Note: Ensure that the Data Model Manager (mdpdmm) is running before using this command.

```
/opt/MagellanMDP/bin/rdfreport
-node <Passport IP address>
-login <Passport userID>
-password <Passport password>
-load <Passport loadname>
[-loglevel <loglevel>]
[-help | -h]
```

where:

-node <Passport IP address>

This parameter specifies the IP address of the Passport.

-login <Passport userID>

This parameter specifies the userID used to access the Passport.

-password <Passport password>

This parameter specifies the password associated with the Passport userID.

-load <Passport loadname>

This parameter specifies the loadname of the Passport load (for example, CB03S2C).

[-loglevel <loglevel>]

This optional parameter specifies the level of logs to be reported. The default level is 3.

[-help | -h]

This optional parameter lists the command options.

Launching the MDP Disk Manager and setting the minimum disk space

For more information about the MDP Disk Manager, see “Configuring data file retention” (page 94).

Note: mdpdiskmgr is controlled using the MDM Server Administration tool (SVM). For more information, see 241-6001-310 *Preside MDM Server Reference Guide*.

```
/opt/MagellanMDP/bin/mdpdiskmgr
[-freespace <space>]
[-loglevel <loglevel>]
[-help | -h]
```

where:

[-freespace <space>]

This optional parameter specifies the amount of available disk space to be retained on an MDP host. The default is 100000M.

[-loglevel <loglevel>]

This optional parameter specifies the level of logs to be reported. The default level is 4.

[-help | -h]

This optional parameter lists the command options.

Aggregating Vector call records (legacy billing)

Use the MDP administrator userID to execute the accaggregator command.

```
/opt/MagellanMDP/bin/accaggregator <options>
```

The available options are

-i <input_file_name,...>

Input file names. This option is mutually exclusive with the -f, -s, -d, and -a options.

-f <fabric_id>

Vector switch fabric identifier. This option is mutually exclusive with option -i.

-s <switchID>

Vector switch identifier. This option is mutually exclusive with option -i.

-o <output_file_name>

Output file name; for the default name, see “Aggregated file names” (page 77).

-d <start_time>

Start time of the aggregation period.

-a <aggregation_period>

Aggregation period.

-r <directory>

Directory location where the files to be aggregated reside. The default directory is the merge directory.

-h <help>

Available options.

Aggregating Vector performance data

Use the MDP administrator userID to execute the pmaggregator command.

/opt/MagellanMDP/bin/pmaggregator <options>

The available options are

-i <input file name,...>

Input file names; relative to the -r option. This option is mutually exclusive with the -f, -a, and -d options.

-r <working directory>

Working directory for input and output aggregator files; the default is the merge directory.

-f <fabric id>

Vector switch fabric id. This option is mutually exclusive with option -i.

-a <agginterval>

Aggregation interval; the default 60 minutes (this option must be used with the -d option).

-d <seq_date>

Date and time starting from a given sequence date up to <agginterval> number of minutes later.

-o <output file name>

Name of the aggregator output file (relative to the -r option). For the default name, see “Aggregated file names” (page 77).

-c <counts file name>

Name of the counts file to use for the aggregation period (relative to the -r option).

-g <debug option>

Log of more detailed error messages.

-h <help>

Available options.

Correlating Vector call records (legacy billing)

Use the MDP administrator userID to execute the acccorrelator command.

`/opt/MagellanMDP/bin/acccorrelator <options>`

The available options are

`-i <input file name,...>`

Input file names. This option is mutually exclusive with the -s, -d, and -e options.

`-r <working directory>`

Working directory for input and output correlator files; the default is the merge directory.

`-s <switch id>`

Vector switch identifier. This option is mutually exclusive with option -i.

`-d <start_time>`

Start time of the aggregation period. This option is required with -s and -i options.

`-e <end_time>`

End time of the aggregation period. This option is required with -s and -i options.

`-o <output file name>`

Name of the correlator output file (relative to the -r option). For the default name, see “Correlated file names” (page 77).

`-h <help>`

Available options.

Correlating Vector call records (Egress billing)

Use the MDP administrator userID to execute the acccorrelator command.

```
/opt/MagellanMDP/bin/acccorrelator <options>
```

The available options are:

```
-i <input_file_name input_file_name...>
```

This optional parameter identifies input file names; each file name separated by a space. This list corresponds to the range of times specified by the -t0 and -t1 options.

```
-s <switchID>
```

This optional parameter identifies a Vector switch. This option can be used instead of the -i option to indicate the appropriate switch.

Note: Either the -i option or the -s option must be specified with this command.

```
-t0 <beginTime>
```

This mandatory parameter identifies the start of the time interval for processing. This parameter is to indicate to start this process for call records beginning on the hour, every hour.

```
-t1 <endTime>
```

This mandatory parameter identifies the end of the time interval for processing. This parameter is to indicate to process for call records which end upto one minute before the hour, every hour.

```
-o <output_file_name>
```

This mandatory parameter identifies the name of the file output by this process. For the default name, see “Correlated file names” (page 77).

```
-dir <working directory>
```

This optional parameter identifies the location of the raw, aggregated and correlated files; the default is the merge directory.

```
-f <force>
```

This optional parameter forces various schema databases to be rebuilt.

```
-ignore
```

This optional parameter indicates to the process not to alarm tag errors when the tag exists in the raw schema file but is not recognized by the program..

-h <help>

Available options.

Correlating Vector performance data

Use the MDP administrator userID to execute the pmcorrelator command.

/opt/MagellanMDP/bin/pmcorrelator <options>

The available options are:

-i <input file name,...>

Input file names. This option is mutually exclusive with the -s, -d, and -a options.

-r <working directory>

Working directory for input and output correlator files; the default is the merge directory.

-s <switch id>

Vector switch identifier. This option is mutually exclusive with option -i.

-a <corrinterval>

Correlation interval; the default is 60 minutes (this option must be used with the -d option).

-d <seq_date>

Date and time starting from a given sequence date up to <corrinterval> number of minutes later.

-o <output file name>

Name of the correlator output file (relative to the -r option). For the default name, see “Correlated file names” (page 77).

-h <help>

Available options.

Processing archived raw data

The Management Data Provider (MDP) can process archived raw data.

CAUTION
Use this option for testing purposes only.

Re-processing raw data can generate duplicate records which can be transferred to downstream applications.

1. Stop the file manager (mdpdpnmgr, mdpppmgr, mdpvssmgr) using the MDM SVM.
2. Copy the archived raw data file from a sub-directory of the archive directory /opt/MagellanMDP/data/mdp/archive to the MDP spool directory /opt/MagellanMDP/data/mdp/spool.
3. Restart the file manager (mdpdpnmgr, mdpppmgr, mdpvssmgr) using the the MDM SVM.

Viewing BDF files with Data Viewer

Bulk data format (BDF) files can be viewed online in various forms, including spreadsheet and graphics, using the Preside Multiservice Data Manager (MDM) **Data Viewer**. For more information about the Data Viewer, see 241-6001-031 *Preside MDM Performance Management User Guide*.

Note: Including the record description file (RDF) version in the BDF records enables the Data Viewer application to select the correct RDF for BDF file viewing. To include the RDF version in BDF records, see “Including the DMId and RDF version with BDF records” (page 129).

Viewing BDF files with the bdfview command

Bulk data format (BDF) files can be viewed with the command **bdfview** to ensure that converted BDF files are consistent with the raw data files generated by the switches.

bdfview translates ASCII BDF records to **FieldName Value** pairs and displays the output. bdfview does not support filtering or field selection.

Record description files (RDF) are used to decode the BDF file. bdfview selects the RDF using the first two fields of a BDF data file record. These fields are dataType or switchType.

For Passport BDF files, bdfview attempts to use the RDF identified in the RDF version portion of the dataType field.

- If the RDF version is not specified in the dataType field, bdfview uses the current customized RDF for the dataType.
- If the RDF for the dataType has not been customized, the default RDF is used.

For DPN-100 and Vector BDF files, bdfview attempts to obtain the RDF from the directory /opt/MagellanMDP/cfg/mdp/rdf/<switchType>/<dataType>.

- If the current directory does not contain a compatible RDF, bdfview checks the directory /opt/MagellanMDP/lib/mdp/rdf/<switchType>/<dataType>.
- If this fails, bdfview terminates.

```
/opt/MagellanMDP/bin/bdfview -i <BDF_data_file>
[-d “<delimiter>”]
[-esc “<delimiter>”]
[-h|-help]
[-loglevel <value>]
[-m <MaxRecord>]
[-p]
```

where:

```
-i <BDF_data_file>
```

This mandatory parameter specifies the filename of the input BDF file.

[-d “<delimiter>”]

This optional parameter specifies the field delimiter in a BDF file. Field values in the output are separated by this character (either a single non-integer character or an integer representing the ASCII code for a character). The default is 127, which is the ASCII <*DEL*> character. Use of double-quotes around the delimiter is required to ensure that the delimiter is not mistaken for a UNIX special character.

[-esc “<delimiter>”]

This optional parameter specifies the escape character used in a BDF file.. The default is “%”. Use of double-quotes around the delimiter is required to ensure that the delimiter is not mistaken for a UNIX special character.

[-h|-help]

This optional parameter lists the available options.

[-loglevel <value>]

This optional parameter specifies the level of logs to be reported. The default level is 3.

[-m <MaxRecord>]

This optional parameter specifies the maximum number of records to display.

[-p]

This optional parameter directs the process to use the previous, pre-R10.8, display format for DPN-100 alarms. Use of this option causes the values for fields sourceId and faultCode to be displayed in decimal format, only, and fields expertData and operatorData to be displayed in one continuous hex string.

Viewing Published Format files

Use the MDP administrator userID to execute the pfview command.

```
/opt/MagellanMDP/bin/pfview <options>
```

The available options are

```
-i <accounting data file>
```

Specifies the filename of the Published Format accounting file.

```
[-big]
```

specifies big-endian PF files. If the -big option is not specified, small-endian is assumed.

```
[-d <delimiter>]
```

Specifies the field delimiter for the spreadsheet option.

If this parameter is typed on the command line, then output is presented in a spreadsheet format. The field values in the output are separated by the delimiter characters (a maximum of three). Records are separated by a newline character. The file Acc.rdf or Acc.sch can be used to parse the spreadsheet output. The resulting file can be imported into a spreadsheet for viewing.

```
[-m <max records>]
```

Specifies the maximum number of records to be returned starting from the first record.

```
[-ebcdic]
```

Specifies that the file to be viewed is in EBCDIC format. If EBCDIC is not specified, the default is ASCII.

Note: Flag fields are reported as binary strings.

Chapter 7
MDP logs

This section describes Management Data Provider (MDP) logs.

The following topics are discussed in this section:

- "Log format" (page 203)
- "Log file names" (page 204)
- "Log levels" (page 207)
- "MDP Log Viewer" (page 207)
- "Log messages" (page 218)

Log format

The format of the Management Data Provider (MDP) logs is

```
<datetime>: <severity>: <fault_code>: <nodeID>: <process_name>: <log_msg>
<datetime>: <severity>: <fault_code>: <nodeID>: <process_name>: <log_msg>
<datetime>: <severity>: <fault_code>: <nodeID>: <process_name>: <log_msg>
```

where:

- each field is separated by a colon ":"
- <datetime> is the date and time of the start of the current process operation; in the format YYYYMMDDThhmmss
- <severity> is the severity of the current process operation. This log parameter can include any of the following:

  - — CRITICAL indicates that an operation cannot be performed, and this failure compromises the integrity of the process results. Processing may or may not continue.
  - — ERROR indicates that an operation cannot be performed, but this failure does not compromise the integrity of the process results. Processing continues.
  - — WARNING indicates that an operation has completed without errors, but the integrity of the process results are in doubt.
  - — INFO indicates an information message about the current process operation.
  - — VERBOSE indicates a verbose form of an information message.

- <fault_code> provides a reference to resolutions in section "Log messages" (page 218)
- <nodeID> is the name of the node that provided a raw data file or the name of the MDP host (if applicable)
- <process_name> is the name of the current MDP operation

  The File Prober process name (mdprober) may include the datatype. For example, mdprober_acc.

  The Data Model Manager process name (mdpdmm) may include the UNIX process identifier (PID). For example, mdpdmm_1234.

- <log_msg> is the process indication message

Log file names

This section describes the file name formats for Management Data Provider (MDP) logs. MDP log files are stored in the directory /opt/MagellanMDP/data/mdp/admin.

The table "MDP log files" (page 205) indicates the log file name for each MDP process.

Table 4
MDP log files

Process	Log file
Passport File Manager	MDPPPMgr(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
DPN File Manager	MDPDPNMgr(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
Passport process (data conversion)	MDPPPData_all_(Sun|Mon|Tue|Wed|Thu|Fri|Sat) _YYYYMMDD.log
DPN process (data conversion)	MDPDPNData_all_(Sun|Mon|Tue|Wed|Thu|Fri|Sat) _YYYYMMDD.log
Vector File Manager	MDPVSSMgr(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
File Mover Manager	MDPFMMgr_YYYYMMDD.log
File Mover	MDPMover_<filetype>_YYYYMMDD.log where <filetype> is one of: ACC_PF, PP_ACC_BDF, PP_ALA_BDF, PP_LOG_BDF, PP_SCN_BDF, PP_STA_BDF, PP_OTG_BDF, PP_SRS_BDF, DPN_ACC_BDF, DPN_ALA_BDF, DPN_LOG_BDF, DPN_STA_BDF, DPN_OTG_BDF, VSS_ACC_BDF, VSS_STA_BDF, AUDIT_RPT, AVA_BDF
File Cleanup	MDPClean(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
Disk Manager	MDPDiskMgr(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
Outage Controller	MDPOCtrl(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
Topology Generator	MDPNMTopGen(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_ YYYYMMDD.log
Availability Calculator	MDPAC<YYYYMMDD>.log
Configuration	MDPConfig(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
Flexible Directory Installation	MDPFID(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
File processing audit	MDPAudit(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
File Prober Manager	MDPFPMgr_YYYYMMDD.log
File Prober	/mdprober/<datatype>/mdprober_<Passport_nodename>_ YYYYMMDD.log
Data Model Manager	MDPDMM_YYYYMMDD.log
(Sheet 1 of 2)	

Table 4 (continued)
MDP log files

Process	Log file
RDF Generator	MDPRdfgen_YYYYMMDD.log
Schema Generator	MDPSchemagen_YYYYMMDD.log
Statistics Retrieval System	MDPSRS(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
(Sheet 2 of 2)	

Temporary log files

To support multi-threaded file managers, temporary log files are created for each Passport or DPN raw data input file processed by the Management Data Provider (MDP). These temporary log files are created in the directory /opt/MagellanMDP/data/mdp/admin/tmp.

The file name format for the temporary log files is

```
<switch_type>_<raw_data_file>.log.<co|cc>
```

where:

<switch_type> is pp for Passport or DPN for DPN-100

<raw_date_file> is the name of the raw data file being processed

<co> indicates that the temporary log file is open

<cc> indicates that the temporary log file is closed

Archived log files

Individual Management Data Provider (MDP) logs can be archived using the Log Archival window of the MDP Configuration tool; see “Configuring log archiving” (page 103). The MDP processes that create archived log files are the Passport File Manager, the DPN File Manager, and the Passport File Prober. Archived log files are maintained in custom sub-directories of the archive directory /opt/MagellanMDP/data/mdp/admin/archive.

The file name format for the Passport File Manager archive log file is

```
MDPPPData_(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
```

The file name format for the DPN File Manager archive log file is

```
MDPDPNData_(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
```

The file name format for the Passport File Prober archive log file is

```
mdprober_(Sun|Mon|Tue|Wed|Thu|Fri|Sat)_YYYYMMDD.log
```

Log levels

Log levels assign the type of information recorded for each MDP process.

There are five levels of log reporting

- 0 specifies that critical errors are to be logged.
  Critical errors cause the process to terminate.
- 1 specifies that general errors and critical errors are to be logged.
  General errors indicate that a process operation failed, but this failure did not compromise the integrity of the process. The process continues.
- 2 specifies that warnings, errors, and critical errors are to be logged.
  Warnings indicate that a process operation was performed without errors, but questionable results were produced. This is the default log level.
- 3 specifies that information, warnings, errors, and critical errors are to be logged.
  Information logging includes processing start time and completion time.
- 4 specifies that verbose information, information, warnings, errors, and critical errors are to be logged.
  Verbose information includes information about file operations and statistics.

MDP Log Viewer

You can create a report of Management Data Provider (MDP) log files.

The MDP Log Viewer graphical user interface (GUI) consists of a single window with which you select logs and display log information.

The MDP Log Viewer restricted command line interface (RCLI) displays MDP logs by generating reports to screen or file from the UNIX command line. For more information about the MDP Log Viewer RCLI, see “Generating log reports from the command line” (page 217).

Note: The MDP Log Viewer is not compatible with logs generated before MDP software release R12.4.

This section describes how to use the MDP Log Viewer and describes MDP Log Viewer window components.

- "Opening the MDP Log Viewer window" (page 208)
- "MDP Log Viewer window" (page 209)
- "Using the MDP Log Viewer window" (page 213)
- "Generating log reports from the command line" (page 217)

Opening the MDP Log Viewer window

Launch the Management Data Provider (MDP) Log Viewer using one of the following methods.

The MDP Log Viewer window options are described in section "MDP Log Viewer window" (page 209).

Note: To launch the MDP Log Viewer, your UNIX userID must be either the MDP administrator userID or have MDP user group (mdpgroup) permissions.

Access from the Preside MDM window

1 To launch the MDP Log Viewer from the Preside Multiservice Data Manager (MDM) window, as the MDP administrator, select **Accounting -> MDP Log Display**

The **MDP Log Viewer** window opens.

Access from the UNIX command line

1 To launch the MDP Log Viewer from the UNIX command line, as the MDP administrator, type the following command:

```
/opt/MagellanMDP/bin/mdplv
```

The **MDP Log Viewer** window opens.

MDP Log Viewer window

This section describes the menus and panels of the MDP Log Viewer window.

The following topics are discussed in this section:

- "Pull-down menus" (page 209)
- "Logfile Location" (page 211)
- "Report fields" (page 211)
- "Log report panel" (page 212)
- "Log records" (page 212)

Pull-down menus

The MDP Log Viewer window includes the following pull-down menus, located at the top of the window:

- **File** options
  - **Log directory** - this option opens a dialog box to specify the location of input logs. The default location for MDP logs is the directory /opt/MagellanMDP/data/mdp/admin.
  - **File Prober Log directory** - this option opens a dialog box to specify the location of input File Prober logs. The default location for File Prober logs is the directory /opt/MagellanMDP/data/mdp/admin.
  - **Get Filter** - this option opens a dialog box that lists MDP Log Viewer filters stored in the directory /opt/MagellanMDP/cfg/mdp.

    You can navigate to other MDP directories to find filters stored in other directories using the Get Filter dialog.
  - **Save Filter** - this option opens a dialog box to specify a name for the current log selection criteria and saves the filter to a file.

    The default is to save the filter as /opt/MagellanMDP/cfg/mdp/<filterName>.filter , where <filterName> is the name you specified.

    If you select an existing filterName, the existing filter is over-written with the new selection criteria.

You can also navigate to other MDP directories to store filters in other locations.

Log Viewer filters not stored in directory /opt/MagellanMDP/cfg/mdp are not displayed with the **File->Get Filter** option.

— **Delete Filter** - this option opens a dialog box to specify or select a saved filter for deletion.

The default is to list the filters in /opt/MagellanMDP/cfg/mdp.

You can also navigate to other MDP directories to find filters in other locations.

— **Save Report** - this option opens a dialog box to specify a name for the current report and save the report to a file.

The default is to save the report as $HOME/<reportName>.rpt , where $HOME is your home directory and <reportName> is the name that you specified.

You can navigate to other MDP directories to store reports in other locations using the Save Report dialog.

— **Print Report** - this option prints the current report to the printer destination for environment variable PRINTER.

• **Options** options

Note: The defaults set by these pull-down menu items are specific to the userID.

— **Set log directory as default** - this option sets the current directory as the default log directory.

— **Set File Prober Log directory as default** - this option sets the current File Prober directory as the default File Prober log directory.

• **Report** options

— **Run** - this option executes the Log Viewer reporting process using the current selection and sorting criteria.

- **Help** options
  - — **On Context** - this option is not in operation.
  - — **On Window** - this option displays information about using the MDP Log Viewer.
  - — **About** - this option displays information about the MDP Log Viewer application software.

Logfile Location

The **Logfile Location** panel:

- **MDP log directory** - this information indicates the directory currently used to obtain input log files. This information is changed when you use pull-down menu item **File->Log directory** to change directories.

  Beside this label is the button **set as default**. Clicking this button sets the current directory as the default MDP log directory.

- **File Prober log directory** - this information indicates the directory currently used to obtain input File Prober log files. This information is changed when you use pull-down menu item **File->File Prober Log directory** to change directories.

  Beside this label is the button **set as default**. Clicking this button sets the current directory as the default File Prober log directory.

Report fields

Use the **Report fields** panel to add or remove log fields in the log report panel.

- If a log message field is not currently included in the log report panel, clicking the log field button in the Report fields panel adds the field to the log report panel.
- If a log message field is currently included in the log report panel, clicking the log field button in the Report fields panel removes the field from the log report panel.

The log fields that can be included in the log report panel are

- Time,

- Log Level,
- Fault Code,
- Node Id,
- Process, and
- Message Text

Log records

The MDP Log Viewer window includes information about the log records used by the MDP Log Viewer. The information about the log records is displayed below the **Selection Criteria** and **Report fields** panels.

- **Display counts only** - select this button to prevent the display of log field data. The number of records found as a result of a search are indicated by **Records found**.

  The default is to display log data and to indicate the number of records found.

- **Records found** - is the number of log records found as a result of a search.
- **Maximum number of records to include in report** - use this data entry box to specify the maximum number of records to include in the report.

  If the specified maximum is exceeded, you are prompted to continue or halt processing. If you halt processing, the maximum number of log records is displayed. If you choose to continue processing, the MDP Log Viewer searches for log records until the search criteria is exhausted, all of the input log files are searched, or the specified maximum is once again exceeded.

  The default is to include a maximum of 100 records in a report.

Log report panel

The MDP Log Viewer window includes a panel to display the retrieved logs.

This panel

- displays the specified log fields in tabular format. For information about including and excluding log fields, see “Report fields” (page 211).
- displays the results of the log record search.
- column headings contain the names of log fields.

  Column headings can be used to sort the report. The default is for all fields to be reported in ascending order. If you left mouse click on a column heading, the report is re-sorted in reverse order based on the selected field.

Using the MDP Log Viewer window

1. Launch the **MDP Log Viewer**; see “Opening the MDP Log Viewer window” (page 208).
2. To retrieve a stored log report filter, select pull-down menu item **File->Get Filter**. For more information about File->Get Filter, see “Pull-down menus” (page 209).
3. If the logs required for this report are not located in the directory current default directory, select the logs using the one of the pull-down menu items **File->Log directory** or **File->File Prober Log directory**. For more information about these menu items, see “Pull-down menus” (page 209).

   After you change the current directory, you can set this directory as the default by clicking the **set as default** button beside the directory display box.
4. Using the **Report fields** panel, select log report fields.

   To select a log report field, click the log field button.

   The order that you select log fields is the order that log fields are displayed.
5. Using the **Selection Criteria** panel, specify a starting date and time for your search of logs.

   This is the date and time of the oldest log record to include in the report.

   The default starting date and time is the start of the current year; for example, 20020101T000000.

   You cannot specify a future date.

a. Type the date in the format YYYYMMDDTHHMMSS in the **Starting Date & Time** box.

b. For the current day's logs, type **today**.

c. For a previous day's logs, relative to the current date, type **-n**, where n is an integer.

6 Using the **Selection Criteria** panel, specify an end date and time for your search of logs.

This is the date and time of the latest log record to include in the report.

The default end date and time is the current date and time.

You cannot specify a future date.

a. Type the date in the format YYYYMMDDTHHMMSS in the **Ending Date & Time** box.

b. For the current day's logs, type **today**.

c. For a previous day's logs, relative to the current date, type **-n**, where n is an integer.

7 Using the **Selection Criteria** panel, select the the log levels to include in the report.

The default is to report all log levels.

a. To select a single log level, left-mouse click on the log level in the **Log Level** box.

b. To select multiple log levels, control-left mouse click on each log level in the **Log Level** box.

c. To select a range of log levels, left-mouse click on the first log level and shift-left mouse click on the last log level in the **Log Level** box.

8 Using the **Selection Criteria** panel, select the fault codes to include in the report.

The default is to report all fault codes. This is indicated by .* in the **Fault Code** box.

a. Type any UNIX regular expression to parse fault codes in the **Fault Code** box.

9 Using the **Selection Criteria** panel, select the nodeIDs to include in the report.

The default is to report all nodeIDs. This is indicated by .* in the **Node Id** box.

a. Type any UNIX regular expression to parse nodeIDs in the **Node Id** box.

10 Using the **Selection Criteria** panel, select the the MDP processes to include in the report.

The default is to report all MDP processes.

a. To select a single MDP process, left-mouse click on the MDP process in the **Process** box.

b. To select multiple MDP processes, control-left mouse click on each MDP process in the **Process** box.

c. To select a range of MDP processes, left-mouse click on the first MDP process and shift-left mouse click on the last MDP process in the **Process** box.

11 Using the **Selection Criteria** panel, select the message texts to include in the report.

This is the message text contained in each log. The message text describes an event, the success or failure of the event, and, sometimes, a corrective action.

The default is to report all message texts. This is indicated by .* in the **Message Text** box.

a. Type any UNIX regular expression to parse MDP log message texts in the **Message Text** box.

12 If fields are now included that are not required, remove the fields using the **Report fields** panel. Click on each unrequired field. For more information about the Report fields panel, see “Report fields” (page 211).

13 Optionally, change the **Display counts only** setting. For more information about this setting, see “Log records” (page 212).

14 Optionally, change the **Maximum number of records to include in report** setting. For more information about this setting, see “Log records” (page 212).

15 Select pull-down menu item **Report->Run**.

A dialog box opens with the message

```
Report is being generated.
```

16 When the MDP log search is complete, the report is displayed. For more information, see “Log report panel” (page 212).

A dialog box opens with the message

```
Report has been created.
```

The dialog box contains an Ok button. Click **Ok** to acknowledge report completion.

17 To change the order of the fields displayed

a. press and hold the left mouse button on a column heading

b. move the selected column over another column

c. the selected column is inserted to the left of the covered column

18 To change the size of a column displayed

a. press and hold the left mouse button on a column separator line

b. move the column separator line left or right to shrink or enlarge the column

19 To save the current report to a file, use pull-down menu item **File->Save Report**. For more information about this menu item, see “Pull-down menus” (page 209).

A dialog box opens.

If a filename is not specified and the dialog box closes, you are prompted to confirm that you do not want to save the current report to file.

20 To save the current selection criteria to a filter file, use pull-down menu item **File->Save Filter**. For more information about this menu item, see “Pull-down menus” (page 209).

The following selection criteria is saved:

- selected log input directory
- included report fields
- selection criteria for each included report field
- display record counts, only
- maximum number of records to report in report

A dialog box opens.

If a filename is not specified and the dialog box closes, you are prompted to confirm that you do not want to save the filter.

Generating log reports from the command line

The MDP Log Viewer restricted command line interface (RCLI) displays MDP logs by generating reports to screen or file from the UNIX command line.

Log information can be selected (filtered) and sorted using filters saved by an Log Viewer GUI session. For information about saving Log Viewer filters, see “Using the MDP Log Viewer window” (page 213).

Log reports can be scheduled to run using the UNIX crontab facility. The Log Viewer GUI is normally used to create log report filters and the Log Viewer RCLI is used to schedule periodic generation of log reports.

Command syntax

The syntax of the Log Viewer report generator is

```
/opt/MagellanMDP/bin/mdplv -nogui
( -fn <filter_name> [-o <output_file>] )
[-lf]
[-h|-help]
```

The available options are

-nogui

This option instructs the Log Viewer to generate a log report to the screen or file. The Log Viewer GUI is not opened.

-fn <filter_name>

This mandatory option specifies the filter to use when generating a log report. If the filter is not in the current directory, specify the absolute path and file name.

[-o <output_file>]

If you include this option with the command mdplv -nogui, the generated report is saved to a file and not displayed to the screen. <output_file> specifies the name of the file where the generated report is written. If you do not want to save the file in the current directory, specify the absolute path and file name.

If you want the generated report displayed to screen, do not include the -o <output_file> option.

The default is to generate the report to screen, only.

`[-lf]`

This option directs the command mdplv -nogui to list available filters. Log Viewer filter files in the directory /opt/MagellanMDP/cfg/mdp are listed.

`[-h|-help]`

This option displays information to assist in using the Log Viewer RCLI.

Log messages

This section describes Management Data Provider (MDP) log messages. Identified are the fault code associated with each message, the message text, the MDP process that generated the message and possible corrective actions.

Note: Not all MDP log messages are documented. “MDP log messages” (page 218) contains MDP log messages applicable to some, but not all, MDP processes.

The suggested corrective actions are general recommendations. If you are unable to correct the indicated fault, contact Nortel Networks Customer Support.

Table 5
MDP log messages

Fault code	Message	Generated by: Resolution:
00001	Cannot open input file.	All Ensure that the specified file exists and has the correct permissions.
00005	Cannot open output file.	All Check permissions and disk space.
00010	Cannot open configuration file.	All Ensure that the file exists and has correct permissions. If the file does not exist, consult the NTP for instructions on configuring.
00020	Cannot access directory.	All Ensure that the directory exists and has the correct permissions.

(Sheet 1 of 7)

Table 5 (continued)
MDP log messages

Fault code	Message	Generated by: Resolution:
00025	Error moving/copying file or directory.	All Ensure that the source file and directory exist and have the correct permissions. Ensure that the target directory exists, has write permission and adequate disk space.
00030	File <filename> is not a directory.	All The specified file is a file but it should be a directory. If this is a command line parameter, specify a directory instead of a file.
00035	Cannot close file.	All Ensure that there is sufficient disk space.
00040	Invalid filename.	All The specified filename is invalid.
00045	System call failed.	All MDP made a system call to the OS which failed. Refer to the specific message for details.
00100	Invalid user.	All The userID that attempted to run this program was not the valid user. Log in as the valid user and rerun.
00105	Can't determine the userid of current user.	All Ensure that the current user is the valid user for this program.
00106	Can't determine the userid of the MDP administrator.	All The MDP administrator is determined by the owner of directory /opt/MagellanMDP/cfg/mdp, ensure that this directory is accessible and owned by the MDP administrator.
(Sheet 2 of 7)		

Table 5 (continued)
MDP log messages

Fault code	Message	Generated by: Resolution:
00120	Another instance of this program is already running.	File Managers, Outage Calculator, Outage Controller, SRS Some programs can only have one instance running to preserve file integrity. Stop the first instance of a program before starting another.
00121	Diskmanager is not running.	File Managers The disk manager must be running before the File Managers will start. Configure the disk manager using gmdpconfig. If it is configured but not started, start it using SVM.
00150	Invalid or expired license.	All Contact your Nortel Networks Customer Support to get a new license.
00200	Forced to die due to signal.	All A signal was received. Rerun without changes.
00220	Command line error.	All Use the -help option to determine the correct command line usage.
00300	Configuration error.	All The configuration for this tool is invalid or corrupt. Configure using gmdpconfig.
00320	Module file is corrupt.	Topology Generator Rerun the topology generator.
00325	RDF file is corrupt.	All If this is a user defined RDF, inspect for errors. If this is the default Nortel supplied RDF, contact your Nortel Networks Customer Support.
00400	Invalid group name.	File Prober. Specify a valid group name.
01000	Cannot open schema database <filename>.	BDF Converter Check permissions.
(Sheet 3 of 7)		

Table 5 (continued)
MDP log messages

Fault code	Message	Generated by: Resolution:
01100	Raw file is corrupt.	BDF Converter Contact Nortel Networks Customer Support.
02500	MDM is not installed or is configured incorrectly.	SRS Refer to MDM NTPs for information on resolving the specific problem.
09000	MDP is not installed correctly.	All Re-install MDP.
09010	Out of memory.	All The workstation is out of memory. Stop processing and restart tool. Check engineering specifications.
09100	Process terminated with error.	All The process terminated with an error. Refer to log file for details.
09999	Internal error.	All Contact your Nortel Network Customer Support.
10000	Error occurred.	All This is an informational message only. An error occurred but no action is required.
10001	Cannot access file.	All Check permissions. If the process is attempting to write data, check disk space.
10045	System call failed.	All MDP made a system call to the OS which failed. For details, refer to the message that accompanied this message.
10070	Failed to connect to host.	File Prober Check connectivity to host including userID/password.
10090	FTP failed.	File Prober FTP failed. Retry FTP connection.
(Sheet 4 of 7)		

Table 5 (continued)
MDP log messages

Fault code	Message	Generated by: Resolution:
10100	Failed to connect to switch.	File Prober Check connectivity to switch including userID/password.
10174	Cannot connect to or send alarm to the IMDR.	All Ensure that the IMDR is active on either the local MDP host or on the MDM host host specified in the MDP Surveillance window.
10320	Module file is corrupt.	Outage Calculator Rerun the topology generator.
14000	Raw record is corrupt.	BDF Converter The raw record obtained from the switch is corrupt. Contact Nortel Networks Customer Support.
14100	Database is corrupt.	File Managers, BDF Converter Stop and restart the File Manager. If you are running the BDF Converter, use the -force option.
10500	Conversion failed.	BDF Converter Contact Nortel Network Customer Support.
10550	Summary of the number of error records in a raw file.	BDF Converter Contact Nortel Networks Customer Support.
10700	Duplicate file received from switch.	File managers No action required.
10900	Insufficient disk space.	All Free disk space.
10950	Failed to send trap.	All. Ensure MDP is correctly configured to send traps. Ensure the SNMP host is set up to receive traps.
(Sheet 5 of 7)		

Table 5 (continued)
MDP log messages

Fault code	Message	Generated by: Resolution:
12000	FMIP communication error.	File Prober, SRS There is a problem with the FMIP communication between a Passport and the MDP workstation. If the problem persists, contact Nortel Networks Customer Support.
12500	The specified component does not exist on the specified Passport.	SRS Either the component name is incorrect or that component is not provisioned on the Passport.
13000	System busy.	SRS The Passport was unable to send polled information due to traffic congestion. Increase the polling interval or reduce the number of components polled.
19011	Cron job error.	MDP Config Ensure that the MDP administrator is able to create/delete a cron job.
19098	System call error.	MDP Config MDP made a failed system call to the OS. See specific message for details.
19099	Internal Error	MDP Config An internal error has occurred. Contact Nortel Network Customer Support.
19999	Internal error.	All An internal error has occurred. Contact Nortel Network Customer Support.
20000	Various warning messages.	All Information warning message. No action required.
21000	Unknown attribute.	BDF Converter There was an unknown attribute in the raw file.
(Sheet 6 of 7)		

Table 5 (continued)
MDP log messages

Fault code	Message	Generated by: Resolution:
21020	Corrupt records found.	PF Converter. Some corrupt records were found and saved to file. Contact Nortel Network Customer Support.
22000	Current configuration does not process all file types.	File Managers If you do not wish to process the file type specify, you can ignore this message.
30000	Various Info Messages	All Informational message. No action required.
30001	Started processing file.	File Managers MDP has started processing the raw file.
30002	FINISHED processing file successfully.	File Managers MDP has successfully completed processing the raw file.
30010	Finished process file, errors occurred.	File Managers This message indicates the number of errors found in the raw file.
30020	Processed records, unsupported records, and error records.	File Managers This message indicates the number of: records, unsupported records, and error records found in a file.
40000	verbose messages	All Verbose informational messages. No action required.
(Sheet 7 of 7)		

Chapter 8
MDP alarms and/or traps

This section describes Management Data Provider (MDP) alarm and/or trap generation.

This section includes the following topics:

- "Overview" (page 225)
- "MDP events, and alarms and/or traps" (page 226)
- "Retransmission of alarms and/or traps" (page 228)

Overview

The purpose of Management Data Provider (MDP) alarm and/or trap generation is to alert an MDP administrator of significant events occurring on MDP hosts.

- MDP alarm and/or trap generation does not support any SET or GET requests from an SNMP Manager.
- The MDP Trap Generator does not determine whether an SNMP Manager has received a alarm and/or trap; it only indicates success in sending a alarm and/or trap.
- MDP alarms and/or traps are not generated for the Topology Generator or Report Generator.
- Each significant event class on an MDP host has a unique alarm and/or trap. Specific event information is supplied in the alarm and/or trap message. See "Mapping between events and alarms and/or traps" (page 226).

- The name of the user allowed to run MDP processes is supplied in the alarm and/or trap generation configuration file.
- MDP alarm and/or trap generation is optional. For information on how to configure it, see “Configuring MDP surveillance” (page 105).

MDP events, and alarms and/or traps

MDP alarms and/or SNMP traps are generated when a significant event has occurred on an MDP host. Each significant event can be correlated to a unique alarm and/or trap type. “Mapping between events and alarms and/or traps” (page 226) shows the mapping between MDP alarms and/or traps and significant events.

Table 6
Mapping between events and alarms and/or traps

Significant events	Alarm/trap type	Suggested severity	MDP process
Starting of MDP process	startTrap	Normal	gmdpconfig mdprober mdpppmgr mdpdpnmgr mdpfpmgr mdpfmmgr
Stopping of MDP process	stopTrap	Normal	gmdpconfig mdprober mdpppmgr mdpdpnmgr mdpfpmgr mdpfmmgr
MDP has changed due to a migration.	migNoteTrap	Normal	mdpvssmgr
Failure to clean up any directory	errCleanupTrap	Minor	mdpclean
Error records were found during conversion of raw data file	errRecordTrap	Minor	mdpdpnmgr mdpppmgr mdpvssmgr
Sending files to backup	sendBackupTrap	Minor	mdprober
Invalid user	errUserTrap	Major	mdprober
(Sheet 1 of 3)			

Table 6 (continued)
Mapping between events and alarms and/or traps

Significant events	Alarm/trap type	Suggested severity	MDP process
Failure to transfer file (using X.25,IPCor FTP)	errTransferTrap	Major	mdpmover mdpcol mdprober
Problems were encountered while determining MDP disk usage.	errDiskTrap	Major	mdpdiskmgr
MDP workstation has used 90% of its allowable disk space	errNearFullTrap	Major	mdpdiskmgr
No good records were generated by a convertor from a raw data file	errFileTrap	Major	mdpdpnmgr mdpppmgr mdpvssmgr
Detection of duplicate raw data file	errDupTrap	Major	mdpdpnmgr
Secondary MDP receiving files for primary MDP	receiveFileTrap	Major	mdpvssmgr
The availability calculator has encountered problems.	errAvailTrap	Major	mdpavcalc
The outage controller has encountered problems.	errOtgTrap	Major	mdpoctrl
Cannot access log file	errLogTrap	Critical	All MDP process except mdpcol
Problems were encountered while verifying an MDP license.	errLicenseTrap	Critical	mdpdpnmgr mdpppmgr mdpvssmgr mdpavcalc
Cannot access configuration file	errCfgTrap	Critical	All MDP processes
Configured disk space threshold reached on MDP workstation	errDiskFullTrap	Critical	mdpdiskmgr
Directory permission error	errDirTrap	Critical	mdpdpnmgr mdpppmgr mdpvssmgr mdpmover
(Sheet 2 of 3)			

Table 6 (continued)
Mapping between events and alarms and/or traps

Significant events	Alarm/trap type	Suggested severity	MDP process
Creating database error	errDbTrap	Critical	mdpdpnmgr mdpppmgr mdpvssmgr
Failure to connect to host	errConnectTrap	Critical	mdpmover mdprober
Failure to access HGDS	errHGDSTrap	Critical	mdprober
Failure to create Publish Format Hourly file	errPfTrap	Critical	mdpmover
Problem executing converter process	errConvTrap	Critical	mdpdpnmgr mdpppmgr mdpvssmgr
Problems found with correlated file	errCorrTrap	Critical	mdpvssmgr
Problems found in aggregated file	errAggTrap	Critical	mdpvssmgr
Problems encountered with Data Model Manager	errDmmTrap	Critical	mdpdmm
(Sheet 3 of 3)			

Retransmission of alarms and/or traps

Certain events cause a Management Data Provider (MDP) process to send a alarm and/or trap and terminate. These alarm and/or traps are

- errLogTrap
- errCfgTrap
- errDirTrap
- errDbTrap (only for DPN and Passport)

The MDM Server Administration tool (SVM) attempts to restart terminated processes. The cycle of sending a alarm and/or trap followed by process termination is repeated until the problem is resolved.

When the configured threshold for maximum disk space capacity of an MDP host is approached, the following alarms and/or traps are generated:

- errDiskFullTrap

- errNearFullTrap

The errDiskFullTrap and errNearFullTrap alarms and/or traps are resent every 15 minutes.

Chapter 9
Value-added data applications

This section describes the Management Data Provider (MDP) value-added data applications.

Outage calculators use alarms and state change notifications to determine network service interruptions for DPN-100 and Passport switch networks. The following sections describe the outage calculation application:

- "Outage calculation overview" (page 232)
- "DPN outage calculation" (page 233)
- "Passport outage calculation" (page 235)
- "Outage calculation processes" (page 241)
- "Outage calculation file names" (page 251)

The availability calculator uses data from the outage calculators to analyse and report network availability. The following sections describe the availability calculation application:

- "Availability calculation" (page 253)
- "Availability report generation" (page 264)

Note: MDP value-added processes, such as the Outage and Availability Calculators, are unable to correlate Passport nodeIDs with Passport nodenames. Ensure that the MDP generates raw data filenames with nodeIDs or nodenames in the file name format, but not raw data filenames with nodeIDs and raw data filenames with nodenames. If the MDP is generating raw data filenames with one format (eg. nodeIDs) and

you need to generate raw data filenames from the same Passport using the alternate file name format (eg. nodenames), complete all value-added processing before retrieving Passport raw data files with the new filename format. For more information about Passport raw data file names, see “Raw data” (page 52).

Outage calculation overview

Switch outage calculation uses DPN alarm data, or Passport alarm and state change notification (SCN) data, collected and converted to bulk data format (BDF) by an MDP host, as input. By filtering and analyzing alarms, the outage calculators determine which components have experienced service interruptions, calculate the outages, and output the results to a BDF output file on the primary MDP host.

Outage files are produced for each node for each day that an outage occurs.

The outage period extends from the time a network component goes out of service to the time the component resumes service.

Outage calculation requires all the alarm files, and Passport SCNs, for a particular node; therefore, the alarm files must be available to either the primary or secondary MDP for that node.

A DPN or Passport network can only spool data to a maximum of two MDPs. For larger networks, these networks can be subdivided into separate regions for each pair of MDP hosts.

Indication of which MDP is primary and which is secondary is irrelevant to the network, as long as the network data files arrive on one of the two MDP hosts. The relevancy of which MDP host is the primary and which is the secondary is of concern only to the outage calculation process. For more information, see:

- “Hosts” (page 34) for an explanation of primary and backup MDPs.
- “Configuring the Outage Controller” (page 115) for a description of the configuration process.

DPN outage calculation

The basic approach to calculate outages is to simply match SET and CLEAR alarms, sorted chronologically. In a network, a SET alarm is generated at the beginning of a service interruption and a CLEAR alarm is produced when the component returns to a normal operating state. By taking the starting time of the outage from the SET alarm and the ending time of the outage from the CLEAR alarm, we can calculate the duration of the outage.

Alarms are not always generated as pairs of SET and CLEAR alarms. It is possible to receive a SET alarm with no corresponding CLEAR alarm, or a CLEAR alarm with no corresponding SET alarm, or to have multiple SET alarms for a CLEAR alarm. The strategy for handling these conditions is outlined as follows:

- Unmatched SET/CLEAR alarms are written to the file /opt/MagellanMDP/data/mdp/oc/dpn/unmatched/<namsID>.db (where <namsID> is the namsID of the switch that generated the alarm). If a subsequent invocation of the DPN Outage Calculator includes a mate to a unmatched SET/CLEAR alarm, these matched alarms can be used for outage calculation.
- The starting time of an outage is always taken from the first SET alarm. Intervening SET alarms received before the CLEAR alarm are ignored.

To determine the outages, the outage calculation process must first determine which alarms indicate a network component failure. The DPN network components for which outage calculation is possible are

- an access module (AM)
- a resource module (RM)
- a processing element (PE)
- a link
- a trunk
- a port

Types of DPN outages

There are four catagories of outages calculated by DPN Outage Calculator:

- "Component outages" (page 234)
- "Possible component outages" (page 234)
- "Combined outages" (page 234)
- "Indeterminate outages" (page 234)

Component outages

A component outage is calculated if any of the following DPN components goes out of service: access modules (AM) or resource modules (RM), processing elements (PEs), links, or trunks.

Possible component outages

Some alarms do not necessarily indicate outages. They indicate the possibilities of component failures, only. In this case, possible component outages are calculated for those alarms. Possible outages are only calculated for modules.

Combined outages

Combined outages are those outages propagated from a failed network component to its subcomponents. For example, if a module goes down, all the PEs that belong to that module are included in the outage report. Similarly, if a PE goes down, all the ports that belong to that module are included in the outage report. A current network topology is needed to calculate the combined outages. Combined outages exist for PEs and ports.

Indeterminate outages

Indeterminate outages are outages that have not yet terminated. They are expected to terminate during a later sampling period. These outages are indicated by values of zero in their duration and endDateTime fields.

Passport outage calculation

The outage period for a component extends from the time the component is out of service to the time the component resumes service. The philosophy to calculate these outages varies significantly between DPN and Passport networks.

In a DPN network, outage calculation is based upon the idea of SET and CLEAR alarms to indicate the beginning and end of an interruption. No concept of OSI state information exists for a component. Instead, specific alarms are used to determine network component failures.

In a Passport network, outage calculation is based upon OSI state information obtained from component alarm and SCN records. A component is always considered in-service until an alarm or SCN with an OSI state indicating otherwise is received. Receipt of an alarm or SCN indicating an out-of-service condition is considered the beginning of the service interruption. Depending upon the component and the details surrounding the outage, the beginning of an interruption can be marked by either a Set, Clear, or Message alarm, or an SCN record. The end of the interruption is indicated by a change in OSI state from out-of-service to in-service operation. The end of interruption can also be indicated by either a Set, Clear, or Message alarm, or an SCN record. Exceptions to this rule are introduced by specific network component alarm records which indirectly influence the OSI states of one or more components to be in-service or out-of-service.

The following subsections include information important to the calculation of Passport outages:

- "Parsing Passport alarms and SCNs for analysis" (page 235)
- "Outage calculation approach" (page 236)
- "Outage calculation risks and limitations" (page 238)

Parsing Passport alarms and SCNs for analysis

Passport alarms can be categorized as being either a Message, Set, or Clear (mono or hierarchial) status alarm. This status field is equivalent to the DPN-100 Alarm Type field. It is currently used by Preside Multiservice Data Manager (MDM) to add (on receiving a Set alarm) and delete (on receiving a Clear alarm) alarms from the alarm display. For Passport outage calculation,

however, simply relying on matching Set and Clear alarms is not sufficient to calculate the outages required. Passport alarms are normally only generated for components that are the source of the problem, not for components that are impacted by the failure. The SCNs are generated to report the impact of a component failure.

All alarm and SCNs must be processed for outage calculation analysis. This requires that alarms and SCNs are expected to have reliable component OSI state information.

Extending the analysis to all alarms and SCNs increases the reliability of the outage calculator. If the alarms parsed in the outage calculation have reliable component OSI state information, the analysis can potentially recover from component failures that lead to loss of alarms or SCNs; this enables computation of at least partial outages.

Outage calculation approach

The basic approach to calculating component outages is to analyze the OSI state changes indicated in the alarms and SCNs, sorted chronologically. In a network, an alarm or SCN indicating an OSI state that is out-of-service is generated at the beginning of a service interruption. At the end of an interruption, an alarm or SCN indicating an OSI state of in-service is generated. By taking the start time of the outage from the record marked begin and the end time of the outage from the record marked end, the duration of the outage can be calculated.

For every SCN and alarm parsed, the raw state of the component is deduced on the basis of the OSI state attributes of the SCN or alarm. “Initial mapping of OSI state to rawState” (page 236) shows the mapping from OSI state to raw state.

Table 7
Initial mapping of OSI state to rawState

OSI operational state	OSI administrative state	rawState value
disabled	locked	outOfService
enabled	locked	outOfService

Table 7
Initial mapping of OSI state to rawState

OSI operational state	OSI administrative state	rawState value
enabled	shutting down	inService
disabled	shutting down	outOfService
disabled	unlocked	outOfService
enabled	unlocked	inService

The alarms or SCNs of each component, along with their associated raw states, are sorted chronologically. In principle, outage calculation is simply the period of time a component is out-of-service. Applying this to the sorted raw states for the required Backbone and Topology components, the outage is the time period of the first outOfService raw state alarm or SCN and the following first inService raw state alarm or SCN.

Exceptions to this rule exist. Out-of-service and in-service raw states are not always generated as pairs for a particular component. It is possible to receive an out-of-service raw state record with no corresponding in-service raw state record, or an in-service raw state record with no corresponding out-of-service raw state record, or have multiple out-of-service raw state records for an in-service raw state record. The strategy for handling these conditions is outlined as follows:

- Unmatched out-of-service raw state records are written to the file /opt/MagellanMDP/data/mdp/oc/pp/unmatched/ <nodeID|nodename>.db (where <nodeID|nodename> is the nodeID or nodename of the Passport switch). If a subsequent invocation of the Passport Outage Calculator includes a mate to a unmatched alarm, these matched alarms can be used for outage calculation.
- Unmatched in-service raw state records are ignored.
- The start time of an outage is always taken from the first out-of-service SCN. Intervening out-of-service SCNs received before the in-service SCN are ignored.

Outage calculation risks and limitations

Outages cannot be calculated for the following conditions:

- Power failure to the module. Presently, no method exists to determine the duration of a power failure to a module. To reduce the risk of such an outage, uninterrupted power supplies are recommended for the Passport configuration.
- Single CP module failure. As with power failure, no method exists to determine the outage duration. To reduce the risk of such an outage, a redundant CP architecture is recommended for the Passport configuration.
- Double CP Fault module failure. No method exists to determine this outage duration. This type of outage is of low probability.
- Active CP switchover. Depending upon the Passport software release and the services offered, a CP switchover can cause a module outage.
- Module reboot. The duration of the reboot can be available. If there are no logs to indicate the start of the outage, this outage is ignored.

  Note: Single CP module failure, active CP switchover, and module reboot outages can be calculated for Passports using a software release of 5.1, or later.

Outages can be unrepresentative or undetermined for the following conditions:

- Passports perform log buffering before spooling to disk. If the active CP reboots or crashes, the logs in the buffer are lost. Even matching component OSI state logs in this buffer can be lost. This can skew post outage analysis results (for example, availability analysis).
- If alarms or SCNs are missing from the spooled data, partial outages for a component can indicate a longer outage then what actually occurred. This occurs if two outages occur back to back on the same component, but the record indicating the end of the first interruption is lost. The outage calculated is from the beginning of the first interruption to the end of the second interruption.

The Passport components for which outage calculation is possible are

- Backbone components (those components which comprise the hardware and logical suppport for topology components):
  - — module
  - — control processor (CP) or functional processor (FP) card (CARD)
  - — logical processor (LP)
  - — CP switchover
- Topology components (those components which connect the Passport to the network):
  - — trunk (TRUNK)
  - — DPN gateway (DPNGATE) - Passport 6000/7000 switches, only

Note: Outages for modules and CP switchover durations can only be calculated for Passports using a software release of 5.1, or later. For Passports using a pre-5.1 software release, CP switchover counts, only, can be calculated.

Types of Passport outages

There are five catagories of outages calculated by the Passport Outage Calculator mdpppoc:

- "Component outages" (page 239)
- "Partial outages" (page 240)
- "Indeterminate outages" (page 240)
- "CP switchover outages" (page 240)
- "Software migration outage" (page 240)

Component outages

A component outage is an outage that represents a components true out-of-service state duration. If all alarms and SCNs are collected and processed sequentially, component outages are accurate.

Partial outages

A partial outage is an outage that represents only a portion of the actual outage. The alarms or SCNs that indicate the exact beginning or end of the interruption are missing. The outage is computed from other alarms or SCNs surrounding the outage. There can be partial outages for both backbone and topology components.

Indeterminate outages

An indeterminate outage is an outage for which an alarm SET has occurred with no associated CLEAR currently available. This situation is indicated by an outage record whose duration and endDateTime fields have a value of zero.

CP switchover outages

The duration of CP switchovers can be calculated for dual CP Passport switches using Passport release 5.1 software loads. The outage duration indicates the time from active CP failure to standby CP activation.

For pre-5.1 Passport software releases, CP switchover outages are indications of a CP switchover or Module reboot. The actual duration of the outage cannot be determined. This is indicated by an outage record whose duration and endDateTimefields have values of zero.

Software migration outage

The software migration outage defines an outage for spared FPs if one FP is removed from service to load new software ,and provisioning data, while the other FP provides service.

A software migration outage is calculated for Passport 15000 modules, only. The module software migration outage extends from the time that the service shelf went out-of-service to the time that the migration shelf resumed service.

By default, software migration outages are not reported by the Passport Outage Calculator.

Alarm exceptions file

The Passport Outage Calculator mdpppoc uses the file /opt/MagellanMDP/lib/mdp/cfg/pp_otg.exp to ignore specified alarms.

- Alarm ntpIndex 7012 0102 indicates that the CP startup sequence has begun. This alarm does not include the CP's last in-service time stamp and prevents the outage duration from being calculated. Ignoring this alarm allows the outage calculator to report that the module has been rebooted, if not the actual out-of-service duration.
- Alarm ntpIndex 0000 0000 indicates hierarchical alarms for a LogicalProcessor. The hierarchical alarm is treated as a normal in-service alarm for the indicated LP. It is used in the calculation of LP component outages.
- Alarm ntpIndex 7012 0203 indicates a module outage. This alarm is kept in the exceptions file as it needs special treatment to calculate module/CP switchover outages.
- The following line is included in the alarm exceptions file:

```
70120203:LogicalProcessor:CreateOutage:UseRecord:0:0:
MigrationOutage
```

This file entry prevents reporting of software migration outages for Passport 7000/15000 switches. If you want software migration outages reported in outage reports, you must change the above line to a comment by adding an octothorpe (#) to the beginning of the line. Do not alter this line in any other way.

Outage calculation processes

The software processes that perform switch outage calculation are described in the following sections:

- "Process overview" (page 242)
- "MDP outage controller" (page 243)
- "MDP topology generator" (page 244)
- "Outage calculators" (page 246)

Process overview

The DPN File Manager, on both the primary and secondary MDPs, periodically checks for the arrival of alarm data files in the spool directory. The Passport File Manager, on both the primary and secondary MDPs, periodically checks for the arrival of alarm and SCN data files in the spool directory. The File Managers then convert these alarm, and SCN, files to BDF format and deposits them in the directory /opt/MagellanMDP/data/mdp/oc/dpn/primary of its respective MDP.

The Outage Controller mdpoctrl process is started every day on the primary MDP, at a user configurable time, to perform the tasks of outage calculation. These tasks include

- moving alarm files from the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/primary and the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/secondary (which is actually /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/primary on the secondary MDP) to the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process
- generating a list of nodes to process from the data files in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process
- for DPN-100, starting the Topology Generator mdpnmtopgen to get network topology information from the Preside Multiservice Data Manager (MDM) Network Model
- for DPN-100, starting the DPN Outage Calculator for each DPN node found within the files of the directory /opt/MagellanMDP/data/mdp/oc/dpn/process. The DPN Outage Calculator reads the alarm files in the directory /opt/MagellanMDP/data/mdp/oc/dpn/process and outputs outages to a BDF file in the directory /opt/MagellanMDP/data/mdp/oc/dpn/outage, and optionally writes the output to the dump/outage directory.
- for Passport, starting the Passport Outage Calculator for each Passport node indicated by the presence of alarm and SCN files in directory /opt/MagellanMDP/data/mdp/oc/pp/process. The Passport Outage Calculator reads the alarm files in the directory /opt/MagellanMDP/data/mdp/oc/pp/process and outputs outages to a BDF file in the directory /opt/MagellanMDP/data/mdp/oc/pp/outage, and optionally writes the output to the directory /opt/MagellanMDP/data/mdp/dump/outage.

The File Mover process periodically checks for the arrival of files in the dump directory. If files are found, the File Mover transfers these files to a network engineering host for analysis.

The BDF outage files in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/outage can be used by other MDP value-added data (VAD) applications (for example, availability analysis).

MDP outage controller

The Management Data Provider (MDP) Outage Controller mdpoctrl is responsible for administering the various outage calculation tasks. The Outage Controller process performs the following tasks in the sequence indicated:

1 Open a daily log file in the admin directory to record items such as events and errors.

2 Move alarm files, and SCN files for Passport, in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/primary to the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process.

3 Move alarm files, and SCN files for Passport, in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/secondary to the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process.

4 For DPN-100, generate a DPN namsID list from the contents of the data files in the directory /opt/MagellanMDP/data/mdp/oc/dpn/process.

For Passport, generate a list of Passport nodeIDs, and Passport nodenames, from the names of files in the directory /opt/MagellanMDP/data/mdp/oc/pp/process.

5 For DPN-100, start the MDP Topology Generator mdpnmtopgen to retrieve network topology information from the Preside Multiservice Data Manager (MDM) Network Model.

6 Start the appropriate outage calculator (mdpdpnoc for DPN-100 or mdpppoc for Passport) separately for each node identified in Step 4. When the outage calculator has completed outage calculation for all nodes in the node list, the input BDF files are removed from the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process . If errors occurred

during outage calculation, the Outage Controller renames the erroneous BDF data files in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process with the prefix err.

7 Copy the outage files to the directory /opt/MagellanMDP/data/mdp/dump/outage. This task happens only if you previously chose to transfer outage files to other hosts. See “Configuring the Outage Controller” (page 115).

8 Copy outage files to the directory /opt/MagellanMDP/data/mdp/backup/outage. This task happens only if you previously chose to archive outage files. See “Configuring outage calculation” on page 99.

The MDP Outage Controller is a run-to-completion process that is started from a crontab once each day. The crontab entry is created using the MDP Configuration tool when outage calculation is enabled. Configure this process to run on the primary MDP host, only.

Command syntax

The syntax of the MDP Outage Controller command is

```
mdpoctrl [-help]
```

MDP topology generator

The Management Data Provider (MDP) Topology Generator mdpnmtopgen interrogates the Preside Multiservice Data Manager (MDM) Network Model Server to identify DPN network modules and the hardware components that comprise those modules.

The component data extracted from the MDM Network Model for outage calculation purposes includes: PM, PE, PI, and PO.

The MDP Topology Generator creates one description file per DPN module. Each module description file contains one record for each component. Each record contains a component name field.

The field delimiter is the colon (:) character and the record delimiter is the linefeed character. For example:

```
:PE 3:
:PE 3 PI 3:
:PE 3 PI 3 PO 1:
:PE 3 PI 3 PO 2:
```

The MDP Outage Controller is used to configure the MDP Topology Generator to start daily, prior to the execution of the outage calculators. See “Configuring the Outage Controller” (page 115). You can also execute the MDP Topology Generator manually, or from the crontab, on a less frequent basis, depending on the volatility of the network configuration.

Prior to running the topology generator, ensure that the Network Model is up-to-date with respect to the state of the network. This task includes removing all obsolete modules from the Network Model.

Command syntax

The syntax of the MDP Topology Generator command is

```
/opt/MagellanMDP/bin/mdpnmtopgen
-s <switch_type>
[ -n <namsID/nodeID> ]
[ -d <directory > ]
[ -m <network model host> ]
[ -h|-help ]
[ -l loglevel <0-4> ]
```

The available options are

[-s <switch_type>]

specifies the switch type; use `dpn`.

[-n <namsID>]

specifies the NAMS identifier for a DPN module. The default is all modules of the specified switch type.

[-d <directory>]

specifies the directory where the module description files are written. The default is /opt/MagellanMDP/data/mdp/oc/model.

[-m <network model host>]

specifies the MDM host where the network model server is running. The default is the localhost.

[-h|-help]

This option requests command usage information.

[-loglevel <0-4>]

The level of logs to be reported. The default level is 3.

All critical, error, warning, and information messages are displayed to your screen (as well as to the log file). Verbose information messages are written to the log file, only.

There are five levels of log reporting. For more information about log levels, see “Log levels” (page 207).

Outage calculators

The switch outage calculators are responsible for computing the outages from the available DPN alarms, or Passport alarms and scns, for each switch node.

The following tasks are performed by the switch outage calculators:

- The outage calculators are separately licensed features within the MDP package. The outage calculators search the file /etc/opt/Magellan/LIClicenses.cfg for licensing information on invocation. If a valid license exists the outage calculator continues to run otherwise, a log is generated indicating the reason for the refusal.
- Inputs all the alarm files, and SCN files for Passport, in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process for each node in the node list; optionally input the module description file.
- For DPN outage, the following outages are calculated: modules, PEs, links/trunks, possible outages for modules, and combined outages for PEs and ports.

  For Passport outage, the following outages are calculated: CP switchovers, modules, card, logical processor, trunk, DPN gateway, partial outages for backbone (cards and logical processors) and gateway components (trunks and DPN gateways). For Passport 15000 switches, software migration outages can also be calculated.

- Outputs the calculated outages, in BDF format, for each node in the node list, to the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/outage for that sampling period. If no outages exist for the sampling period requested, an output BDF file is not generated.
- Dumps corrupted records to the error file in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/outage.

- Writes unmatched alarms to the unmatched alarm file (<namsID>.db for DPN and <nodeID|nodename>.db for Passport) in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/unmatched.
- Renames unprocessable alarm files (and SCN files for Passport) in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process to the file err.<input_file_name>.
- If the calculation of combined outages is specified, but the module description file is not present, DPN outage calculation still proceeds. The Outage Calculator logs the absence of the module description file.

The outage calculators are run-to-completion processes that are started by the MDP Outage Controller or executed manually.

Command syntax

The syntax of the Outage Calculator command is

```
/opt/MagellanMDP/bin/mdp<dpn|pp>oc <options>
-nid <namsID|nodeID|nodename> -u <unmatched_directory>
[-s <start date>] (Format: MMDDhhmm)
[-e <end date>]   (Format: MMDDhhmm)
[-i <input directory>]
[-o <output directory>]
[-d <output delimiter character>]
[-cfg <config file>]
[-t|min <threshold value>]
[-max <threshold value>]
[-k <days kept value>]
[-force]
[-init]
[-dispcfg]
[-help|-h]
```

The available options are

```
-u <unmatched_directory>
```

This parameter is mandatory and specifies the directory where unmatched alarms can be found. The Outage Controller always invokes the outage calculators with this option selected.

There is one file for each nodeID type. If the -init parameter is specified, any existing unmatched alarms file is replaced with a new file.

[-nid <namsID|nodeID|nodename>]

This parameter provides the namsID of the DPN-100, the nodeID or nodename of the Passport, that collects the outage data. The outage calculators process all the alarm files in the directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process for the specified node.

[-s <start_date>]

This option identifies the beginning of the time period for which outage calculation is to be processed. If no end date is specified, outage records for all dates greater than or equal to the start date are processed.

For DPN, start dates are specified in yymmdd (year, month, day) or yyyymmdd (year, month, day) format. See “Data collection” (page 63) for century determination information.

For Passport, start dates are specified in MMDDhhmm (month, day, hours, and minutes) format.

[-e <end_date>]

This option identifies the end of the time period for which outage calculation is to be processed. If no start date is specified, outage records for all dates less than or equal to the end date are processed.

For DPN, end dates are specified in yymmdd (year, month, day) or yyyymmdd (year, month, day) format. See “Data collection” (page 63) for century determination information.

For Passport, end dates are specified in MMDDhhmm (month, day, hours, and minutes) format.

[-i <input_directory>]

This option specifies the input directory that contains the BDF alarm, and SCN for Passport, files. The default input directory is /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/process.

[-o <output_directory>]

This option specifies the output directory. The default output directory is /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/outage.

[-m <network_model_directory>]

For DPN only, this option specifies the directory where the network module description files can be found. The default directory is /opt/MagellanMDP/data/mdp/oc/model.

[-cfg <configuration_file>]

This option identifies the configuration file of the outage calculator.

For DPN, the default configuration file is /opt/MagellanMDP/cfg/mdp/MDPDPNOC.cfg.

For Passport, the default configuration file is /opt/MagellanMDP/cfg/mdp/MDPPPOC.cfg.

If the default configuration file is not located, the default values of the outage calculator parameters are used.

[-min <threshold> | -t <threshold>]

Outages that exceed this threshold are included in outage calculations.

This parameter specifies this threshold in units of seconds. Maximum is 365 days. Default is 0 seconds.

Use of this parameter on the command line overrides the setting recorded in the outage calculator configuration file.

Indetereminate outages are always generated.

[-max <threshold>]

Outages with durations less than this threshold are included in outage calculations.

This parameter specifies this threshold in units of seconds. Maximum is 365 days. Default is 7 days (604800 seconds).

Use of this parameter on the command line overrides the setting recorded in the outage calculator configuration file.

Indeterminate outages are always generated.

[-sk <days_set_kept>]

This option applies to DPN only. This option specifies the number of days the unmatched SET alarms are kept in the unmatched alarm files. The default value is 100 days.

Use of this parameter on the command line overrides the setting recorded in the DPN Outage Calculator configuration file.

[-ck <days_clear_kept>]

This option applies to DPN only. This option specifies the number of days the unmatched CLEAR alarms are kept in the unmatched alarm files. The default value is 7 days.

Use of this parameter on the command line overrides the setting recorded in the DPN Outage Calculator configuration file.

[-k <days_kept>]

This option applies to Passport only. This option specifies the number of days the unmatched out-of-service alarms are kept in the unmatched alarm files. The default value is 100 days.

Use of this parameter on the command line overrides the setting recorded in the Passport Outage Calculator configuration file.

Use of a negative integer causes the unmatched alarms to be retained until they are matched.

[-com]

For DPN, only, this option specifies that combined outages are to be calculated. The default is combined outage is not calculated.

Use of this parameter on the command line overrides the setting established in the outage calculator configuration file.

[-init]

This option is used to initialize the unmatched records database file used for alarms and SCNs.

[-dispcfg]

This option is used to display the outage calculator configuration parameters.

For DPN, these configuration settings are stored in the file /opt/MagellanMDP/cfg/mdp/MDPDPNOC.cfg.

For Passport, these configuration settings are stored in the file /opt/MagellanMDP/cfg/mdp/MDPPPOC.cfg.

[-force]

This option forces any database that is used by outage calculator to be reparsed from their source file.

[-help|-h]

This option prints out all the command line options specified in this section.

Outage calculation file names

This section describes the file names of the files associated with outage calculation.

The following files are described in this section:

- "Outage file names" (page 251)
- "Topology module description file names" (page 252)
- "Unmatched alarm file names" (page 253)

Outage file names

The DPN-100 and Passport Outage Calculators create BDF output files that use the following file naming convention:

DPN

The DPN Outage Calculator (mdpdpnoc) generates files with the following file names:

```
dpn_otg_<startDateTime>_<endDateTime>_<nodeID>.<ext>
```

Passport

The Passport Outage Calculator (mdpppoc) generates files with the following file names:

```
pp_otg_<startDateTime>_<endDateTime>_
<nodeID|nodename>_<alarmSeq#>_<scnSeq#>.<ext>
```

where:

<startDateTime> is the date and time of the earliest alarm or scn file record processed. The format is YYYYMMDDhhmmss (year, month, day, hour, minute, second).

<endDateTime> is the date and time of the latest alarm or scn record processed. The format is YYYYMMDDhhmmss (year, month, day, hour, minute, second). <nodeID|nodename> is the nodeID or nodename of the Passport, or namsID of the DPN-100, switch that generated the data.

<alarmSeq#> is the lowest sequence number obtained from Passport alarm input files. If no Passport alarm files are processed, this parameter indicates na (not applicable).

<scnSeq#> is the lowest sequence number obtained from Passport SCN input files. If no Passport SCN files are processed, this parameter indicates na (not applicable).

<ext> is the file extension. This is bdf for a BDF file and err for those input files which cannot be read by the Outage Calculator.

Examples

- for DPN-100
  `dpn_otg_19970501142354_19970501162501_338.bdf`
- for Passport
  `pp_otg_19960501142354_19960501162501_4031_683_na.bdf`

Topology module description file names

All topology module description files generated by the MDP Topology Generator use the following file-naming conventions:

```
<dpn|pp>.<namsID|nodeID>
```

Unmatched alarm file names

Unmatched alarms and scns use the following file-naming convention:

```
unmat_ala.<nodeID>
```

where <nodeID> is the nodeID of the switch that generated the alarm or scn.

Availability calculation

The MDP Availability Calculator calculates network availability statistics for switch components. Outage records generated by the DPN Outage Calculator and Passport Outage Calculator processes are used as input.

- For DPN-100, network components can be: modules, Processing Elements (PEs), trunks, and netlinks.
- For Passport, network components can be: modules, cards, Logical Processors (LPs), trunks, and DPN gateways (Passport 6000/7000, only).

The Availability Calculator generates the following metrics for all components for which outage records are processed:

Table 8
Availability metrics

Outage Time	Sum of individual outage durations less the period of outages covered by service windows defined in the exceptions file.
Service Time	Total time of sample period less any service windows defined in the exceptions file.
Number of Outages	The number of individual outages recorded, which were not completely covered by service windows defined in the exceptions files.
MTBF	Mean Time Between Failures is always expected to have a positive value. A negative value in this field indicates an MTBF of infinity. (Service Time - Outage Time) / (Number of Outages)
MTTR	Mean Time to Repair. (Outage Time) / (Number of Outages)

Table 8
Availability metrics

Percentage Availability	(MTBF / (MTBF + MTTR)) x 100
CP switchovers	The number of Control Processor switchovers recorded; valid for Passport components only. Durations are reported for Passports equipped with software release 5.1, or later.

Network availability statistics can be accumulated and retained (in an accumulated statistics file). These accumulated statistics provide totals for the period of time that the MDP Availability Calculator has been in operation and the period of time that a particular component has been tracked for availability.

Availability analysis can be repeated for requested time periods. See “Rollback of availability analysis statistics” (page 260).

Output from the MDP Availability Calculator is in the form of a BDF file that can be transfered by the MDP File Mover to a customer host.

The MDP File Mover can be configured to copy availability reports to a user-specified directory. This directory can be used by the Report Generator as an input directory.

For each execution of the Availability Calculator, an administration log file /opt/MagellanMDP/data/mdp/admin/MDPAC<date>.log (where <date> is the date the log file was generated) is created. This file records which outage files were processed, the renaming or deletion of any files, and any errors that occured. If a log file already exists for the date on which the Availability Calculator is executed, any new records are appended to the existing file. A preset number of log files are retained. The Availability Calculator process deletes the oldest file when the value specified by the -n option of mdpavcalc is exceeded.

The MDP Availability Calculator is a run-to-completion process that is typically started from a crontab entry, either weekly or monthly. This crontab entry must be created manually; it is not created using the MDP Configuration tool. This process can also be started at any time from the UNIX command line.

Note: The MDP Availability Calculator can only be run on the primary MDP host.

This section includes the following topics:

- "Types of reportable outages" (page 255)
- "Start life calculation" (page 257)
- "Availability calculator" (page 258)
- "Rollback of availability analysis statistics" (page 260)
- "Availability report generation" (page 264)
- "Availability calculation file names" (page 268)

Types of reportable outages

Four types of outages are used as input by the Availability Calculator.

Complete outages (component, possible, and combined)

These are outages for which alarm sets and clears, or SCNs, have been matched by the outage calculator. If selected, these outages are applied to the current sample period and the accumulated statistics.

Indeterminate outages

These are outages that have unmatched alarm sets, or SCNs. They are only reported in the current sample period. These outages are not reported in the accumulated statistics until complete.

The availability calculator reports indeterminate outages in the current sample period, as follows:

1 If an outage is detected in the current sample period and the outage start time is available but the outage end time is not available, the availability calculator reports the component outage from the outage start time to the end of the current sample period.

2 If the outage end time for an outage detected in a previous sample period is not available in subsequent sample periods, the availability calculator reports the component outage from the start of the current sample period to the end of the current sample period.

3 If the outage end time for an outage detected in a previous sample period is detected in the current sample period, the availability calculator reports the component outage from the start of the current sample period to the outage end time.

Passport module CP switchovers

These outages are recorded for a Passport module Control Processor card component when the Control Processor switches from standby to active.

For Passports using release software 5.1, or later, CP switchover counts and durations of CP switchovers is calculated.

For Passports using pre-5.1 Passport release software, the duration of this outage type is always zero, so the usual availability statistics cannot be calculated. However, a count of the number of CP switchovers is maintained. Special records are created in the Availability Report BDF file for these CP switchovers. These special records are the last records collected for a switch and have blank MTTR and availability fields for the current sample period and the accumulated sample period. These statistics cannot be calculated if the outage time is unknown.

The Report Generator highlights CP switchover records in the statistics table.

Passport 15000 software migration outages

The software migration outage defines an outage for spared FPs when one FP is removed from service to load new software ,and provisioning data, while the other FP provides service.

Software migration is a planned outage. You can exclude this outage from the network availability statistics by indicating the planned outage period in an exceptions file. See “Service window configuration” (page 120) for a detailed description of the exceptions file.

Accumulated statistics

The Availability Calculator accumulates the outage time, service time, number of outages, and number of Passport module CP switchover metrics. This process allows the MTBF, MTTR, and percentage availability to be calculated for the entire period of time during which the Availability Calculator has been in use, and during which the components have been reported.

The data recorded by each execution of mdpavcalc includes the component name, total service time, total outage time, total number of outages, and period of time for which these statistics have been accumulated.

This data is recorded in file /opt/MagellanMDP/data/mdp/avail/<dpn|pp|ppc>_acc_avail_<date>.data where <date> is the date the Accumulated Statistics file was created. By default, the Availability Calculator accumulated statistics files are retained for 100 days.

If a Passport is generating raw data files with one file name format (for example, using nodeIDs) and you need to generate raw data files from the same Passport using the alternate file name format (for example, using nodenames),

1 complete all value-added processing, and

2 delete the Accumulated Statistics file that contains entries for the Passport, before sending the raw data files, in the new format, to the MDP.

For more information about Passport raw data file names, see “Raw data” (page 52).

For each invocation of the Availability Calculator, with accumulated statistics option enabled, the file: /opt/MagellanMDP/data/mdp/avail/<dpn|pp|ppc>_otgfile_list_<date>.data, (where <date> is the date the current Outages Files Processed file was created) is used. This file contains a list of the outage files processed during the current run. If the Availability Calculator is executed more than once on the same day for the same switch type, any new records are appended to the existing Outage Files Processed file. On each invocation of the Availability Calculator, Outage Files Processed files that are more than 100 days old are deleted.

Start life calculation

The specific date and time at which a component becomes available for Availability Calculation purposes can be established by creating an entry in the start life file /opt/MagellanMDP/cfg/mdp/MDPSTLIFE.cfg. Otherwise, the start life value is automatically set to the start of the current sample period in which an outage for the component is first encountered. See “Start life configuration” (page 121).

If an outage starts before the specified start life of that component, the segment of the outage before the start life is discarded. This concept allows outages during the commissioning period for a component to be ignored.

The start life of a component is established once, only; that is when the first outage for the component is processed. It is not possible to change the start life once outages have been processed for that component, other than by rolling back the availability calculations to a sample period prior to the one where an outage for the component was first encountered.

When accumulated statistics are not enabled, the start life of a component is established for each run of the availability calculator where outages for that component are processed. A user-defined start life has no effect on availability calculations unless that start life is defined as being within, or later than, the current sampling time period.

Availability calculator

The MDP Availability Calculator can be started, typically weekly or monthly, by a crontab entry or manually from the command line. The runtime options can be specified on the command line or using a configuration file. See “Availability calculator configuration” (page 119). Command line options take precedence over configuration file entries.

Command syntax

The syntax of the MDP Availability Calculator command is

```
/opt/MagellanMDP/bin/mdpavcalc

[-i <input_directory>]
[-r <RDF_directory>]
[-o <output_directory>]
[-x <exceptions_file>]
[-s <start_life_file>]
[-d <delimiter>]
[-dpnd <delimiter>]
[-ppd <delimiter>]
[-loglevel <0-4>]
[-n <number of logs>]
[-a ]
[-help|h ]
```

Where the available options are

[-i <input_directory>]

This option specifies the directory that contains the input outage files. If a directory is not specified, the availability calculator uses outage files contained in both the DPN outage directory /opt/MagellanMDP/data/mdp/oc/dpn/outage and the Passport outage directory /opt/MagellanMDP/data/mdp/oc/pp/outage.

[-r <RDF_directory>]

This option specifies the directory that contains the record description files (RDFs); defaults to /opt/MagellanMDP/lib/mdp/rdf/<switch_type>/outage for outage RDF files and /opt/MagellanMDP/cfg/mdp/rdf/gen/avail and then /opt/MagellanMDP/lib/mdp/rdf/gen/avail for the output availability report RDF files.

[-o <output_directory>]

This options specifies the directory that contains the availability reports and defaults to /opt/MagellanMDP/data/mdp/dump/avail.

[-x <exceptions_file>]

This file lists the network service windows for components. This option overrides the default file MDPSERVWIN.cfg in directory /opt/MagellanMDP/cfg/mdp. If a file name is specified without using a pathname, the directory /opt/MagellanMDP/cfg/mdp is searched for the named file. See “Service window configuration” (page 120) for a detailed description of this file.

[-s <start_life_file>]

This file lists the component start lives. This option overrides the default file /opt/MagellanMDP/cfg/mdp/MDPSTLIFE.cfg. If a file name is specified without using a pathname, the directory /opt/MagellanMDP/cfg/mdp is searched for the named file. See “Start life configuration” (page 121) for a detailed description of this file.

[-d <delimiter>]

This is the field delimiter for the output Availability Report BDF files. The default is DEL. For a list of reserved characters that cannot be used as BDF delimiters, see “Interpreting BDF output” (page 26).

[-dpnd <delimiter>]

This is the field delimiter for input DPN Outage BDF files. The default is DEL.

[-ppd <delimiter>]

This is the field delimiter for input Passport Outage BDF files. The default is DEL.

[-loglevel <0-4>]

The level of logs reported to screen. The default level is `0`. All critical messages are displayed to your screen.

All critical, error, warning, and information messages are written to the log file. This level of log reporting is not configurable.

There are five levels of log reporting. For more information about log levels, see “Log levels” (page 207).

[-n <number of logs>]

This is the number of old log files to retain. The default is 3.

[-a]

This parameter specifies that accumulated statistics are to be calculated. The process reads in accumulated statistics, updates accumulated statistics from the outages files processed, and writes back the new values. The default is to produce statistics for the selected outages files, only.

[-h|-help]

This option requests command usage information.

Rollback of availability analysis statistics

In certain situations, it is necessary to repeat availability analysis for a specific period of time or for a specific set of outage files. This process is appropriate in the following situations: to exclude an outage which should have been excluded due to planned maintenance, or to correct an outage where the alarm

clear was missed and as a result the duration of the outage was inaccurate. The Accumulated Statistics Rollback Utility automates the process of recalculating availability statistics.

The MDP Outage Controller must be configured to save outage files in the backup directory and the retention period for these files must be appropriate to the normal frequency of the Availability Calculator being executed. For example, if the Availability Calculator is to be run once a month, it is suggested that the retention period for the archived outage files be set to 31 or more days.

The Accumulated Statistics Rollback Utility must be executed on the Primary MDP.

Operator rollback

Perform the following tasks:

1 Ensure that the Availability Calculator is not running and is not scheduled to run before the rollback operation is completed. If necessary, convert the crontab entry that invokes the Availability Calculator to a file comment by placing an octothorpe (#) in the first column of the crontab entry; save the file.

2 Copy the outage files to be corrected from the backup directory /opt/MagellanMDP/data/mdp/backup/outage to the appropriate outage directory /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/outage; edit the records as necessary.

3 Invoke the Rollback Utility . If outage files for only one switch type have been edited, the Rollback Utility can be invoked with the command line option -s <dpn|pp> to specify the switch type. Specifying this option prevents outage files for other switch types from being unnecessarily reprocessed.

4 If the crontab entry that invokes the Availability Calculator was converted to a comment in Step 1, ensure that it is uncommented by removing the octothorpe (#) in the first column.

Rollback utility automated tasks

The following tasks are performed by the MDP Accumulated Statistics Rollback Utility mdpavrback:

1 A list of outage files processed for each run of the Availability Calculator is created. The names of the outage files currently in the outage directories are compared with this list. The oldest Outage Files Processed file with an outage file currently in an outage directory is determined.

2 All the outage files identified in the oldest Outage Files Processed list file, as determined in Step 1, and any subsequent Outage Files Processed list files are copied from the backup directory to the appropriate outage directory.

3 The oldest Outage Files Processed list file, as determined in Step 1, and any subsequent Outage Files Processed list files are deleted.

4 The Accumulated Statistics file, with a generation date that corresponds to the oldest Outage Files Processed list file, as determined in Step 1, and all subsequent Accumulated Statistics files are deleted.

5 The Availability Calculator is invoked.

The Accumulated Statistics Rollback Utility can be invoked for one switch type but the default is to rollback statistics for all switch types. In this case, outages files for other switch types are not copied from backup directories and the Accumulated Statistics and Outage Files Processed list files are not deleted. Any new outage files for the switch type not being recalculated are processed normally and new Accumulated Statistic files and Outage Files Processed list files are created.

The MDP Accumulated Statistics Rollback Utility is started manually from the command line. Runtime options are specified on the command line.

Command syntax

The syntax of the MDP Accumulated Statistics Rollback Utility is

```
/opt/MagellanMDP/bin/mdpavrback
[-s dpn|pp]
[-a "<avail_calc_options>"]
[-b <backup_directory>]
[-o <outage_directory>]
[-loglevel <0-4>]
[-help ]
```

where the available options are

[-s [dpn|pp]]

Select the switch type. The default is all switch types.

[-a “<avail_calc_options>”]

This option sets the Availability Calculator runtime options. This parameter defaults to the values in the Availability Calculator configuration file, then to Availability Calculator runtime defaults.

The Availability Calculator runtime options must be enclosed in double quotes to distinguish Availability Calculator runtime options from Accumulated Statistics Rollback Utility runtime options.

[-b <backup_directory>]

This is the directory from which the outage files are obtained. This parameter defaults to /opt/MagellanMDP/data/mdp/backup/outage.

[-o <outage_directory>]

This is the directory to which the outage files are copied. This parameter defaults to /opt/MagellanMDP/data/mdp/oc/<dpn|pp>/outage.

[-loglevel <0-4>]

The level of logs reported to screen. The default level is `0`. All critical messages are displayed to your screen.

All critical, error, warning, and information messages are written to the log file. This level of log reporting is not configurable.

There are five levels of log reporting. For more information about log levels, see “Log levels” (page 207).

[-h|-help]

This option requests command usage information.

Availability report generation

The Report Generator process converts a BDF Availability Report file into formatted ASCII text output. This process can be used to obtain availability statistics for installations that do not use a separate reporting application. The user can control which statistics are displayed in the report and set page size parameters to control the output.

If the MDP File Mover is configured to transfer Availability Report BDF files to external customer hosts, then the File Mover must also be configured to copy Availability Report BDF files to a user-defined directory location. This location can be used as the input directory for the MDP Report Generator using the -idir paramater. See “Backing up converted files” (page 91).

Availability reports can only be generated from a primary MDP host.

Availability report presentation

Availability Reports provide the following information:

- Time measurements are rounded up to the next unit at the following thresholds:

  60 seconds become 1 minute
  60 minutes become 1 hour
  24 hours become 1 day
  365.25 days become 1 year

- If no outages are reported for a component during the current sample period, a dash (-) is printed in the MTBF column.
- Passports using a pre-5.1 software release report the number of CP switchover outages by indicating the number of outages (Outages) for the shelf cards of the active and standby CPs. Outage Time is blank for CP switchovers. These outages are reported in a separate section at the end of the Availability Report.

  Passports using a 5.1, or later, software release report the number (Outages) and the duration (Outage Time) for CP switchover outages, with the component indicating logical processor LP/0.

- Module outages are indicated by a blank component.

- The following is an example of an Availability Report (the last column (availability percentage) is wrapped around):

Example

```
Availability ReportPage 1/1

Report Type: All ComponentsModule: 1041

Sample Period: 17/Sep/1998 17:44 - 21/Sep/1998 11:44

ComponentOutage TimeService TimeOutagesMTBFMTTRAvail

4.43mins3.75days31.2days1.47mins99.91%

EM/PCS Logical
     Processor/041.00secs3.75days13.74days 41.00secs
99.98%

EM/PCS Shelf Card/1 9.00secs3.75days13.74days
  9.00secs99.99%

EM/PCS Shelf Card/2 9.00secs3.75days13.74days
  9.00secs99.99%
```

Availability report generator

The MDP Report Generator can be started automatically, using a crontab entry, or manually from the command line. The runtime options can be specified on the command line or using a configuration file. See “Availability report generation” (page 122). Command line options take precedence over configuration file entries.

To report CP switchovers for Passports:

- for Passports using a pre-5.1 software release CP switchover counts are reported in a separate section at the end of the Availability Report. To generate this type of report, you must use reportType ALL and you must include the -cpsw option.
- for Passports using a 5.1, or later, software release CP switchover counts and durations are included with the Logical Processor/0 component.

Command syntax

The syntax of the MDP Report Generator command is:

```
/opt/MagellanMDP/bin/mdprepgen
[<report_type>]
[<module>]
[-a]
[-cpsw]
[-i <input_file>]
[-idir <input_directory>]
[-r <RDF_directory>]
[-o <output_file>]
[-d <delimiter>]
[-t <availability_threshold>]
[-w <page_width>]
[-l <page_length>]
[-loglevel <0-4>]
[-help|h]
```

Where the available options are:

[<report_type>]

This option specifies the type of report, as follows, to generate (the default is ALL):

MODLINK: modules and links
SUBCOMP: module subcomponents
BACKBONE: processors, cards and LPs
TOPOLOGY: trunks, links and gateways
LOGPROC: Passports LPs only
ALL: all component types (default)

[<module>]

This option indicates the nodeID, or nodename, of a module. The report is limited to this module and its subcomponents. The default is to report on all modules.

[-a]

This option instructs the process to report accumulated statistics. The default is to use last sample period only.

[-cpsw]

For Passports using a pre-5.1 software release, this option instructs the report generator to display CP switchover counts in a separate section at the end of the Availability Report. The default is not to display CP switchover counts for Passports using a pre-5.1 software release.

[-i <input_file>]

The file name (including the path if the file is not in the default directory) of the availability report file to generate the report from. The default is the most recent file in the directory /opt/MagellanMDP/data/mdp/dump/avail.

[-idir <input_directory>]

The absolute path of a directory to use as the default for input Availability Report BDF files. The default for this option is /opt/MagellanMDP/data/mdp/dump/avail.

[-r <RDF_directory>]

The directory for the availability report RDF. The default is /opt/MagellanMDP/cfg/mdp/rdf/gen/avail and then /opt/MagellanMDP/lib/mdp/rdf/gen/avail.

[-o <output_file>]

The file name, including full path, for the generated report. The default is UNIX stdout.

[-d <delimiter>]

The field delimiter character for BDF files. The default is DEL.

[-t <availability_threshold>]

The threshold percentage availability over which a component is be included in the report generated.

[-w <page_width>]

The maximum number of characters per line. The default is no line limit.

For configurable windows, for example, Xterms, it is suggested that this parameter be set to a minimum of 90 characters and the window size be adjusted as required.

[-l <page_length>]

The maximum number of lines per page. The default is 66.

[-loglevel <0-4>]

The level of logs reported to screen. The default level is `0`. All critical messages are displayed to your screen.

All critical, error, warning, and information messages are written to the log file. This level of log reporting is not configurable.

There are five levels of log reporting. For more information about log levels, see “Log levels” (page 207).

[-h |-help]

This options requests command usage information.

Availability calculation file names

This section describes the file names of the files associated with availability calculation.

The following files are described in this section:

- “Availability report file names” (page 268)
- “Accumulated statistics file names” (page 268)

Availability report file names

The Availability Calculator processes individual outage records to calculate availability statistics over a specified period and creates bulk data format (BDF) output files that use the following file-naming convention:

```
avail_<date-of-generation>.bdf
```

where:
<date> is the date that the file was generated and uses the format YYYYMMDD (year, month, day).

Accumulated statistics file names

The Availability Calculator can combine individual availability records in an accumulated statistics file. The file-naming convention used for this file is

```
[dpn|pp]_acc_avail_<date>.data
```

where:
<date> is the date that the file was generated and uses the format YYYYMMDD (year, month, day).

Index

A

accaggregator, Vector 72
acccorrelator, Vector 72, 74, 196
  legacy call records 73, 195
administration 181
  client
    common buttons 85
    logs 86
    window status 86
  controlling processes 38
  directory 204
aggregator, Vector
  legacy call records 72, 193
amconv 188
archive
  processing data from 198
archiving 31
  BDF records 133, 163
  bulk data format 31
  configuring for BDF 96
    procedure 97
  MDP logs 32
  raw data 31
audits
  configuring 101
availability calculation 253
  accumulated statistics
    file names 268
  configuring 118
    procedure 119
  file names 268
  report generation 264
    command syntax 265
    file names 268
  report presentation 264
  rollback of 260
  start life 257
availability calculator
  command syntax 258
  service window configuration 120
  start life configuration 121

B

backup MDP 35
backups
  configuring
    converted data files 91
  published format data files 93
BDF
  data compression
    SRS 151
  file naming
    short file names 65, 79
  interpreting output 26
  viewing 198, 199
BDF converter
  command syntax 186
BDF data file names
  Vector 78
benefits of MDP 23

bulk data format
archiving 31, 96
procedure 97
audit reports 28
backing up files 91
configuring
file retention time 95
DPN 163
archiving 163
converting to 163
outage calculation 166
setting BDF data compression 164
setting the escape character 166
setting the field delimiter 164
setting the log level 165
introduction 25
Passport 126
archiving 133
backward compatibility 129
converting to 127
customizing 130
DMId and RDF version in records 129
empty files 133
including the DMId in file names 128
outage calculation 134
setting BDF data compression 128
setting the escape character 132
setting the field delimiter 127
setting the log level 132
Vector 176
converting to 176
logging warnings 178
setting BDF data compression 177
setting the field delimiter 177
viewing 28, 198, 199

C

collecting data 24
combined outages
configuring 157, 172
commands
bdfview 199
configuration
administration client
common buttons 85
logsl 86
window status 86
backing-up converted data files 91
customer data transfers
scheduling customized programs 93
customer file transfers
backing up PF files 93
failures 94
setting the log level 92
customer hosts 88
adding 88
changing the password 89
customized MDP directories 106
flexible directory installation
window 110
recording 113
restrictions 112
setting a secondary mount point 114
customizing 82
data file retention 94
log level 96
minimum diskspace 96
setting the time 95
DPN 161
BDF data management 163
archiving 163
converting to 163
setting BDF data compression 164
setting the escape character 166
setting the field delimiter 164
setting the log level 165
outage calculation 166
PF data management 167
backward compatibility 168
converting to 167
data encoding 167
data storage format 168

prerequisites 162
setting the File Manager log level 167
storing raw data 162
file processing audits 101
file transfers to customer hosts 87, 90
log archiving 103
MDP software 81
new MDPs
optional features 82
prerequisites 82
outage calculator 156, 171
combined outages 157, 172
log level 158, 173
maximum threshold 158, 173
minimum threshold 157, 172
number of days to keep CLEAR alarms 173
number of days to keep SET alarms 173
number of days to keep unmatched OOS records 158
setting the BDF delimiter 157, 172
outage controller 115
archiving outage files 118
enabling outage calculation 117
identifying a secondary MDP 116
identifying the MDM host 116
log level 117
primary or secondary MDP 115
scheduling 116
topology generator 117
transferring outage files to customer hosts 118
Passport 125
BDF data management 126
archiving 133
backward compatibility 129
converting to 127
customizing 130
DMID and RDF version in records 129
including the DMId in file names 128
setting BDF data compression 128
setting the escape character 132
setting the field delimiter 127
setting the log level 132
collecting data 136
managing collection entries 137
setting collection options 140
empty files 133
outage calculation 134
PF data management 134
backward compatibility 135
converting to 135
data encoding 135
data storage format 136
prerequisites 125
setting the File Manager log level 134
storing raw data 126
surveillance 105
tool 85
launching 87
from Preside MDM 87
from the UNIX command line 87
transferring files to multiple directories on the same host 92
Vector 175
BDF data management 176
converting to 176
logging warnings 178
setting BDF data compression 177
setting the field delimiter 177
prerequisites 175
secondary MDP 178
setting the File Manager log level 178
storing raw data 176
configuring
availability calculation 118, 119
report generation 122
service window 120
start life 121
BDF archiving 96
procedure 97

DPN
data collection 171
spooling site 169
DPN switches 169
Passport data management 125
SRS
adding Passport groups 152
backup 151
BDF data compression 151
BDF field delimiter 151
BDF file closure interval 150
committed RCF 148
log level 151
maximum BDF file size 150
Passport access host 151
polling interval 149
removing Passport groups 152
Statistics Retrieval System 145
Vector switches 179
configuring MDP
introduction 37
controlling processes 38
correlator, Vector
Egress call records 74, 196
performance data 74, 197
customer host 36
customer hosts
checking
file transfers to 91
configuring 88
adding 88
changing the passwordt 89
file transfers to 87, 90
outage files 118
customizing BDF records 130

D

data collection
DPN 63
MDP 51
Passport
introduction 48
spooled data files 49
Passport data 125
data conversion 24
bulk data format (BDF) 25
introduction
audit reports 28
published format 29
Vector 71
data file names
DPN
archived BDF data 66
BDF data 64
PF with backward compatibility disabled 67
PF with backward compatibility enabled 66
short BDF file names 65
Passport 52
archived BDF data 55
BDF data 53
PF with backward compatibility disabled 56
PF with backward compatibility enabled 55
raw data 52
short BDF file names 54
SRS 57
Vector
short BDF file names 79
data file retention
configuring 94
log level 96
minimum diskspace 96
data file retention time, setting 95
data flow
Passport 42
Vector 69
data models 46
Data Viewer 198
datatypes

DPN 62
Passport 45
Vector 71
directories
admin 204
merge 77
directory structure 39
diskspace, setting minimum 96
DPN
availability calculation 253
rollback of 260
start life 257
configuring 161
a spooling site for a DPN module 169
BDF data management 163
archiving 163
converting to 163
setting BDF data compression 164
setting the escape character 166
setting the field delimiter 164
setting the log level 165
data collection 171
outage calculation 166
PF data management 167
backward compatibility 168
converting to 167
data encoding 167
data storage format 168
prerequisites 162
setting the File Manager log level 167
storing raw data 162
data collection 63
data file names
archived BDF data 66
BDF data 64
data file names
DPN 63
PF with backward compatibility
disabled 67
PF with backward compatibility
enabled 66
short BDF file names 65
data flow
data flow
DPN 60
datatypes 62
introduction 60
outage
calculation 233
combined 234
component outage 234
controller 243
possible component outages 234
types of outages 234
outage calculation
process overview 242
PAD daemon 169
Published Format Converter 188
raw data files 64
switch setup 169
topology generator 244
value-added application 68

E

empty data files 133
events and traps 225

F

File Managers
log format 203
Vector 71
file naming 251
aggregated Vector data files 77
availability calculator 268
accumulated statistics 268
reports 268
correlated Vector data files 77
DPN raw data files 64
log files 204
archived 206
temporary 206
outage files 251

topology module description files 252
unmatched alarm files 253
Vector raw data files 75
file transfers to customer hosts
checking 91
configuring 87, 90
flexible directory installation window 110
fpconv 188
FTP 179

G

generating Log Viewer reports 217

H

hosts 34
backup MDP 35
customer host 36
primary MDP 34
secondary MDP 35

I

installation
directory structure 39
interpreting BDF output 26
Introduction 23
archiving 31
collecting data 24
configuring MDP 37
data conversion 24
DPN 60
MDP logs 38
Passport
Statistics Retrieval System (SRS) 58
Passport support 42
Passport value-added applications 58
supporting MDP 34
transferring data to down-stream applications 33
Vector 69

L

launching the Configuration tool 87
from Preside MDM 87
from the UNIX command line 87
log level
setting for Disk Manager 96
Log Viewer 207
command 208, 217
generating reports 217
procedures
using the Log Viewer 213
window
included fields 211
log records 212
log report 212
pull-down menus 209
selected logs and filters 211
logs
log levels 207
messages 218
viewer window 209
opening 208
logs, MDP 203
format 203
naming 204
archived 206
temporary 206
viewing 207

M

MDP directories
customizing 106
flexible directory installation window 110
recording 113
restrictions 112
setting a secondary mount point 114
MDP logs 86
archiving 32
configuring archives 103
DPN

File Manager 167
introduction 38
log level
setting for customer file transfers 92
outage calculator 158, 173
outage controller 117
Passport
File Manager 134
Vector
File Manager 178
MDP workstations 37
mdpavcalc
command syntax 258
mdplv 208, 217
mdpoctrl 242
mdpppmgr 188
mdprepgen 265
mdpvssmgr 71, 72
merge directory 77
messages 218

O

optional features
configuring 82
outage calculation 232
DPN 233
assigning data 166
Passport 235
alarm exceptions file 241
assigning data 134
risks and limitations 238
outage calculator 246
configuring 156, 171
combined outages 157, 172
log level 158, 173
maximum threshold 158, 173
minimum threshold 157, 172
number of days to keep CLEAR alarms 173
number of days to keep SET alarms 173
number of days to keep unmatched OOS records 158
setting the BDF delimiter 157, 172
file naming 251
unmatched alarm files 253
outage controller 242, 243
configuring 115
archiving outage files 118
enabling outage calculation 117
identifying a secondary MDP 116
identifying the MDM host 116
log level 117
primary or secondary MDP 115
scheduling 116
topology generator 117
transferring outage files to customer hosts 118

P

PAD daemon setting 169
Passport
availability calculation 253
rollback of 260
start life 257
collecting data
configuration 136
managing collection entries 137
setting collection options 140
configuring 125
BDF data management 126
archiving 133
backward compatibility 129
converting to 127
customizing 130
DMId and RDF version in records 129
including the DMId in file names 128
setting BDF data compression 128
setting the escape character 132
setting the field delimiter 127
setting the log level 132
empty files 133

outage calculation 134
PF data management 134
backward compatibility 135
converting to 135
data encoding 135
data storage format 136
prerequisites 125
setting the File Manage log level 134
Statistics Retrieval System 145
storing raw data 126
data collection
MDP 51
data file names 52
archived BDF data 55
BDF data 53
PF with backward compatibility disabled 56
PF with backward compatibility enabled 55
raw data 52
short BDF file names 54
SRS 57
data flow 42
data management configuration 125
data models 46
datatypes 45
File Manager 188
introduction to MDP support 42
outage calculation 235
alarm exceptions file 241
approach 236
parsing alarms and SCNS 235
process overview 242
risks and limitations 238
types of outages 239
component 239
CP switchover 240
indeterminate 240
migration 240
partial 240
Published Format Converter 188
SRS
setting log level 151
Statistics Retrieval System
selecting Passport component instances 154
selecting Passport components and attributes 152, 153
starting the RCF Editor 152
Passport data collection
introduction 48
spooled data files 49
pfview 201
Planning
hosts 34
backup MDP 35
customer host 36
primary MDP 34
secondary MDP 35
pmaggregator, Vector 72
pmcorrelator, Vector 72, 74, 197
primary MDP 34
processes
controlling 38
processing archived data 198
Published Format
amconv 188
backward compatibility option
disabled 56, 67
enabled 66
converter
syntax 188
fpconv 188
viewing PF files 201
published format
backing up files 91
configuring
file retention time 95
data conversion
introduction 29
DPN 167
backward compatibility 168

converting to 167
data encoding 167
data storage format 168
Passport 134
backward compatibility 135
converting to 135
data encoding 135
data storage format 136
viewing 30

R

raw data
archiving 31
DPN
storing 162
Passport
storing 126
Vector
storing 176
raw data files
DPN 64
processing archived 198
Vector 75
RDFs 26
file naming 24

S

scheduling customized data analysis programs 93
secondary MDP 35, 116
selecting Passport component instances 154
setting the BDF field delimiter
SRS 151
SNMP traps
event mappings 226
process overview 225
retransmission of traps 228
SRS
configuring
adding Passport groups 152
backup 151
BDF data compression 151
BDF field delimiter 151
BDF file closure interval 150
committed RCF 148
log level 151
maximum BDF file size 150
Passport access host 151
polling interval 149
removing Passport groups 152
Statistics Retrieval System
configuring 145
selecting Passport components and attributes 152, 154
selecting Passport components and attributes 153
starting the RCF Editor 152
Statistics Retrieval System (SRS) 58
support MDP
introduction
MDP workstations 37
supporting MDP
introduction 34
surveillance
configuring 105
syntax
availability calculator 258
availability report generator 265
BDF Converter 186
DPN Published Format converter 188
Egress call record correlator 74, 196
legacy call record aggregator 72, 193
Log Viewer 217
Passport Published Format converter 188
performance data correlator 74, 197
Published Format Converter 188
Vector legacy call record correlator 73, 195

T

topology generator 244
module description files 252
transferring data to down-stream

applications 33
transferring files to customer hosts
outage 118
transferring files to multiple directories on the same host 92
traps
MDP 225
overview 225
retransmission 228
Troubleshooting
customer file transfer failure 94
types of outages
DPN 234
combined 234
component 234
possible component 234
Passport 239
component 239
CP switchover 240
indeterminate 240
migration 240
partial 240

U

using the Log Viewer 213

V

value-added applications
DPN 68
Passport 58
Value-Added Data (VAD) 231
availability calculation 253
report generation 122, 264
report generator syntax 265
report presentation 264
rollback of 260
start life calculation 257
availability calculator
command syntax 258
outage calculation 232
DPN 233
Passport 235
approach 236
parsing alarms and SCNS 235
risks and limitations 238
process overview 242
outage calculators 246
outage controller 242, 243
topology generator 244
Vector
aggregated Vector data files 77
BDF data file names 78
configuring 175
BDF data management 176
converting to 176
logging warnings 178
setting BDF data compression 177
setting the field delimiter 177
prerequisites 175
secondary MDP 178
setting the File Manage log level 178
storing raw data 176
correlated Vector data files 77
data conversion 71
data file names
data file names
Vector 75
short BDF file names 79
data flow 69
datatypes 71
Egress call record correlator 74, 196
File Manager 71
missing data 72
introduction 69
legacy call record aggregator 72, 193
legacy call record correlator 73, 195
performance data correlator 74, 197
raw data files 75
switch setup 179
VMI 180
viewing
bulk data format 28

logs 208
published format 30
viewing BDF files 198, 199
viewing MDP logs 207
viewing Published Format files 201

Preside Multiservice Data Manager

Management Data Provider

User Guide

R14.3

Publication: 241-6001-309
Document status: Draft
Document version: 14.3D3
Document date: June 2003
Printed in Canada

NORTEL NETWORKS