

DIH 1.2

Centralized Configuration Manager Administration Guide

910-6509-001 Revision A

August 2012



Copyright 2010 – 2012 Tekelec. All Rights Reserved. Printed in USA.
Legal Information can be accessed from the Main Menu of the optical disc or on the
Tekelec Customer Support web site in the *Legal Information* folder of the *Product Support* tab.

Table of Contents

Chapter 1: About This Help Text.....	15
Overview.....	16
Scope and Audience.....	16
About the Diameter Intelligence Hub (DIH).....	16
User Preferences.....	17
Customer Care Center.....	21
DIH Documentation Library.....	24
Locate Product Documentation on the Customer Support Site.....	24
Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents.....	25
Chapter 2: CCM Overview.....	26
CCM Overview.....	27
Chapter 3: Key Concepts.....	28
PMF IP Data Acquisition.....	29
Monitored Network Elements.....	29
About PDU Collection.....	29
PDU Collection on PMF IP Networks.....	30
PDU Routing and Filtering.....	30
About Traffic Classification Filtering.....	30
About IP Dataflows.....	31
About Dataflows.....	31
Dataflows Versus IP Streams.....	31
About Data Transport Service (DTS).....	31
About Input Streams.....	31
About Routing.....	32
About xDR Generation.....	32
About Sessions and Dictionaries.....	32
About xDR Data Feeds.....	32
About Network Views.....	32
About Security and Permissions.....	33
About Equipment Registry.....	33
About Sites.....	33
About Hosts.....	34

About Subsystems.....	34
Chapter 4: Using CCM.....	35
About CCM.....	36
Logging into NSP.....	36
Opening CCM.....	37
Understanding the CCM Screen.....	37
About Tool bar and Right-click Menu Functions.....	38
Buttons and Pop-up Menus.....	38
Column Functions.....	38
Chapter 5: Home Screen Operations.....	39
About CCM Home Page Operations.....	40
Network Elements.....	40
Nodes.....	40
IP Signaling Point List Screen.....	41
Network View Lists.....	41
Session Views.....	41
xDR-Related Elements.....	42
xDR Sessions.....	42
Protocols.....	42
Dictionaries.....	43
Stacks.....	43
PDU Hiding.....	44
Bulk Load.....	44
Bulk Loading Process.....	45
PMF Element Configurations.....	45
Importing PMF Configurations.....	52
PMF IP Filter Configurations.....	53
Importing PMF IP Filters.....	55
Exporting Bulk Load Configurations.....	56
Creating a Configuration Report.....	57
Setting the Severity of Platform Alarms.....	58
Chapter 6: Equipment Registry.....	60
About Equipment Registry.....	61
Sites.....	61
Site Creation and Discovery Process.....	61
Managing the Report Server.....	65

About Subsystems.....	66
Virtual IP Address Assignment.....	67
Adding an IXP Subsystem.....	67
Modifying an IXP Subsystem.....	70
Deleting an IXP Subsystem.....	70
Re-discovering Applications.....	70
Managing an IXP Storage Pool.....	71
Storage Server Designations.....	72
Adding a Storage Server to an IXP Storage Pool.....	72
Deleting a Storage Server.....	75
About xMF (PMF) Subsystems.....	75
Adding a PMF Subsystem to a Site.....	75
Modifying a PMF Subsystem Host.....	78
Deleting a PMF Subsystem.....	78
Chapter 7: Network Element Configuration.....	79
About Network Elements.....	80
Filtering Network Elements.....	80
About Nodes.....	81
Creating a Node.....	81
Modifying a Node.....	82
Deleting a Node.....	82
About Non-node Network Elements.....	82
About IP Network Elements.....	83
Chapter 8: Network View Configuration.....	90
About Network Views.....	91
Creating Network Views.....	91
Creating Network Session Views.....	93
Nesting Network Views.....	93
About Network Views that Separate xDR Sessions.....	94
About Link-based Network Views.....	95
Configuring link Views.....	95
Creating Link-based Network Views.....	95
Selecting Traffic Classifications.....	98
Modifying Link-based Network Views.....	99
Deleting Link-based Network View.....	100
Chapter 9: xMF Acquisition.....	101

About the Acquisition Perspective.....	102
About PMF Subsystem Management.....	102
Viewing Changes to an PMF Subsystem.....	103
Loading an Empty Configuration on to an PMF Subsystem.....	103
Cancelling Changes to an PMF Subsystem	104
About xMF Subsystem Settings.....	105
Viewing PMF Subsystem Status.....	108
About Feeder Thresholds.....	108
About PMF Applications.....	111
Modifying PMF Applications.....	111
Deleting PMF Applications.....	111
About PMF Traffic Classifications	112
About PMIA (for PMF Subsystems).....	118
About Data Transport Service (DTS).....	120
About PDU Filters.....	120
xMF MSU and EMP Correspondance Values.....	121
About IP PDU Filters.....	122
About Diameter Protocol Filters.....	135
About PDU Dataflows.....	138
About IP Dataflows.....	138
Adding an IP Dataflow.....	138
Modifying an IP Dataflow.....	142
Deleting an IP Dataflow.....	142
About Alarms.....	142
Managing Platform Alarms.....	143
Chapter 10: IXP Mediation.....	144
About Mediation Perspective.....	145
About Managing each IXP Subsystem.....	145
About IXP Subsystem Functions.....	146
About Applying Changes to an IXP Subsystem	147
Viewing Changes to an IXP Subsystem.....	148
Enabling and Disabling IXP Subsystem Automatic Failover.....	148
Loading an Empty Configuration on to an IXP Subsystem.....	148
Cancelling Changes to an IXP Subsystem	149
Backup and restoring an IXP Subsystem.....	149
Deleting an archived Backup.....	150
Discovering xDR Builders.....	150
Discovering Frame and Port Position.....	151
Modifying a server Role.....	151

Changing a Primary Server Role.....	151
About IXP Storage Servers.....	152
Changing the State of a Storage Server.....	152
IXP Storage Pool States.....	153
Configuring Servers in an IXP Subsystem.....	154
About Streams.....	155
Adding a PDU Stream.....	156
Adding an xDR Stream.....	156
Modifying a Stream	157
Deleting a Stream	159
Configuring xDR Dataflow Processings.....	159
About Dataflow Processings.....	159
About Dataflow Processing Retention Times.....	159
Listing xDR Dataflow Processings.....	160
About xDR Dataflow Assistant.....	161
About Managing Dataflow Processings Manually.....	164
About Partial xDRs.....	188
Creating an xDR Session for a Dataflow Processing.....	188
Modifying an xDR session for a dataflow Processing.....	190
Deleting an xDR session from a dataflow Processing.....	191
About Q.752 Dataflows.....	191
About the Q.752 Dataflow Assistant.....	192
About Distributions.....	195
About Software.....	195
About Subsystem Preferences.....	196
Managing Multiple IXP Subsystems.....	198
About Dictionaries.....	198
Creating a Dictionary.....	199
Modifying a Dictionary.....	200
Enabling or Disabling PDU Decode Hiding for a Dictionary.....	202
Editing Category Titles in a Dictionary.....	203
Enabling and Disabling PDU Summary Hiding.....	203
Deleting a Dictionary.....	203
Viewing a Dictionary Source.....	204
Listing Unused Dictionaries.....	205
About xDR Filters.....	206
Adding xDR Filters.....	206
Modifying xDR Filters.....	208
Deleting xDR Filters.....	208
About Sessions.....	209
About xDR Session Table Layout.....	209

Listing xDR Sessions.....	210
Adding a Protocol-Specific xDR Session.....	210
Modifying an xDR Sessions.....	212
Deleting xDR Sessions.....	213
Purging Static Sessions.....	213
Creating an xDR filter for an existing Session.....	213
Modifying xDR Session Backups.....	214
Creating and associating a dictionary with a Session.....	214
xDR Builder Parameters.....	215
About Enrichment Files.....	216
Adding Enrichment Files.....	216
Deleting Enrichment Files.....	217
Viewing Enrichment File Source Code.....	217
Chapter 11: Monitoring Policies.....	218
About 3G Monitoring Policies.....	219
The Monitoring Policies Screen.....	219
Adding a Monitoring Policy.....	220
Modifying a Monitoring Policy.....	221
Deleting a Monitoring Policy.....	221
Activating and Deactivating Monitoring Policies.....	222
About Filtering Monitoring Policies.....	222
Filtering Monitoring Policies.....	222
Appendix A: Configuration Workflows.....	223
Provisioning Guide for Configuring a DIH System.....	224
Setting up DIH Sites.....	224
IP Network Data Acquisition for PMF.....	225
Configuring for 3G Intelligent Data Monitoring (IDM).....	225
Routing PDUs to xDR Builders.....	225
Appendix B: xDR Builder Parameters.....	227
List of Parameters for Each xDR Builder.....	228
Initial Parameters.....	228
IP Transport Screen.....	229

List of Figures

Figure 1: Date/Time Tab Screen.....	17
Figure 2: Directory Tab Screen.....	18
Figure 3: Mapping Tab Screen.....	19
Figure 4: Point Code Tab Screen.....	19
Figure 5: Formatting Rules (CIC) Screen.....	20
Figure 6: Default Period Tab Screen (ProTrace only).....	21
Figure 7: Pmf Ip Data Acquisition Sequence.....	29
Figure 8: NSP Portal Screen.....	36
Figure 9: SS7 Node(s) List Screen.....	41
Figure 10: IP Signaling Point List Screen.....	41
Figure 11: Network Sessions List Screen.....	42
Figure 12: xDR Sessions List Screen.....	42
Figure 13: Protocols Screen.....	43
Figure 14: Dictionaries Present Screen.....	43
Figure 15: Stacks List Screen.....	44
Figure 16: Bulk Load Import Screen.....	53
Figure 17: Browse Screen.....	55
Figure 18: Bulk Export Configurations Prompt.....	56
Figure 19: Zip Extract Screen.....	57
Figure 20: Open/Save Prompt For Configuration Report.....	57
Figure 21: Sample Report.....	58
Figure 22: Alarms Configuration Screen.....	58
Figure 23: Modify Platform Alarm Configuration Screen.....	59
Figure 24: Site List Screen.....	62
Figure 25: Site Add Screen.....	62
Figure 26: New Site With Subsystems.....	63
Figure 27: Site Modify Screen.....	64
Figure 28: Subsystem Results Summary Screen.....	69
Figure 29: Results Summary Screen With Error Symbol.....	69
Figure 30: Object Tree Showing Added Subsystem With Results Screen.....	70
Figure 31: IXP Subsystem List Screen.....	71
Figure 32: IXP Subsystem After Re-discover Process.....	71
Figure 33: Add IXP Subsystem Screen.....	73
Figure 34: Subsystem Results Screen.....	74
Figure 35: Results Screen With Error Symbol.....	74
Figure 36: Object Tree Showing Added Subsystem With Results Screen.....	75
Figure 37: PMF Results Summary Screen.....	77

Figure 38: Discovery Summary Screen - Hosts Tab.....	77
Figure 39: Discovery Summary Screen - Application Tab.....	77
Figure 40: Discovery Summary Screen - PMF Card Discovery.....	78
Figure 41: Network Element Filter Screen (Linkset shown).....	80
Figure 42: Filter Screen Filled.....	81
Figure 43: Node Add Screen.....	82
Figure 44: Add Signaling Point Screen.....	84
Figure 45: Network View Perspective.....	91
Figure 46: Initial Setup Screen.....	92
Figure 47: View Type Selection Screen.....	92
Figure 48: Network View List Screen.....	94
Figure 49: View Type Selection Screen.....	94
Figure 50: Network View Perspective.....	95
Figure 51: Link Network View Create Info-Initial Setup.....	96
Figure 52: View Type Selection Screen.....	97
Figure 53: View Type Classification Screen.....	98
Figure 75: PMF Subsystem Pop-Up Menu.....	147
Figure 55: xMF Subsystem Settings List Screen.....	107
Figure 56: xMF Subsystem Parameter Add Screen.....	107
Figure 57: Feeder Thresholds List Screen.....	111
Figure 58: Feeder Thresholds Modify Screen.....	111
Figure 59: PMIA Screen.....	119
Figure 60: Dts List Screen.....	120
Figure 61: Dts Add Screen.....	120
Figure 63: Add IP Address Filter Screen.....	124
Figure 63: IP Filters Screen.....	124
Figure 64: IP Port Filter Screen With GTP Port Filter Default.....	126
Figure 65: Add Port Filter Screen.....	127
Figure 66: Add IP VLAN Filter Screen.....	129
Figure 67: Add SAPI for Gb over IP Filter Screen.....	131
Figure 68: Combination Filters Screen.....	133
Figure 69: IP DataFlow List Screen.....	138
Figure 70: IP DataFlow Add Screen.....	139
Figure 71: Traffic Classifications Screen.....	141
Figure 72: Traffic Classifications Selector Screen.....	141
Figure 73: Alarms Configuration Screen.....	143
Figure 74: IXP Subsystem Overview.....	146
Figure 75: Subsystem Pop-Up Menu.....	147
Figure 76: Archived List Of Configurations.....	150
Figure 77: Discovery Results Screen.....	151
Figure 78: Server Role Change Screen.....	152

Figure 79: Storage Server Object and List Table.....	152
Figure 80: Add Screen.....	153
Figure 81: Streams List.....	155
Figure 82: Add Streams Screen.....	156
Figure 83: Stream Modify Screen.....	158
Figure 84: Dataflow Processings List.....	160
Figure 85: xDR Dataflow Assistant Inital Screen-PDU Sources.....	162
Figure 86: Dataflow Assistant Xdr Builder Selection.....	163
Figure 87: Xdr Assistant - Enrichment Selection.....	163
Figure 88: xDR Assistant - Configuring Sessions Screen.....	164
Figure 101: Add Screen.....	172
Figure 102: Dataflow Building Screen.....	172
Figure 103: Dataflow Input PDU Tab (PDU Dataflows selected).....	173
Figure 98: Input PDU Tab (PDU Streams selected if working with external PDU streams).....	170
Figure 104: Xdr Builders Tab.....	173
Figure 105: Parameters Tab (with SS7, GPRS, IP and Misc xDR Builders selected).....	174
Figure 101: Add Screen.....	172
Figure 102: Dataflow Building Screen.....	172
Figure 103: Dataflow Input PDU Tab (PDU Dataflows selected).....	173
Figure 98: Input PDU Tab (PDU Streams selected if working with external PDU streams).....	170
Figure 104: xDR Builders Tab.....	173
Figure 105: Parameters Tab Showing SS7 ISUP ANSI CDR Tab	174
Figure 101: Add Screen.....	172
Figure 102: Dataflow Building Screen.....	172
Figure 103: Dataflow Input PDU Tab (PDU Dataflows selected).....	173
Figure 104: xDR Builders Tab with VOIP SIP Builders Selected.....	173
Figure 105: Parameters Tab with VoIP SIP-T ANSI CDR Tab.....	174
Figure 106: VoIP SIP with Answer selected.....	174
Figure 118: Add Screen.....	183
Figure 119: Input Streams Screen.....	184
Figure 120: xDR Filter Screen.....	184
Figure 110: xDR Filter Screen.....	176
Figure 111: xDR Filter Screen with condition.....	177
Figure 112: Add Dataflow Processing Screen.....	178
Figure 113: IP Streams Screen.....	178
Figure 114: Xdr Filters Screen.....	179
Figure 115: Output Steams Screen.....	180
Figure 116: Enrichment Screen.....	181
Figure 117: Xdr Operation Screen.....	182

Figure 118: Add Screen.....	183
Figure 119: Input Streams Screen.....	184
Figure 120: xDR Filter Screen.....	184
Figure 121: xDR Storage Screen.....	184
Figure 122: Xdr Builder List Screen.....	185
Figure 123: Add Sessions Screen.....	186
Figure 124: Completed Session In Session List.....	187
Figure 125: Selected Session For Modification.....	187
Figure 126: Create Session Screen.....	188
Figure 127: Completed Xdr Session Screen.....	189
Figure 128: Added Session In Xdr Storage Screen.....	190
Figure 129: Q.752 Processing List Screen.....	192
Figure 130: Inputs Screen (PDU Streams Tab).....	193
Figure 131: Inputs Screen (PDU Dataflows Tab).....	193
Figure 132: General Parameters Screen.....	193
Figure 133: SSN Filter Screen.....	194
Figure 134: Linkset Filters Tab.....	194
Figure 135: Distribution List.....	195
Figure 136: Software List Screen.....	195
Figure 137: Subsystem Preferences List Screen.....	196
Figure 138: Subsystem Preferences List Screen.....	197
Figure 139: Dictionary List Screen.....	199
Figure 140: Add Dictionary Screen.....	200
Figure 141: Modify Dictionary - Dictionary Info Tab.....	201
Figure 142: Modify Dictionary - Dictionary Attribute Info Tab.....	202
Figure 143: Dictionary List Screen.....	204
Figure 144: Dictionary List Screen.....	204
Figure 145: Dictionary List with Unused Dictionary Selected.....	205
Figure 146: Unused Dictionary Discrepancy Report.....	206
Figure 147: Xdr Filter List Screen.....	206
Figure 148: Xdr Filter Add Screen.....	207
Figure 149: Filter Definition Screen.....	207
Figure 150: Added Xdr Filter To List.....	208
Figure 151: xDR Sessions List Screen.....	209
Figure 152: xDR Session Add Screen.....	211
Figure 153: Completed Session In Session List.....	212
Figure 154: Selected Session For Modification.....	212
Figure 155: Modify Session Screen.....	212
Figure 156: Xdr Session Filter Icon.....	214
Figure 157: Modify Session Backup Toolbar.....	214
Figure 158: Sessions List.....	215

Figure 159: Associate Dictionary Screen.....	215
Figure 160: Enrichment Files List Screen.....	216
Figure 161: Xdr Session Add Screen.....	216
Figure 162: Source Code Screen.....	217

List of Tables

Table 1: Time Tab Screen.....	18
Table 2: Directory Tab Field Description.....	18
Table 3: Mapping Tab.....	19
Table 4: Point Code Tab.....	20
Table 5: CIC Tab Field Descriptions.....	20
Table 6: Default Period Tab Field Descriptions.....	21
Table 7: Site Configuration.....	45
Table 8: Host Configuration.....	46
Table 9: Node Configuration.....	46
Table 10: SS7 Signaling Point Configuration.....	46
Table 11: Gb Signaling Point Configuration.....	47
Table 12: Linkset Configuration.....	47
Table 13: SS7 Link Configuration.....	48
Table 14: Gb Link Configurations.....	49
Table 15: PMF Card Configuration.....	49
Table 16: PMF Port Configuration.....	49
Table 17: PMF Port Assignment Configuration.....	50
Table 18: IP Address Filter Configuration.....	54
Table 19: IP Port Filter Configuration.....	54
Table 20: VLAN Filter Configuration.....	54
Table 21: IP Combo Filter Configuration.....	55
Table 22: IXP Subsystem Add Screen Field Descriptions.....	67
Table 23: IXP Storage Server States.....	72
Table 24: IXP Server Designations.....	72
Table 25: IXP Subsystem Add Screen.....	73
Table 26: xMF Subsystem Add Screen Field Descriptions.....	76
Table 27: Add Node Screen.....	81
Table 28: Link Network View Fields.....	98
Table 29: IP Stream Selector Filter Fields.....	99
Table 30: PMF Subsystem Pop-Up Menu Options.....	147
Table 31: Ranges for Pre-defined Subsystem Parameters.....	106
Table 32: Threshold Values.....	109
Table 33: Traffic Classification Fields.....	113
Table 34: Add / Modify Port Filter Screen Fields.....	124
Table 35: IP Filter Screen Fields.....	124
Table 36: Port Filter Screen Fields.....	127
Table 37: VLAN Filter Screen Fields.....	129

Table 38: Add SAPI Filter for GP over IP Screen Fields.....	131
Table 39: Combination Filter Screen Fields.....	133
Table 40: Diameter Filter Screen Fields.....	136
Table 41: Add / Modify IP DataFlow Screen Fields.....	139
Table 42: IXP Subsystem Pop-Up Menu Options.....	147
Table 43: Storage Pool Server States.....	153
Table 44: Values Associated with each State	154
Table 45: NSP Applications Effected by Each State.....	154
Table 46: Dataflow Processings List Table.....	160
Table 47: Dataflow Processing Naming Conventions.....	161
Table 48: Xdr Builder List Descriptions.....	185
Table 49: Xdr Table Layout.....	210
Table 50: xDR Tool Bar.....	210
Table 51: Add Policies Screen Field Descriptions.....	220
Table 52: Initial Step Screen.....	228
Table 53: Initial Step Screen.....	229

Chapter 1

About This Help Text

Topics:

- *Overview.....16*
- *Scope and Audience.....16*
- *About the Diameter Intelligence Hub (DIH).....16*
- *Customer Care Center.....21*
- *DIH Documentation Library.....24*
- *Locate Product Documentation on the Customer Support Site.....24*
- *Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents.....25*

Overview

The Diameter Intelligence Hub (DIH) system monitors a network to collect PDUs for correlation and storage. The Centralized Configuration Manager (CCM) is a management application for configuring the DIH system so that these PDUs can be utilized in different ways by the Network Software Platform (NSP) applications such as ProTrace and Data Feed Export.

A typical DIH system consists of computer servers and data storage systems that are connected to each other over an IP network. The computer systems that collect, process and store data are located in the premises of the service provider that contains the switching, signaling and routing equipment. These provider locations are referred to as sites.

DIH web-based applications, such as CCM, are hosted by a cluster of application servers located at the customer's Network Operations Center (NOC). CCM enables system administrators to configure the system using the following principles:

- Administration from a single point - all system administration tasks are performed from the system administration console.
- Administration utilizing a global view - the system administrator provisions the system as a single logical entity. The centralized configuration is automatically propagated to the appropriate servers where applications share common data.
- Multi-user access - the system allows multiple users to provision simultaneously.

Scope and Audience

This guide is designed to assist the NSPConfigManager and NSPAdministrator in working with the Centralized Configuration Manager administration application. Users should find the information they need to cover important activities required to manage Data Feed Export.

About the Diameter Intelligence Hub (DIH)

The Diameter Intelligent Hub (DIH) is used to monitor a LTE network. DIH also creates a small hardware "footprint" for customers who administer 3G and 4G diameter networks. The DIH:

- Is a single blade server and storage blade collocated within a single or dual Diameter Signaling Router (DSR) enclosure(s).
- Provides filtering, data feed, tracing, decoding, and SNMP functions.
- Enables the selective collection and storage of diameter traffic within one or more instances of PMF and IXP.
- Provides nodal diameter troubleshooting.
- Provides data export for diameter messages.
- Supports both IPv4 and IPv6 traffic simultaneously.
- Provides KPI tracking using ProTrace application as well as viewing KPIs in graphic format using ProPerf dashboard configured at installation.
- Provides filtering for alarms using ProTraQ Cell filter (see system alarms online help).

- Uses diameter protocol exclusively.

Note: The DIH system can use other protocols if the Diameter mode has not been selected and system is in Standard mode. (Default setting is Standard mode. For more information on selecting Diameter mode, see Centralized Configuration Manager Administration online help, "Setting System to Diameter Mode."

The Diameter Protocol

The diameter protocol has evolved from the Radius protocol and enables diameter applications to extend the base protocol by adding new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP).

The diameter protocol provides for an Authentication, Authorization, and Accounting (AAA) framework that overcomes the limitations of RADIUS, (a protocol that handles AAA and EAP), which cannot effectively deal well with remote access, IP mobility and policy control. The Diameter protocol defines a policy protocol used by clients to perform Policy, AAA and Resource Control. This allows a single server to handle policies for many services.

As mentioned above, Diameter protocol provides AAA functionality, but in addition it is made more reliable by using TCP and SCTP instead of UDP. The Diameter protocol is further enhanced by the development of the 3rd Generation Partnership Project (3GPP) IP Multimedia Subsystem (IMS). Through the use of extensions, the protocol was designed to be extensible to support Proxies, Brokers, Strong Security, Mobile-IP, Network Access Servers (NASREQ), Accounting and Resource Management.

User Preferences

All applications that query xDRs, (or observe their status as in Diagnostic Utility), xDRs use a specific User Preferences option. The description outlined goes over the formatting screens.

Note: All screen shots presented here show default values.

Date/Time tab screen

Format the time parameters.

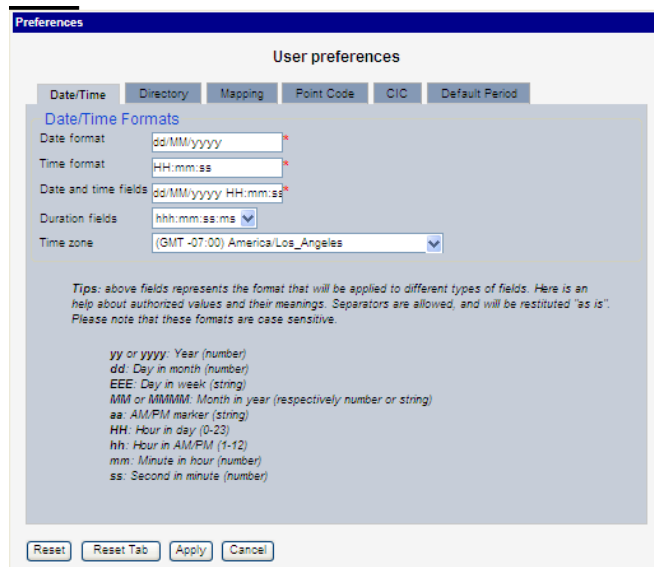


Figure 1: Date/Time Tab Screen

Table 1: Time Tab Screen

Field	Description
Date Format	Required field - Sets date format.
Time Format	Required field - Sets time format.
Date and time fields	Required field - Sets the date and time format.
Duration fields	Sets a duration format.
Time Zone	Pull-down list for selecting the desired time zone.
Reset Button	Resets all the tabs to default values.
Reset Tab Button	Resets to default values for the specific tab.
Apply Button	Applies any changes to the system.
Cancel Button	Exits the screen.

Directory tab

Select the **Directory** tab to set the defaults directories used in transport screen.

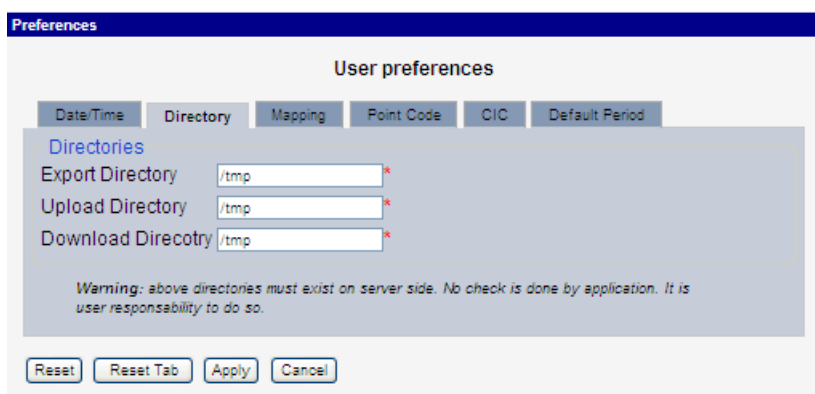


Figure 2: Directory Tab Screen

Table 2: Directory Tab Field Description

Field	Description
Export Directory	Enables you to set the default directory for exporting.
Upload Directory	Enables you to set the default directory for uploads.
Download Directory	Enables you to set the default directory for downloads.
Reset Button	Resets all the tabs to default values.
Reset Tab Button	Resets to default values for the specific tab.
Apply Button	Applies any changes to the system.
Cancel Button	Exits the screen.

Note: The directories must be present on the NSP server side. See warning at the bottom of the Directory tab screen.

Mapping tab

Select the **Mapping** tab to set the xDR display parameters.

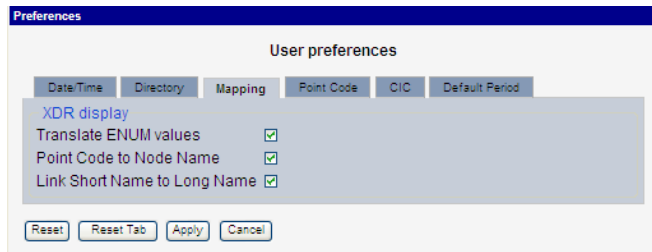


Figure 3: Mapping Tab Screen

Table 3: Mapping Tab

Field	Description
Translate ENUM values	Selects whether ENUM values are translated or not Default is to select ENUM values translation.
Point Code to Node Name	Select this if you want to use the Node Name instead of the Point Code name in the xDR display. Default is to use Node Name.
Link Short Name to Long Name	Selects whether you can use long name (Eagle) for linksets. Default is to use Long Name.
Reset Button	Resets all the tabs to default values.
Reset Tab Button	Resets to default values for the specific tab.
Apply Button	Applies any changes to the system.
Cancel Button	Exits the screen.

Point Code tab

Select the **Point Code** tab, shown and described in the figure and table.

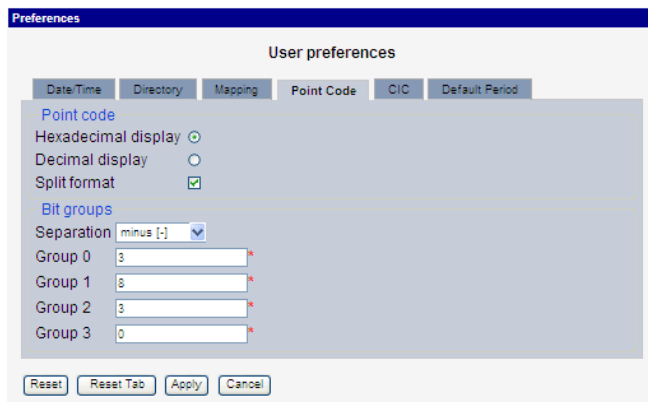


Figure 4: Point Code Tab Screen

Table 4: Point Code Tab

Field	Description
Hexadecimal display	European defaults are hexadecimal and display with Group 0-3, Group 1-8, Group 2-3, Group 3-0.
Decimal display	North American defaults are decimal and display with Group 0-7 and Group 1-5.
Split format	Select or deselect Split format .
Separation	Select a Bit Group Separation .
Group 0	Type a value. (0-7 or 1-5 see hexadecimal or decimal display)
Group 1	Type a value. (0-7 or 1-5 see hexadecimal or decimal display)
Group 2	Type a value. (0-7 or 1-5 see hexadecimal or decimal display)
Group 3	Type a value. (0-7 or 1-5 see hexadecimal or decimal display)
Reset Button	Resets all the tabs to default values.
Reset Tab Button	Resets to default values for the specific tab.
Apply Button	Applies any changes to the system.
Cancel Button	Exits the screen.

CIC tab

Select the **CIC** tab to set the parameters for CIC and Bit groups.

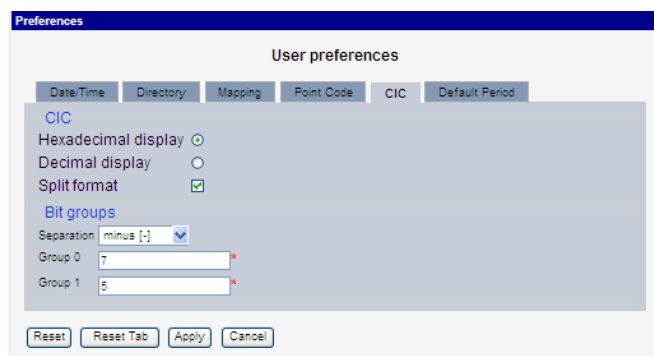


Figure 5: Formatting Rules (CIC) Screen

Table 5: CIC Tab Field Descriptions

Field	Description
Hexadecimal display	European defaults are hexadecimal and display with Group 0-7 and Group 1-5.
Decimal display	European defaults are hexadecimal and display with Group 0-7 and Group 1-5.

Field	Description
Split format	Select or deselect Split format .
Separation	Select a Bit Group Separation : Group 0:8, Group 1:8 .
Group 0	Type a value. (0-7 or 1-5 see hexadecimal or decimal display)
Group 1	Type a value. (0-7 or 1-5 see hexadecimal or decimal display)
Reset Button	Resets all the tabs to default values.
Reset Tab Button	Resets to default values for the specific tab.
Apply Button	Applies any changes to the system.
Cancel Button	Exits the screen.

Default Period tab

Select the **Default Period** tab, for setting the default time period for beginning and ending time for traces (ProTrace only) .

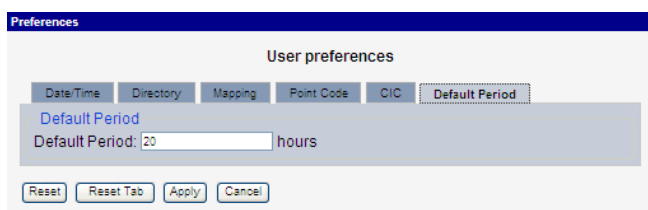


Figure 6: Default Period Tab Screen (ProTrace only)

Table 6: Default Period Tab Field Descriptions

Field	Description
Default Period (in hours)	Sets the default run time period for running traces. Default is 24 hours. Range 1-7200
Reset Button	Resets all the tabs to default values.
Reset Tab Button	Resets to default values for the specific tab.
Apply Button	Applies any changes to the system.
Cancel Button	Exits the screen.

After setting the formatting parameters, click **Next** to move to the next screen in the wizard.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your

requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

Phone:

1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

Phone:

USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

Phone:

0-800-555-5246 (toll-free)

- **Brazil**

Phone:

0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:

8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

Phone:

1230-020-555-5468

- **Colombia**

Phone:

01-800-912-0537

- **Dominican Republic**

Phone:

1-888-367-8552

- **Mexico**

Phone:

001-888-367-8552

- **Peru**

Phone:

0800-53-087

- **Puerto Rico**

Phone:

1-888-367-8552 (1-888-FOR-TKLC)

- **Venezuela**

Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

Regional Office Hours:

8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Signaling**

Phone:

+44 1784 467 804 (within UK)

- **Software Solutions**

Phone:

+33 3 89 33 54 00

- **Asia**

- **India**

Phone:

+91 124 436 8552 or +91 124 436 8553

TAC Regional Support Office Hours:

10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

- **Singapore**

Phone:

+65 6796 2288

TAC Regional Support Office Hours:

9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

DIH Documentation Library

DIH customer documentation and online help are created whenever significant changes are made that affect system operation or configuration. Revised editions of the documentation and online help are distributed and installed on the customer system. Consult your NSP Installation Manual for details on how to update user documentation. Additionally, a Release Notice is distributed on the Tekelec Customer Support site along with each new release of software. A Release Notice lists the PRs that have been resolved in the current release and the PRs that are known to exist in the current release.

Listed is the entire DIH documentation library of online help.

- Centralized Configuration Manager Administration Online Help
- Alarm Forwarding Administration Online Help
- Diagnostic Utility Administration Online Help
- ProTrace Online Help
- System Alarms Online Help
- ProPerf Online Help
- ProTraq Configuration Online Help
- Data Feed Export Online Help
- Quick Start Online Help
- System Alarms Online Help

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the [Tekelec Customer Support](#) site.

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents

© 2012 Tekelec

All Rights Reserved

Printed in U.S.A.

Notice

Information in this documentation is subject to change without notice. Unauthorized use, copying, or translation of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced, translated, or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks

TEKELEC, EAGLE, G-Flex, G-Port, and CAMIANT are registered trademarks of Tekelec. The Tekelec logo, A-Port, EAGLE 5, EAGLE 5 ISS, IP7, IP7 Secure Gateway, V-Flex, ngHLR, BLUESLICE, and Subscriber Data Server (SDS) are trademarks of Tekelec. All other trademarks are the property of their respective owners.

Patents

This product may be covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:

6,456,845; 6,765,990; 6,968,048; 7,043,001; 7,155,512; 7,206,394; 7,215,748; 7,231,024; 7,286,516; 7,286,647; 7,401,360; 7,706,343; 7,844,033; 7,860,799;

Foreign Patent Numbers:

None.

Chapter 2

CCM Overview

Topics:

- [CCM Overview.....27](#)

CCM Overview

Centralized Configuration Manager (CCM) is developed to consolidate all configuration data (PMF and IXP) into a single database. The common network-wide configuration is used to enhance the capabilities of NSP applications such as ProTrace and Data Feed Export. The monitoring features of PMF and IXP are addressed separately by the NSP application called Diagnostic Utility.

Chapter 3

Key Concepts

Topics:

- *PMF IP Data Acquisition.....29*
- *Monitored Network Elements.....29*
- *About PDU Collection.....29*
- *PDU Routing and Filtering.....30*
- *About xDR Generation.....32*
- *About xDR Data Feeds.....32*
- *About Network Views.....32*
- *About Security and Permissions.....33*
- *About Equipment Registry.....33*

PMF IP Data Acquisition

PMF IP data acquisition comprises three general steps. They are:

1. PMF acquires MSUs that match a filter from the IP tap and timestamps them
2. PMF processes the MSUs and filters them for delivery to an IXP
3. The IXP processes the MSUs for storage, xDR correlation and KPIs

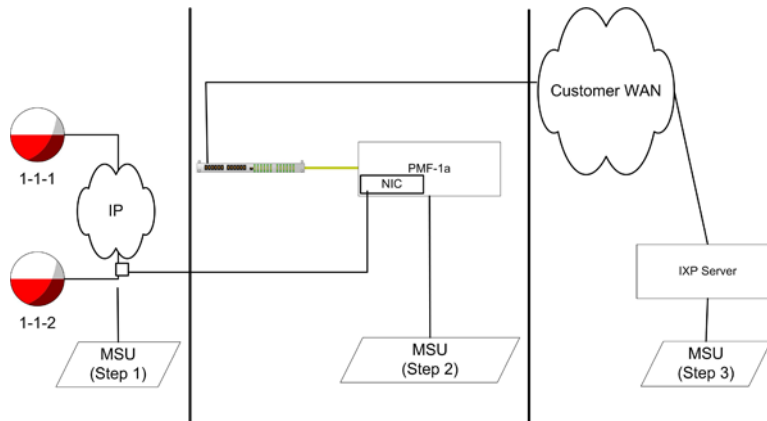


Figure 7: Pmf Ip Data Acquisition Sequence

Monitored Network Elements

The term, Network Elements, refers to customer network IP elements. These elements are divided into:

- Node Elements - elements that are contained in IP nodes.
- Non-node Elements - IP elements such as:
 - Signaling Points
 - IP cards
 - Application servers (ASP)
 - Application Server Processes (ASP)

Because network elements are so fundamental to the rest of the provisioning process, it is recommended that they be setup right after a site has been created.

About PDU Collection

In the DIH system PMF monitors and collects PDUs exchanged between nodes.

PDU Collection on PMF IP Networks

For collecting PDUs from IP networks perform the following actions:

1. Select a NIC card on a specific PMF server
2. Create IP link(s) to be monitored by each NIC port
3. Assign these links to a monitoring port on a specific PMF server
4. Create a link network view and choose an IP link
5. Create an IP dataflow
6. Assign the link network view to the IP dataflow
7. Route the assigned PDU dataflows to input streams on IXP

PDU Routing and Filtering

The PDUs collected by the data collectors must be routed to one or more xDR builders for creating xDR records. These routes are configured using CCM.

There are some important considerations in configuring PDU routes.

- Not all PDUs need to be sent to an xDR builder, therefore, a data collector allows filters to be applied to the PDUs it receives.
- A PDU can be routed to multiple xDR builders for building different types of xDR records. (See PMF IP Data Acquisition Sequence.)
- An xDR builder needs to receive related PDUs that can be converted into an xDR record. For example, in order for the xDR builder to create an ISUP CDR, it needs to receive all the PDUs associated with a call (IAM, ACM, ANM, REL, RLC). (See PMF IP Data Acquisition Sequence.) At the same time, the xDR processing can be distributed across multiple xDR builders for load sharing (see CCM About Distributions). The routing must be configured to support such grouping. This is often the most complex configuration task.
- There is a resource “cost” to routing PDUs to the xDR builders if the data collectors and the xDR builders are at different geographical locations and WAN resources have to be used. While routing, consider minimizing WAN traffic by routing PDUs to local xDR builders or routing over a least-cost route.

Note: The resource cost is bandwidth usage and therefore to conserve bandwidth you can use filtering.

For more details on these important considerations, see CCM About the xDR Dataflow Assistant. For details on data flow procedures see CCM topic Configuring Dataflow Processings.

The following sections describe the logical constructs you use to configure the routes between the data collector and xDR builders for generating the xDRs required for NSP applications.

About Traffic Classification Filtering

Input streams enable IP traffic to be classified, (using filtering), from one or more NIC ports into streams of data. A stream is created on a group of NIC ports by defining an IP filter. After input streams are configured, if a received PDU does not match any of the filtering criteria, it is discarded.

Note: Because of the large volume of IP traffic, it is a common practice to discard unnecessary PDUs at the data collector level for IP networks.

About IP Dataflows

An IP dataflow routes PDUs from an IP stream to IXPs.

About Dataflows

A dataflow provides a way to filter and route MSUs.

Dataflows Versus IP Streams

A dataflow is similar to an IP stream because it allows SS7 and Gb traffic to be filtered. A dataflow has a filter that is applied to a group of SS7 linksets or Gb links (instead of NIC ports in case of input streams). In the case of IP traffic, an IP dataflow is basically a "pass through" in terms of filtering. Dataflows are also used to configure additional routing information.

An IP stream is very similar, in concept, to a dataflow because applies filters to classify traffic. The difference is that for input streams, the classification is performed as soon as a PDU is received by a PMF. For dataflows, the classification is done after the data has been received by PMF and then stored. The reason for this difference is that the volume of IP traffic is much larger and it is more efficient to discard unnecessary PDUs rather than storing them and discarding them later.

About Data Transport Service (DTS)

Routing data from PMF to IXP uses Data Transport Service (DTS) exclusively. Input streams are created on IXP to route the dataflow from the xMF.

All the streams created on the IXP subsystems can be viewed in the PDU dataflow routing screen.

PDU dataflows are also routed to one or more input streams. The PDU dataflow defines the criteria (linkset/links and filters) for PDUs to be sent for correlation. The input streams provide the interface for the IXP to receive the flow of PDUs.

About Input Streams

Input streams, (for more information, see topics About Dataflows and About Streams, are constructs for grouping dataflows for the purpose of routing to one or more xDR builders. The grouping is done so that PDUs belonging to a dataflow are routed over a single communication stream to an xDR generator, resulting in optimized data collection resources.

CCM supports both Message Feeder Protocol (legacy applications only) and Data Transport Service.

When using DTS, the IXP pulls data from a datasource (an IP address and port on PMF).

Note: An IXP subsystem has a limit of 255 input streams. IXP also uses four input streams for monitoring purposes, so the functional limit is 251. If this limit is exceeded, then CCM produces an error message stating that the limit has been exceeded. If this happens, streams will have to be routed differently to keep within the limit.

About Routing

Is the process of routing dataflows to IXP input streams.

About xDR Generation

xDR builder configurations are managed by CCM in the *Mediation* perspective. The details of the xDR builder use and configuration are outlined in the *Mediation* perspective.

About Sessions and Dictionaries

Once xDR generation is configured for a builder, xDR records are stored in a session. A session is associated with a dictionary. The dictionary mechanism is a way of describing the content of the xDR fields. NSP applications, such as ProTrace use the dictionary to access and display the data making the applications independent of the xDR record format.

The IXP and Data Server (legacy) applications provide a mechanism for CCM to discover sessions and dictionaries. Once discovered, the sessions can be accessed by NSP applications such as ProTrace.

Note: A session name must be unique for each IXP subsystem or dataserver, but sessions can have identical names if they reside on separate IXP subsystems.

About xDR Data Feeds

DIP supports exporting of xDRs to third-party applications. This function is referred to as a data feed export. All data feeds are configured by using the Data Feed Export application. For more information on data feeds, see the Data Feed Export User Guide.

About Network Views

Network views are logical, user-defined groupings of elements in an DIH system. The term network view is used to denote some aspect, or perspective, of a customer network. For example, it could be the physical elements comprising a network, or a sub-network, or another carrier's network or a certain type of traffic on the network.

Network views can be nested in hierarchical order and contain other network views (children) that themselves may contain network views and so on depending on how large or complex the network is.

Grouping elements together into network views enables you to divide up the network into more manageable units, not only for convenience, (elements in a network view can be referred to from other parts of the system as a single unit, by referring to the network view), but also for authorization purposes. For example, you can create a network view that only shows certain application users a subset of the total data and this is managed by assigning users rights (privacy settings) to specific

network views . Network views are designed to be the primary mechanism in the DIH system to select a dataset. Applications like ProTrace use network views.

The types of elements that can be grouped together into a network view include PDU sources such as Input streams or xDR sessions. There are two types of network views:

- Session-based network views - xDR sessions can be grouped together to create a view of the network. The ProTrace application uses session-based network views for filtering and call tracing.
- Link-based network views - links (IP) can be grouped together to create a view of the network. This type of network view is used for associating linksets, links, and Input streams to PDU dataflows. The ProTrace also uses link-based network views for filtering and call tracing.

About Security and Permissions

NSP comes with a security and privacy module, (see NSP Security User Guide for more information), that enables objects, such as network views, that are a part of the NSP system to be protected. Each of these objects has an owner and the owner can set the privacy level so that users who belong to specified user groups can have read, write and/or execute privileges on an object(s).

CCM enables an owner to create and modify objects. It also allows the owner of an object to set the privacy of that object. When an object is created or discovered, the user who created or discovered the object becomes the owner of that object and can assign privacy privileges for that object and can set the level of access for other users, or groups of users using that object.

About Equipment Registry

The DIH system is comprised of many applications that are running in a distributed environment. These applications need to be configured for them to perform their functions. Applications are created, discovered and configured using the Equipment Registry perspective.

The principle elements in equipment registry are:

- Sites
- Subsystems (PMF)
- Hosts

About Sites

Sites represent logical locations where a DIH application is located. A DIH application either runs on a single server or it may be distributed over a group of servers (referred to as a subsystem). Sites are defined using CCM.

When creating a site, follow this guideline:

- There can be, at most, one PMF subsystem for a given site along with one IXP subsystem. Depending on the configuration DIH can have a maximum of 2 sites with one PMF and one IXP per site.

About Hosts

A host refers to a server that runs an DIH application. For each DIH server in a site, there is a host in CCM, therefore, allowing one site to contain multiple hosts.

About Subsystems

Some DIH applications are stand-alone and some are clustered. A stand-alone application has only one instance running on one host. Examples of stand-alone applications include ICP and Data Server (legacy systems). Some of the DIH applications run in more than one server or cluster, but to the outside world they behave as a single entity. A cluster of application instances is referred to as a subsystem. Examples of applications that run as subsystems include:

- PMF
- IXP
- DWH

About Server Roles

Primary and secondary roles are not assigned to the servers in the xMF subsystems anymore. Server roles are made transparent to the user and server role changes are also automatic. For an IXP subsystem, the CCM assigns the primary role to server 1a and secondary role to server 1b. The rest of the servers are assigned ancillary roles.

When you discover the first application that belongs to the subsystem, that application is automatically designated as the primary application, and a subsystem entry is automatically created in the system. When subsequent applications are discovered, the applications are designated as backup and ancillary respectively.

Chapter 4

Using CCM

Topics:

- *About CCM.....36*
- *Logging into NSP.....36*
- *Opening CCM.....37*
- *Understanding the CCM Screen.....37*

About CCM

This chapter provides a general overview of CCM. The topics covered are:

- Logging into CCM
- Understanding the CCM user interface

Logging into NSP

Complete these steps to log into NSP.

1. Using a Web browser, type the following URL: `http://nspserver_IPAddress/nsp`

Note: Contact your system administrator to find out the IP Address for NSP portal.

Note: NSP only supports versions of IE 7.0 or later and Firefox 3.6 or later. Before using NSP, turn off the browser pop up blocker for the NSP site.

The *login* screen opens shown below.

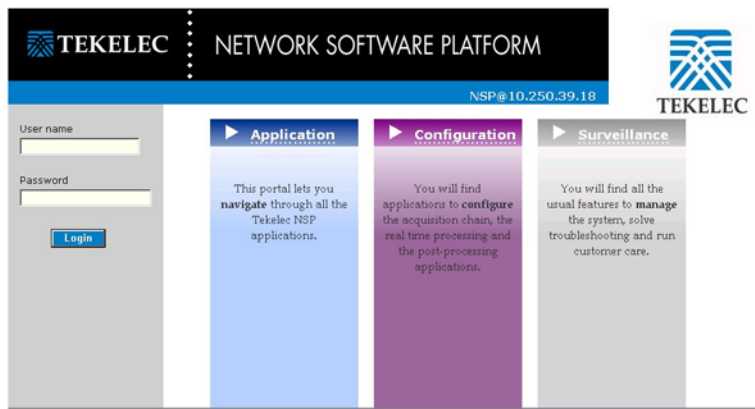


Figure 8: NSP Portal Screen

2. Log into NSP by typing :
 - a) **Your Userid**
 - b) **Your Password**

Note: Check with your system administrator for your userid and password.

The NSP *Application Board* opens with a top frame and a screen presenting all currently deployed applications.

Opening CCM

To open an application, Complete these steps:

Click the **CCM** icon located in the Configuration Section of the Portal Screen.

The CCM Home screen opens.

The screen is divided into two main sections:

- a) Menu Tree - located on the left-hand section shows the three main perspectives and enables you to utilize any of the six perspectives.

The six perspectives are:

- Equipment Registry
- Network Elements
- Network Views
- Acquisition (PMF)
- Mediation (IXP)
- Monitoring Policies

- b) Screen body- on the *Home* screen provides links for viewing a variety of elements and functions.

The major heading for elements and functions are:

- Network Elements
- Network views
- xDR-Related Elements
- Bulk Load Configurations
- Reports
- Thirdparty
- Configure Alarm Severity
- Auto Synchronization

Note: Each of the elements in these headings is described separately and also may not be functional in this DIH release.

Understanding the CCM Screen

This section provides a brief overview of the screen elements for *CCM*. For more detailed information NSP screen elements such as the toolbar and function buttons.

Note: Do not use the Function Keys (F1 through F12) when using the NSP. Function keys work in unexpected ways. For example, the F1 key will not open NSP help but will open help for the browser in use. The F5 key will not refresh a specific screen, but will refresh the entire session and will result in a loss of any entered information.

About Tool bar and Right-click Menu Functions

The section describes the list screen and pop-up menu that have similar toolbar functionality. The functionality is divided into three sections:

- Buttons
- Column functions
- Right-click menu options from the element list

Buttons and Pop-up Menus

Buttons are located either on a List screen toolbar or on the right click pop-up menu in the element section. They are:

Note: Not all tool bar button functions appear in the pop-up menus. Pop-up menu is specifically for the element. The tool bar buttons are general functions for that screen such as first record, next record, previous record, etc.

- First record - enables you to move to the first record
- Next record - enables you to move to the next record
- Previous record - enables you to move to the previous record
- Last record - enables you to move to the last record
- Add - enables you to add a record
- Modify - enables you to modify the selected record
- Delete - enables you to delete the selected record
- Search - enables you to search for a specific record
- Synchronize/Discover - enables you to either discover new applications or synchronize the subsystem after any changes

Note: Do not use the Function Keys (F1 through F12) when using the NSP. Function keys work in unexpected ways. For example, the **F1** key will not open NSP help but will open help for the browser in use. The **F5** key will not refresh a specific screen, but will refresh the entire session and will result in a loss of any entered information.

Right Click Pop-up Menus

Right clicking on an element opens the pop-up menu for that specific element. For example, right clicking on the Sites element in the Equipment Registry perspective opens the pop-up menu that has options such as: Add, Modify, Delete, List and Refresh. Right clicking on the Sites element in the Mediation perspective opens the pop-up menu just shows Refresh.

Column Functions

The column functions enable you to perform the following actions:

Each column can be sorted by ascending or descending order

Each column can be moved to a different order within the screen to facilitate reading and searching for specific records. This action is accomplished through the Select Columns button.

Note: The Select Columns button also enables you to view or hide columns on a screen.

Chapter 5

Home Screen Operations

Topics:

- *About CCM Home Page Operations.....40*
- *Network Elements.....40*
- *Network View Lists.....41*
- *xDR-Related Elements.....42*
- *Bulk Load.....44*
- *Bulk Loading Process.....45*
- *Exporting Bulk Load Configurations.....56*
- *Creating a Configuration Report.....57*
- *Setting the Severity of Platform Alarms.....58*

About CCM Home Page Operations

One of the perspectives that CCM provides is a global listing functionality on its Home screen. These links enable you to view the objects listed below as you would view them using the NSP legacy application system configuration. In addition to these views, there is also a Bulk Load and Reports functionality. The areas covered in this chapter are:

- Network Elements
- Network Views
- xDR-Related Elements
- Bulk Load (Import and Export)
- Reports (Creating a Configuration Report)
- Thirdparty (Linking with external applications)
- Alarm Severity Configuration

Network Elements

The SS7 Analytic Report uses network elements provisioned by the customer in the Central Configuration Management (CCM) application. CCM provides links for a global listing of the following SS7, GPRS and IP network elements:

- SS7 Nodes
- GPRS Nodes
- IP Nodes
- SS7 Signaling Points
- SS7 Linksets
- SS7 Links
- GPRS Signaling Points
- GPRS Gb Links
- IP Signaling Points

Nodes

The Home page lists each type of node separately to make searches easier and quicker. Clicking a the specific link provides a list of the specific node configured in your system along with their associated signaling points. Clicking the link opens the specific Node(s) List screen (SS7 Nodes list page is shown).

Note: The Home screen section shows the list of Nodes independently of the Object Tree on the left-hand section of the screen.

#	Node Name	Description of Node	Owner	State	Created	
<input type="checkbox"/>	1	Node sp_66-67-47-401		cja	N	23/07/2009 10:14:33
<input type="checkbox"/>	2	KenzNode		tekelec	N	27/07/2009 13:42:02
<input type="checkbox"/>	3	Eagle MercurySTP		tekelec	N	20/07/2009 11:34:10
<input type="checkbox"/>	4	Node sp_1-1-101-401		tekelec	N	20/07/2009 11:34:10
<input type="checkbox"/>	5	Node sp_1-1-151-401		tekelec	N	20/07/2009 11:34:11
<input type="checkbox"/>	6	Node sp_66-67-40-401		tekelec	N	20/07/2009 12:11:11
<input type="checkbox"/>	7	Node sp_66-67-41-401		tekelec	N	20/07/2009 12:11:11
<input type="checkbox"/>	8	Node sp_3-28-2-401		tekelec	N	20/08/2009 07:47:18

SS7 Signalling Points list for Node **Node sp_66-67-47-401**

#	SP	Description	Node Name	Code	Flavour Country	Flavour Format	OID
<input type="checkbox"/>	1	sp_66-67-47-401	Node sp_66-67-47-401	66-67-47	ANSI-SS7	8-8-8	.1.3.6.1

Figure 9: SS7 Node(s) List Screen

From this screen you can: add, modify, delete and show details of any selected Node as well as refreshing the screen to view any changes that have occurred to the Node records.

IP Signaling Point List Screen

The IP signaling point list screen provides a list of IP signaling points configured in your system. The IP signaling point list screen is shown below.

#	SP	Description	Node Name	IP Id	OID	Owner	State	Created
<input type="checkbox"/>	1	sp_66-67-47-401	Node sp_66-67-47-401					

Figure 10: IP Signaling Point List Screen

Network View Lists

The CCM Home screen provides links for a global listing of the following network views:

- Session Views
- Link Views

These links provide a complete list of these elements.

Session Views

The Network Session Views link provides a list of ALL the sessions configured in your system. Clicking the link opens the Network Session(s) List screen.

Note: In the Home screen, the Network Sessions section shows the list of Network Sessions independently of the Object Tree on the left-hand section of the screen.

#	Session	Type	Format	Dictionary	Subsystem Name	Lifetime	Sequence ID
1	BVT_SESSION	RECONSTITUTION	SINGLE	SS7 ISUP ANSI CDR_2,6,0	ixp0888_Pool	72	Disabled
2	test_phl_historical	STATISTICS	SINGLE	47702 test_phl_historical	ixp0888_Pool	840	Disabled
3	BSS_RANCC_11Aug1_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled
4	BSS_RANCC_11Aug2_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled
5	BSS_RANCC_PT3_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled
6	BSS_RANCC_PT_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled

Figure 11: Network Sessions List Screen

xDR-Related Elements

The CCM Homescreen provides links for a global listing of the following xDR-related elements:

- xDR Sessions
- Protocols
- Dictionaries
- Stacks
- PDU Hiding

These links provide a complete list of these elements. Each element is discussed separately.

xDR Sessions

The xDR sessions link provides a list of ALL the xDR sessions configured in your system. Clicking the link opens the Sessions present.

Note: The Home screen section shows the list of Sessions independently of the Object Tree on the left-hand section of the screen.

#	Session	Type	Format	Dictionary	Host	Lifetime
1	ISUPANSI_rec_140808	RECONSTITUTION	SINGLE	SS7 ISUP ANSI CDR_2,4,0	ixp1108-1a	72
2	ISUPANSI_cap_140808	CAPTURE	SINGLE	SS7 ISUP ANSI CDR_CAPTURE_2,4,0	ixp1108-1a	72
3	MGCP_TDR_rec_140808	RECONSTITUTION	SINGLE	VoIP MGCP TDR_1,6,1	ixp1108-1a	72
4	MGCP_CDR_cap_140808	CAPTURE	SINGLE	VoIP MGCP CDR_CAPTURE_1,1,2	ixp1108-1a	72
5	MGCP_CDR_rec_140808	RECONSTITUTION	SINGLE	VoIP MGCP CDR_1,1,2	ixp1108-1a	72

Figure 12: xDR Sessions List Screen

Protocols

The Protocols link provides a list of all the protocols present in your system. Clicking the link opens the list protocolslist screen

Note: The Home screen section shows the list of Sessions independently of the Object Tree on the left-hand section of the screen.

▲ Protocol	Version
AIN ANSI	
All	
BICC ANSI	
BICC ETSI	
BSSGP	
BTNUP	
CLASS ANSI	
GENERIC SUDR	
GPRS Gb	
GPRS Gn Gp	
GTP	
GTP-U	
IMS DIAMETER	
INAP	
INAP ETSI	
IP	
IP BGP	
IP DHCP	
IP DNS	
IP FTP	

Figure 13: Protocols Screen

Dictionaries

The Dictionaries link provides a list of all the dictionaries discovered in your system. Clicking the link opens the Dictionaries list screen.

Note: The Home screen section shows the list of dictionaries independently of the Object Tree on the left-hand section of the screen.

Records/Page 50 Page 1/4 Total Records: 160						
Dictionary Name	Type	Version	Protocol	Stack	Action	
1 15546 Stat SUP	STATISTICS	1.0.0	N/A	N/A		
2 15770 WWW	STATISTICS	1.0.0	N/A	N/A		
3 18536 SSSSS	STATISTICS	1.0.0	N/A	N/A		
4 19107 Test PI2002	STATISTICS	1.0.0	N/A	N/A		
5 20232 Test Stat2002	STATISTICS	1.0.0	N/A	N/A		

Figure 14: Dictionaries Present Screen

Stacks

The Stacks link provides a list of all the stacks in your system. Clicking the link opens the Stacks list screen.

Note: The Home screen section shows the PDU Hiding option. This option provides the ability to enable or disable the PDU decode hiding and PDU summary hiding for a specific protocol. Enabling PDU hiding will take away the ability to view the hexadecimal values (header of the decoding) and columns 1, 3 and 4 in the decode screen in ProTrace.

Stack	Path
ANSI	C:/Program Files/Steleus/Common/ProtocolLibrary/GenericStack/~Ansi.stk
ETSI	C:/Program Files/Steleus/Common/ProtocolLibrary/GenericStack/~Etsi.stk
GENERIC	C:/Program Files/Steleus/Common/ProtocolLibrary/GenericStack/~Generic.stk
N/A	N/A

Figure 15: Stacks List Screen

PDU Hiding

The Stacks link provides a list of all the stacks in your system. Clicking the link opens the Stacks list screen.

Note: The Home screen section shows the PDU Hiding option. This option provides the ability to enable or disable the PDU decode hiding and PDU summary hiding for a specific protocol. Enabling PDU hiding will take away the ability to view the hexadecimal values (header of the decoding) and columns 1, 3 and 4 in the decode screen in ProTrace.

Enabling or Disabling PDU Hiding

Complete these steps to enable or disable PDU hiding in ProTrace.

Note: This operation can only be performed by users with the role NSPAdministrator or NSPConfigManager.

1. From the Home Page, click **PDU Hiding**.
The PDU Hiding screen opens. The default setting is "enabled."
2. Select either **Enable PDU Hiding** or **Disable PDU Hiding** depending on the need.
3. Click **Apply** at the bottom of the screen.
The heading will signify what state the PDU hiding is in (enabled or disabled).
4. Click **Close**.

Bulk Load

CCM's Bulk Load process enables you to load PMF configurations offline without requiring PMF to be up and running.

After importing the configuration for the first time, you can also update the same configurations again. You take the export of the existing configuration and make the changes to this configuration in the CSV files generated. Re-importing the files updates the changes made to the files.

Note: To create a new object, the ObjectIDs will be "NA". This will signify whether it is a new insert or not. To update an object, the ObjectID should be NSP_ID (this can be generated through CSV export).

The bulk loading process supports the following file types:

- SSN filters
- DLCI filters

- IP Combination Filters
- IP filters
- Port filters
- VLAN filters
- PC filters
- Raw filters
- Diameter filters
- Sites
- Hosts
- Nodes
- PMF cards
- PMF ports
- PMF Port Assignments

These file types can be uploaded in any order.

Bulk Loading Process

The bulk load process file identifier (ID) is attached as a prefix to each record. Using the record identifier you can select different kinds of bulk loads in one file or separate them into multiple files.

Note: The order of the bulk load needs to be in the following order: Applications - ID Type 1 Network Elements - ID Type 2 or 3 Network Element Assignments to Applications - ID Type 4 or 5

PMF Element Configurations

These tables show the basic PMF element configurations needed when importing PMF subsystem configurations using the bulk load operations.

Table 7: Site Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		1		No	
2	Site ID	Number			No	
3	Name	String			Yes	30
4	Description	String		Yes	Yes	255

Table 8: Host Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		2		No	
2	Host ID	String			No	
3	HostName	String			Yes	30
4	Description	String		Yes	Yes	255
5	Frame	Number			Yes	
6	Position	Number			Yes	
7	Admin IP Address	String			Yes	30
8	Application Name	String			No	30
9	Application Description	String		Yes	Yes	255
10	Application Type	String	PMF-NG		No	
11	Site Name-ID	String			No	30

Table 9: Node Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		3			
2	NodeID	Number			No	
3	Name	String			Yes	80
4	Description	String		Yes	Yes	255
5	Type	String	SS7, IP, GPRS		No	255

Table 10: SS7 Signaling Point Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		4		No	

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
2	SPID	Number			No	
3	SP Name	String			Yes	30
4	Description	String		Yes	Yes	255
5	Flavor ID	Number			No	
6	Point Code	Number			No	
7	CLLI	String		Leave it blank for PMF	No	30
8	Node Name - ID	String			No	30
9	Site Name - ID	String		Leave it blank for PMF	No	30

Table 11: Gb Signaling Point Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		20		No	
2	SP ID	Number			No	
3	SP Name	String			Yes	30
4	Description	String		Yes	Yes	255
5	SGSN ID	Number			Yes	
6	NodeName - ID	String			No	30

Table 12: Linkset Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		5			
2	Linkset ID	Number			No	
3	Linkset Name	String			Yes	30
4	Description	String		Yes	Yes	255

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
5	Type	Char	A,B,C,D,E		Yes	
6	SP1 (Name/ID)	String			No	30
7	SP2 (Name/ID)	String			No	30
8	Resource ID Group				Yes	
9	Site Name/ID				No	30

Table 13: SS7 Link Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		6			
2	Link ID	Number			No	
3	Name	String			No	30
4	Description	String		Yes	Yes	255
5	SLC	Number			Yes	
6	Interface	Number			Yes	
7	Transport Protocol	Number			Yes	
8	Eagle Card	String		Leave it blank for PMF	No	
9	Eagle Port Number	Number		Leave it blank for PMF	No	
10	Linkset Name/ID	String			No	30
11	Site Name/ID	String			No	30
12	EagleID	Number		Leave it blank for PMF	No	

Table 14: Gb Link Configurations

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		21			
2	LinkID	Number			No	
3	Name	String			No	30
4	Description	String		Yes	Yes	255
5	PCM ID	Number			Yes	
6	Interface	Number			Yes	
7	SP Name/ID	Number			Yes	30

Table 15: PMF Card Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		11		No	
2	CardID	Number			No	
3	Slot Number	Number			No	
4	Hardware Type	Number	0- SPAN (E1/T1)		No	
5	Software Mode	Number	1-SS7 - T1 2-SS7 - E1 19-GB - T1 20-GB - E1		Yes	
6	Admin State	Number	0-Disable 1-Enable		Yes	
7	Name/ID	String			No	30

Table 16: PMF Port Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		12			
2	Port Number	Number	0-7		No	

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
3	Zero Spression	Number	7--B8ZS 6--AMI 5--HDB3		Yes	
4	Framing	Number	11--SF 12--ESF 9--CRC4_DF 8--CRC4 MMF		Yes	
5	Access Mode	Number	18-Auto Config 16-Long Haul 17-Monitor 15-Short Haul		Yes	
6	Bit Inversion	Number	0--On 1--Off		No	
7	Host Name/ID	String			No	30
8	Stot Number					

Table 17: PMF Port Assignment Configuration

ID	Field	Data Type	Possible Values	Optional	Can Be Updated	Max Length
1	Bulk Load Type		13			
2	HostName/ID				No	30
3	Card Slot Number				No	
4	Port Number	Number			No	
5	Channel Number	Number	1-32:E1 1-24:T1		Yes	
6	Number of Channels	Number	0-Disable 1-Enable	Yes (In case of SS7 Link)	No	
7	Name/ID	String		No	Yes	30

Example of a PMF csv file

Sample of CSV Formatted PMF File

These are examples of csv files that make up a PMF configuration.

Note: Files can be loaded in any order. Files do not have to be loaded at one time.

Sites csv file

```
1,NA,PMF-Quatro
1,NA,Demo1
1,NA,ixp2627
1,NA,PMF-DUO
1,NA,ML350-0A
1,NA,Prithvi-1A
1,NA,ixp0123
1,NA,DL380-1A
```

Hosts csv file

```
#Hosts.csv,,,,,,,,,
#BulkLoadType,HostID,HostName,Description,Frame,Position,IP,AppName,Description,AppType,Site
2,NA,PMF-DE-1A,,1,1,172.31.254.5,PMF-DE-1A,PMF NG,PMF NG,PMF_Delhi
2,NA,PMF-DE-1B,test1,1,2,172.31.254.6,PMF-DE-1B,PMF NG,PMF NG,PMF_Delhi
2,NA,PMF-DE-1C,,1,3,172.31.254.7,PMF-DE-1C,PMF NG,PMF NG,PMF_Delhi
```

Nodes csv file

```
#Nodes.csv,,,,,
#BulkLoadType,NodeID,NodeName,Description,Type
3,NA,TestGPRSNode,TestGPRSNode,GPRS
```

SS7SP csv file

```
4,NA,SP_1,,402,14428
4,NA,SP_13,,402,14440
4,NA,SP_161,,402,14488
4,NA,SP_165,,402,14492
4,NA,SP_169,,402,14496
4,NA,SP_17,,402,14444
```

Linkset csv file

```
5,NA,ls_PMF_1,1,A,SP_1,SP_161,1
5,NA,ls_PMF_5,5,A,SP_5,SP_165,2
5,NA,ls_PMF_9,9,A,SP_9,SP_169,1
5,NA,ls_PMF_13,13,A,SP_13,SP_173,2
```

5,NA,ls_PMF_17,17,A,SP_17,SP_177,1

5,NA,ls_PMF_21,17,A,SP_21,SP_181,2

SS7 Links csv file

6,NA,link_Card1_Port6_7,,6,8,0,,,ls_PMF_408

6,NA,link_Card1_Port6_8,,7,8,0,,,ls_PMF_408

6,NA,link_Card1_Port7_1,,0,8,0,,,ls_PMF_412

6,NA,link_Card1_Port7_2,,1,8,0,,,ls_PMF_412

GBSP csv file (not shown in this example)

GB Link csv file (not shown not shown in this example)

PMF Card csv file

11,NA,2,0,2,1,ML350-0A

11,NA,3,0,2,1,ML350-0A

11,NA,7,0,2,1,ML350-0A

11,NA,8,0,2,1,ML350-0A

11,NA,1,0,2,1,ML350-0A

PMF Ports csv file

12,0,5,9,18,0,ML350-0A,2

12,1,5,9,18,0,ML350-0A,2

12,2,5,9,18,0,ML350-0A,2

12,3,5,9,18,0,ML350-0A,2

12,4,5,9,18,0,ML350-0A,2

PMF Link Assignment csv file

13,ML350-0A,1,0,1,,link_Card1_Port0_1

13,ML350-0A,1,0,2,,link_Card1_Port0_2

13,ML350-0A,1,0,3,,link_Card1_Port0_3

13,ML350-0A,1,0,4,,link_Card1_Port0_4

13,ML350-0A,1,0,5,,link_Card1_Port0_5

13,ML350-0A,1,0,6,,link_Card1_Port0_6

13,ML350-0A,1,0,7,,link_Card1_Port0_7

13,ML350-0A,1,0,8,,link_Card1_Port0_8

Importing PMF Configurations

Pre-conditions for importing PMF configurations

1. NSP server is running.
2. You have logged into the NSP server and launched CCM.

3. You have created the necessary CSV files in the proper format.

Complete these steps when importing an PMF configuration.

1. Click **Bulk Import Configurations** on the Home Page.
The Import Files screen opens.

[Bulk Import Configurations](#)

File Type SS7 SSN Filters File Path [>> Remove](#)

[+ >> Add more file\(s\) to upload](#)

Figure 16: Bulk Load Import Screen

2. Select the **Sites** from the drop-down menu.
3. Click **Browse** in the first field.
The Choose File screen opens.
4. Select the **Sites.csv**.
5. Click **Open**.
The directory path with the file appears in the field.
6. Repeat steps 2-4 for the following files.

Note: You can import the files in any order and you do not have to import all files at one time.

Note: To add more files, click the **plus (+)** sign above the first file field.

- a) Hosts.csv
 - b) Nodes.csv
 - c) SS7SPs.csv
 - d) GbSPs.csv
 - e) GB Links.csv
 - f) PMFCards.csv
 - g) PMFPorts.csv
 - h) PMFPortsAssignments.csv
7. Click **Load**.
The files are uploaded to the system.

Once you have imported the files, you must resynchronize the subsystem.

PMF IP Filter Configurations

These tables show the basic PMF IP filter configurations needed when importing PMF IP filters using the bulk import operations.

Table 18: IP Address Filter Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		37		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
	Location	String	Source Destination		
5	Address Type	String	Host Address, Network Address		Yes
6	IP List	String			Yes

Table 19: IP Port Filter Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		36		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Type	String	Source Destination		Yes
6	Selected Ports	String	All, Even, Odd		Yes
7	Ports List	String			Yes

Table 20: VLAN Filter Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		35		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes

ID	Field	Data Type	Value	Optional	Can Be Updated
5	VLAN List	String			Yes

Table 21: IP Combo Filter Configuration

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		38		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Expression	String			Yes

Importing PMF IP Filters

Pre-conditions for importing PMF IP filters

1. NSP server is running.
2. You have logged into the NSP server and launched CCM.
3. You have created the necessary CSV files in the proper format.

Complete these steps when importing PMF IP Filters.

1. Click **Bulk Import Configurations** on the Home Page.
The Import Files screen opens.
2. Click **Browse** in the first field.
The Choose File screen opens.

[Bulk Import Configurations](#)

File Type File Path

Figure 17: Browse Screen

3. Select the **IPFilters.csv**.

4. Click **Open**.
The directory path with the file appears in the field.
5. Repeat steps 2-4 for the following files.
Note: You can import the files in any order and you do not have to import all files at one time.
Note: To add more files, click the **plus (+)** sign above the first file field.
 - a) PortFilters.csv
 - b) VLANFilters.csv
 - c) ComboFilters.csv
6. Click **Load**.
The files are uploaded to the system.

Once you have imported the files, you must resynchronize the subsystem.

Exporting Bulk Load Configurations

The Home page screen contains a Bulk Export Configurations function that is used to update your configurations using csv formatted files. You use this function for uploading the following configurations:

- Sites
- Hosts
- Applications (Only for PMF)
- PMF Link Assignments
- IP Filters

If you are not on the Home page complete the following steps. If you are on the Home page skip step 1.

1. From the Home menu, select **Home Page**
The Home page screen opens.
2. Click **Bulk Export Configurations**
The Bulk Export Prompt appears.

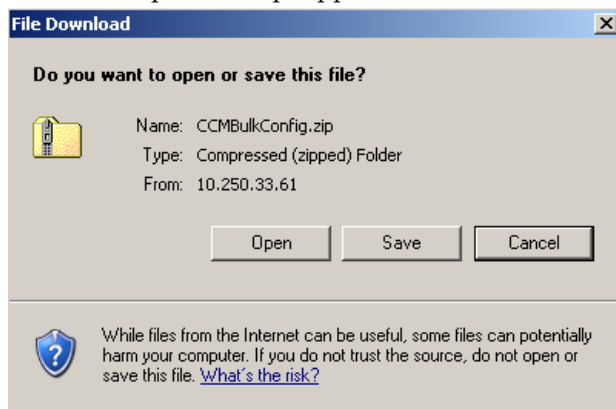


Figure 18: Bulk Export Configurations Prompt

At this step you can either save the zip file or open it to extract the files you want to use. To begin the extract process complete the next step.

3. Click **open**.

The zip extract screen opens.

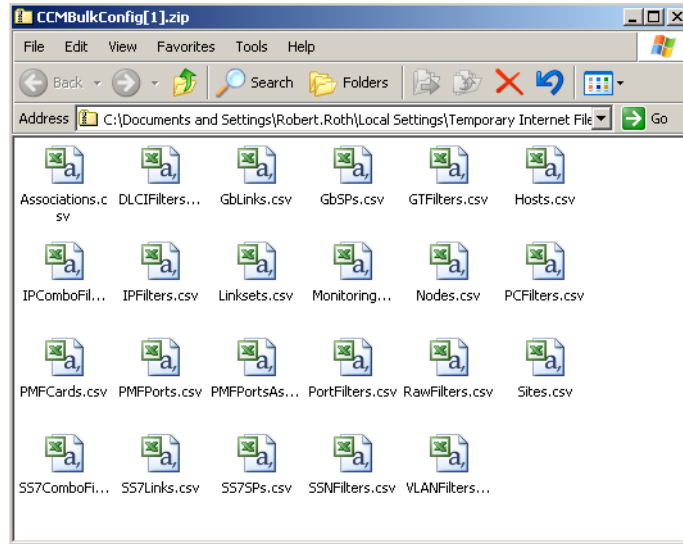


Figure 19: Zip Extract Screen

At this stage, you can extract any of the files needed.

Creating a Configuration Report

The CCM Home page also provides a Create Configuration Report feature that produces a report in MS Excel format. This report provides a spreadsheet (as a tab in the spreadsheet) for each element that is configured in the DIH system.

Selecting the **Create configuration report** option initiates a prompt shown below.

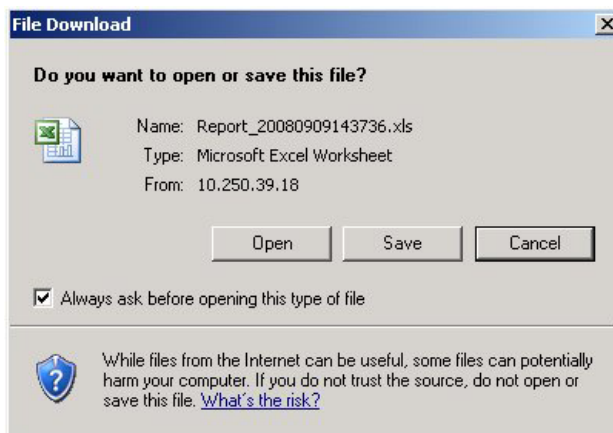


Figure 20: Open/Save Prompt For Configuration Report

You can either **open** the report (see below) or **save** the report to a local directory. When you open the report a spreadsheet opens shown in the figure below.

Session	DWH	Mediation System	Store Dataflow	Operate Dataflow	Build Dataflow	XDR Builder	Acquisition	PI
isp5001StreamMonitor	isp5001-1a(10.250.39.26)	test_06	StreamMonitor					
isp5001BuildMonitor	isp5001-1a(10.250.39.26)	test_06	BuildMonitor					
isp5001OperateMonitor	isp5001-1a(10.250.39.26)	test_06	OperateMonitor					
isp5001StoreMonitor	isp5001-1a(10.250.39.26)	test_06	StoreMonitor					
Morrisville_ISUP	isp5001-1a(10.250.39.26)	test_06	S_Morrisville_ISUP		Morrisville_ISUP	SS7 ISUP ANSI COR reconstruction	Morrisville WMF	
SessionName	isp5001-1a(10.250.39.26)	test_06	cja1		Sample_idr_dataflow	SS7 AN IDR capture		
pr_session	isp5001-1a(10.250.39.26)	test_06	S_pr_session		pr_build	SS7 ISUP ANSI COR reconstruction		
ISUP_Session	isp5001-1a(10.250.39.26)	test_06						

Figure 21: Sample Report

At this point you can select each tab and see information on each element in the system.

Setting the Severity of Platform Alarms

Complete these steps to enable or disable a platform alarm.

1. Select **Acquisition > Alarms > PMF Platform > List**.

The *Alarms* Configuration screen opens.

Alarm Number	Description	Enable	Actions
1	Breaker Panel Breaker Error	<input checked="" type="checkbox"/>	
2	Breaker Panel Breaker Error OK	<input checked="" type="checkbox"/>	
3	Breaker Panel Breaker Failure	<input checked="" type="checkbox"/>	

Figure 22: Alarms Configuration Screen

2. Select the **Alarm** to be enabled or disabled.
3. Click **modify** the Modify Platform Alarm Configuration screen opens with the alarm record details shown below.

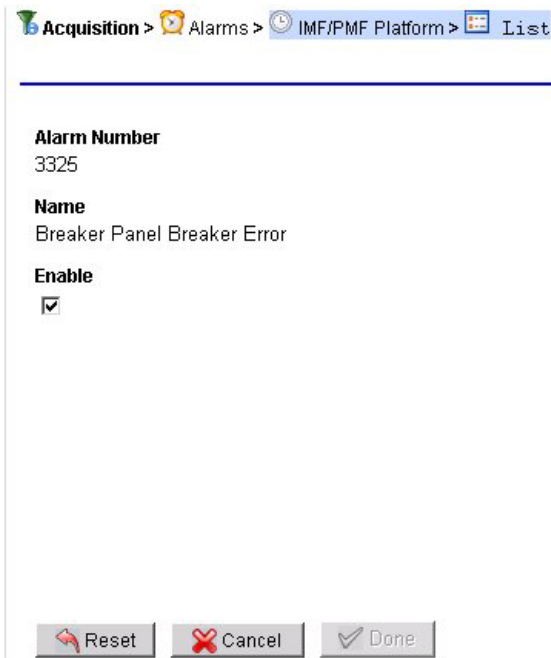


Figure 23: Modify Platform Alarm Configuration Screen

4. Enable or disable the alarm.
 - a) Enable - select the **Enable** check box.
 - b) Disable - click on the **Enable** check box to remove check mark.
5. Click **Done**.

The modifications are saved and you are returned to the alarm list.

Note: To update the alarm list, click the *Refresh* button on the toolbar. The list is updated to show the latest changes.

Chapter 6

Equipment Registry

Topics:

- *About Equipment Registry.....61*
- *Sites.....61*
- *About Subsystems.....66*

About Equipment Registry

The Equipment Registry perspective is used to manage (create, modify and delete) sites, subsystems, and physical servers. This perspective presents you with a graphic orientation of the physical equipment defined in DIH.

In addition, subsystem creation is accomplished in an automated single-step discovery process. CCM automatically discovers all applications and application specific data. Once a subsystem is created, the applications and application specific data can be modified using the Acquisition (PMF) and Mediation (IXP) perspectives.

Sites

A *site* consists of different kinds of subsystems with each subsystem having one or more hosts. Upon installation, CCM, by default, creates two sites (colored blue to denote that they are default sites):

- Legacy - has four categories - MSW and XMF-LEGACY. For legacy systems your only have the capability to create subsystems and add hosts to the CCM system. Discovery of application, network elements and sessions happens automatically on creating the subsystem and adding hosts to the subsystem. No further configuration is possible with the legacy systems.
- NOC - gives information of the servers that make up the CCM. For all servers you do not need to change/add anything under the NOC site. You do not need to change/add anything under the NOC site.

Apart from these two default sites, you can add any number of sites. The number of sites depends on the logical grouping of the monitored location. Once you create a site two categories of subsystems are automatically created under the site:

- IXP - Integrated xDR Processor (Mediation Perspective)
- PMF - Probe Message Feeder (PMF) (Acquisition Perspective)

Note: For DIH, there can only be one PMF and one IXP per site with a maximum of two sites

Note: In DIH the term "site" is synonymous with "enclosure," and means one site per enclosure not two geographically separated sites.

Site Creation and Discovery Process

On creating the subsystems and adding the hosts under the subsystem, CCM conducts a one-step process of creating subsystems, discovering the applications, network elements (in case of a PMF subsystem), discovering xDR builders and dictionaries (IXP subsystem) when you click the **create** button. A summary of the hosts and the elements discovered is provided to the user.

Listing Sites

When you select *Sites* from the object tree, all sites are listed in the left-hand workspace. The figure shown here shows an expanded *Equipment Registry Object* tree with site the sites listed in the workspace. The railway shows the *List* function being active.

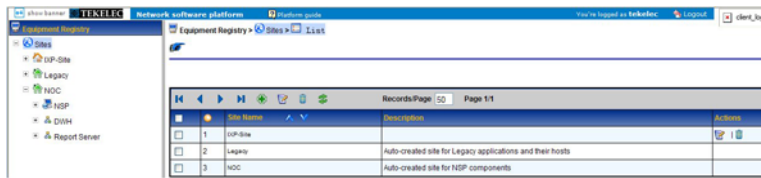


Figure 24: Site List Screen

Creating a Site

Complete these steps to add a site.

Note: Depending on the DIH configuration there can be either one or two sites for DIH (each site having only one PMF and one IXP subsystem).

1. On the object tree, select **Sites**.
2. Select **Add** from the pop-up menu.

The add screen opens shown in the figure.

Figure 25: Site Add Screen

3. Type in the **Name** of the site.
4. (Optional) Type in a **Description** of the site.
5. Click **Add**.

A prompt appears stating that the site has been successfully added, and the site appears in the object tree list in alphanumerical order with associated subsystems shown in this figure.

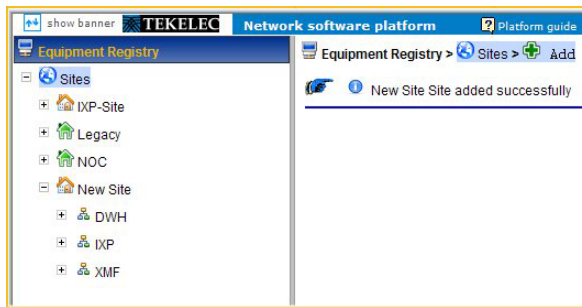
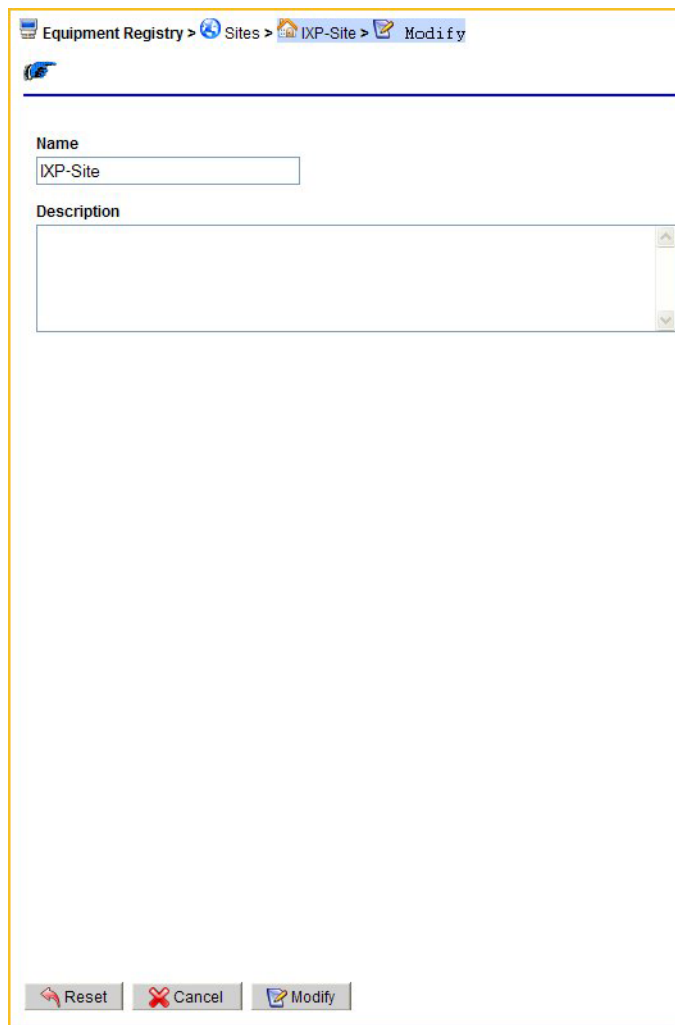


Figure 26: New Site With Subsystems

Modifying a Site

Complete these steps to modify a site.

1. Select the **Site** from the *object tree*.
2. Right-click and select **Modify**.



The screenshot shows a web-based interface for modifying a site. The breadcrumb navigation at the top reads "Equipment Registry > Sites > IXP-Site > Modify". Below the navigation is a horizontal line. The main form area contains two fields: "Name" with a text input field containing "IXP-Site", and "Description" with a larger text area. At the bottom of the form are three buttons: "Reset" (with a circular arrow icon), "Cancel" (with a red X icon), and "Modify" (with a pencil icon).

Figure 27: Site Modify Screen

3. Make necessary modifications to the site information.
4. Click **Modify**.
The modifications are saved.

Deleting a Site

Complete these steps to delete a site.

Note: Before deleting a site, all the hosts belonging to that site must first be deleted.

1. Select the **site** to be deleted from the *object tree*.
2. Click **Delete** from the *pop-up menu*.
3. Click **OK** at the prompt.
The site is deleted from the *object tree*.

Managing the Report Server

The report server subsystem, (if it is discovered), is located in the NOC site, and provides the infrastructure for static enrichment, KPI generation, reporting back-end (including the reporting engine and report database), web applications for viewing and administrating the reports as well as scheduling reports.

Report servers can be clustered and/or decoupled according to load-balancing and automatic-failover and KPI storage needs. There is a potential for CCM to discover three servers in the Report Server Subsystem. They are:

- Report Server (RS) - A server designated as the Primary or Secondary report server that processes and generates the scheduled reports.
- Report Data Server (RDS) - This can be a separate server used to house the report KPI database. The RDS can also house the Centralized Management System (CMS) database.
- Central Management Server (CMS) database - The CMS is an internal database maintained by Business Objects and needed by the RS to run reports.

The discovery process is identical to all subsystem discovery processes on CCM. The results will show:

- What was discovered.
- Any modifications that occurred to the subsystem since the last discovery process.
- Any errors that occurred during the discovery process.

Note: For more information on discovering a report server, see [Adding an IXP Subsystem](#).

Note: Since the Report Server provides the structure for Report Server Platform (RSP), it must be discovered first before the RDS. (There will be a prompt to discover the Report Server first before the CMS if a CMS is designated.).

Once the report servers have been installed and discovered, session network views can be created for reports. For more information, see [Creating Network Session Views](#).

Updating a Report Server

Once the Report Server subsystem has been installed and new report packages are added to a PIC system (installed on the CMS), the CMS has a "discover applications" icon located on the tool bar. Complete these steps to re-discover report package updates on a report server.

1. Select **Equipment Registry > NOC > Report Server**.
2. Select the **Report Server (CMS)** to be updated.
3. Click the **Discover Applications** icon located on the tool bar.
The discovery process begins. Once the discovery process is completed the summary page will show any new report package that has been installed on the CMS but not yet discovered in CCM, any modifications in the existing report package or any errors in the discovery process.

Deleting a Report Server

Complete these steps to delete a Report Server.

Note: The Report Data Server (RDS) must be deleted first before either the Central Management System (CMS) and the Report Server (RS).

When deleting a report server three prerequisites need to be met.

Note: If any of the prerequisites are not met, a prompt appears stating the Report Server cannot be deleted because a dependency exists.

- No report package (that was discovered for the RS being deleted) is in use. For example, the report package is not activated for any xDR session in the Report Admin.
- All historic KPI sessions have been deleted from the RDS.
- All report packages discovered for the RS have been removed from the CCM.

1. Select the **Mediation > Sites > NOC > Report Server (RDS)** to be deleted.
2. Select **Delete** from the tool bar.
3. Click **OK** at the prompt.

If a report server (RS) or Central Management System (CMS) needs to be deleted, they can be deleted next with CMS first and finally RS.

Procedure for Deleting KPIs Used by a RS

Complete these steps to delete KPIs on an RS that is to be deleted.

Note: For more information on using the Report Admin application, see the Report Software Platform User Guide.

Note: If a KPI session has KPIs being written to it, the report package must first be de-activated in the Report Admin application (see Report Software Platform User Guide for details) before the following steps can be performed.

1. Select **Report Admin (application) > Reporting Sessions** to be deleted.
2. Click **Permanently Remove** on the KPI session to be deleted.
3. Select **CCM > Mediation > Sessions**.
4. Select the **KPI session(s)** to be deleted.
5. Click **Delete** on the tool bar.
6. Click **OK** at the prompt.

About Subsystems

When you create a site, the following subsystems are created:

- DWH for storage
- IXP for storage and correlation
- PMF for data acquisition

Note: DIH can have a maximum of two instances of PMF and IXP, but since there can only be one instance of PMF and IXP per site, there can only be a maximum of two sites created.

Note: In DIH the term "site" is synonymous with "enclosure," and means one site per enclosure not two geographically separated sites.

Tree nodes are automatically created for these subsystems. From this perspective you can configure these subsystems by adding hosts and discovering applications that make up the subsystem.

Virtual IP Address Assignment

To assign a Virtual IP Address (VIP address) the following criteria need to be met.

- The VIP must be in the same subnet for the subsystem (IXP or PMF) and not being used for a host.

In addition, it is recommended to take the last available IP from the subnet since the IP is always assigned from the small number to the big number starting with server "1a."

Note: To find out the last available IP address, run `ifconfig` from one of the servers (or `platcfg` for the user) to get the broadcast address.

Here is an example of using the `ifconfig` for finding the last available IP address.

```
[root@ixp0301-1c ~]# ifconfig

eth01      Link encap:Ethernet  HWaddr 00:24:81:FB:CB:78
           inet addr:10.240.9.102  Bcast:10.240.9.127  Mask:255.255.255.192
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:100220031  errors:0  dropped:0  overruns:0  frame:0
           TX packets:103153021  errors:0  dropped:0  overruns:0  carrier:0
           collisions:0  txqueuelen:1000
           RX bytes:1700925078 (1.5 GiB)  TX bytes:3351841865 (3.1 GiB)
           Interrupt:185  Memory:f8000000-f8011100

lo         Link encap:Local Loopback
           inet addr:127.0.0.1  Mask:255.0.0.0
           UP LOOPBACK RUNNING  MTU:16436  Metric:1
           RX packets:10626760  errors:0  dropped:0  overruns:0  frame:0
           TX packets:10626760  errors:0  dropped:0  overruns:0  carrier:0
           collisions:0  txqueuelen:0
           RX bytes:1952272307 (1.8 GiB)  TX bytes:1952272307 (1.8 GiB)
```

In this example the B-cast 10.240.9.127 is one plus the last IP in the subnet, so 10.240.9.126 is the best candidate for the VIP.

Adding an IXP Subsystem

Note: You can have an unlimited number of IXP subsystems per site.

Complete these steps to add an IXP subsystem to a site and discover its elements.

1. Select **Equipment Registry > Site** that has the IXP subsystem.
2. Right-click on the site **IXP**.
3. Select **Add**.

Table 22: IXP Subsystem Add Screen Field Descriptions

Field	Description
Subsystem Name	The name of the IXP subsystem (required).
VIP Address	This is the Virtual IP address of the server where the IXP subsystem resides. Note: The VIP address is established when the IXP subsystem is initially installed and integrated into the customer network. The

Field	Description
	assignment of the VIP address can be the default of the broadcast address (broadcast-1) for the subnet, or it can be manually assigned to an address in the subnet. See Virtual IP Address Assignment .
IP Address	The IP address of IXP server where the IXP subsystem resides.
Add button	Adds the IP address to the list (you can have more than one IP address for a subsystem).
Delete button	Deletes the subsystem parameters from the list.
Reset button	Resets all settings to default.
Cancel button	Cancels the current process and returns back to original screen.
Create button	Adds the subsystem to the site.

4. Enter the **Name** of the IXP subsystem.
5. Enter the **VIP Address** of the subsystem.
6. Enter the **IP Address** of the subsystem.
7. Click **Add** to add the subsystem to the list.

Note: Repeat steps 4-7 to add each additional subsystem.

8. Click **Create**.

A progress bar appears as the system searches out the IP address, applications and protocols. When the discovery process is completed a Results Summary screen opens.

Note: Some systems use a large number of protocols and the time span for the discovery process can take several minutes.

Note: Use the *Modify* function to add a host(s) to an IXP subsystem.



[View Results](#)

Note: If there is a problem with the position, application or protocols, the color of the check mark will be yellow.

Figure 28: Subsystem Results Summary Screen



Figure 29: Results Summary Screen With Error Symbol

9. Click View Results.

The Results screen opens.

The screen has four tabs with five subtabs:

- Host - Shows the host parameters and status (added successfully or not)
- Application - Shows a summary of the number of applications discovered
- xDR Builders - Opens another screen with five tabs that lists the following parameters:

Note: xDR Builders are discovered and are the same for the entire subsystem.

- Added - shows the xDR Builders that added to the subsystem from the last synchronization
- Removed - shows the number of xDR Builders removed from the system from the last synchronization
- Modified - shows any xDR Builders that have been modified from the last synchronization
- No Change - shows any xDR Builders that have not been changed from the last synchronization

- Errors - shows a list of any errors that occurred during the discovery process or synchronization
- d) Synchronize IXP - shows if the synchronization was successful or not.

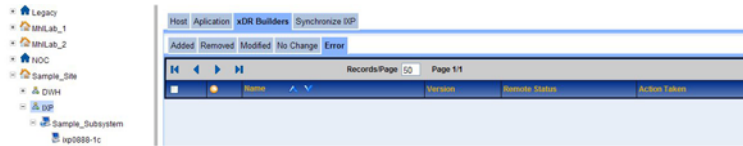


Figure 30: Object Tree Showing Added Subsystem With Results Screen

At this stage legacy subsystems can be added or additional IXP subsystems can be manually added.

10. Right click on the **IXP subsystem** and select **Apply Changes** for the changes to take effect.

Modifying an IXP Subsystem

Complete these steps to modify a subsystem.

1. Select the **subsystem** to be modified.
The *List* screen opens.
2. Select **Modify** from the popup menu.
3. Make the necessary modifications.
4. Click **Modify**.

A prompt appears stating that the subsystem was modified. You must now *apply changes* to that subsystem for the changes to take effect.

Deleting an IXP Subsystem

Note: You cannot delete a subsystem that has dependent applications such as sessions. You must first delete the dependent applications, then you can delete the subsystem.

Complete these steps to delete a subsystem.

1. Select the **subsystem** to be deleted from the list. The *List* screen opens.
2. Select **Delete** from the popup menu.
3. Click **OK** at the prompt, the subsystem is deleted.

You must now *apply changes* for that subsystem for the changes to take effect.

Re-discovering Applications

Once a IXP subsystem has been created, you can re-discover applications by completing the following steps.

1. Select the **subsystem** to be modified.

The *List* screen opens shown below.

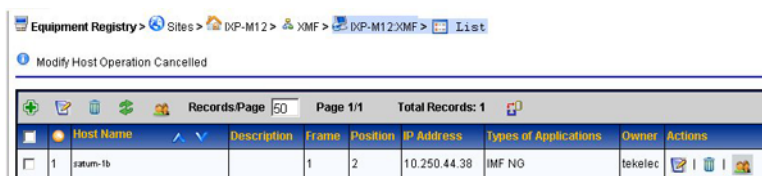
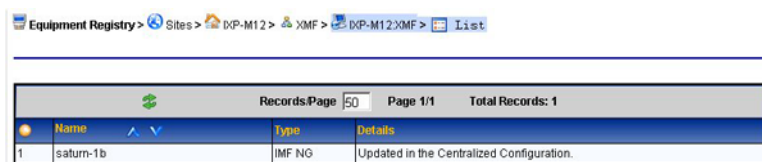


Figure 31: IXP Subsystem List Screen

2. Select **Host** from the list.
3. Click **Discover Applications** on the toolbar.

The screen changes, shown below, to show the re-discovered applications.



Note: For adding protocols and builders to an IXP subsystem, see ["Discovering xDR Builders"](#) and ["Configuring xDR Dataflow Processings."](#)

Figure 32: IXP Subsystem After Re-discover Process

Managing an IXP Storage Pool

There can be an unlimited number of storage servers in a subsystem. Storage servers can be created, modified and removed from a subsystem without interrupting the IXP performance. Each storage server can exist in one of three states.

Table 23: IXP Storage Server States

Server State	Description
Active	Insertion and queries are allowed on a storage server in this state
Query	Only queries are allowed on a storage server in this state
Maintenance	The storage server will not allow any insertion or queries of sessions while in this state.

Note: If an IXP storage server is in "Query" state, no configuration actions can be undertaken. All servers must be in "Active" state when sessions are created for queries on such sessions to be successful. Otherwise, if a query is launched in ProTrace on a newly created session, a "Unable to execute query: ORA-00942: table or view does not exist." will appear.

Storage Server Designations

Once a IXP subsystem has been created, you can an unlimited amount of servers in that subsystem. Once the servers have been discovered, CCM provides one of the following designations for each server on the subsystem.

Table 24: IXP Server Designations

Server Designation	Description
IXP-XDR	This server is used as an xDR storage server
IXP-PDU	This server is used as the PDU server
IXP-BASE	This server is used as the IXP base server

At least one server must have the designation IXP-XDR otherwise the discovery will fail. Once the designations have been made, CCM creates the pool of storage servers with designation IXP-XDR. The first IP Address should be assigned to the storage server.

Note: It is recommended that the sequence of IP Address for server should be the following order:

- All IXP storage servers
- All IXP base servers
- All IXP PDU servers

Adding a Storage Server to an IXP Storage Pool

Complete these steps to add a storage server to an IXP storage pool.

Note: IXP storage servers can be added to a pool without interrupting IXP. After adding a storage server to a pool, IXP evenly distributes xDRs to all storage servers in the pool.

1. Select From the *Equipment Registry* object tree, select **Site > IXP subsystem**.
2. Right-click on the **subsystem**.
3. Select **Add** from the pop-up menu.

The *Add IXP subsystem screen* opens shown in the figure below.

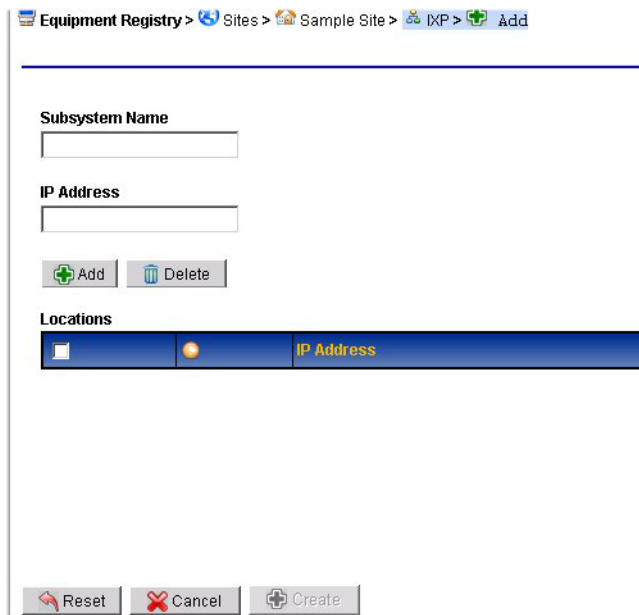


Figure 33: Add IXP Subsystem Screen

Add IXP subsystem screen - field descriptions

Table 25: IXP Subsystem Add Screen

Field	Description
Subsystem Name	The name of the subsystem (required)
IP Address	The IP address of subsystem
Add button	Adds the IP address, to the list (you can have more than one IP address if there are multiple servers in the subsystem)
Delete button	Deletes the subsystem parameters from the list
Reset button	Resets all settings to default
Cancel button	Cancels the current process and returns back to original screen.
Create button	Adds the subsystem to the site.

4. Type in the **Name** of the subsystem .
5. Type in the **IP Address** of the server in the subsystem.
6. Click **Add** to add the subsystem to the list.

Note: Repeat steps 4-7 to add each additional subsystem.

7. Click **Create**.

A progress bar appears as the system searches out the IP address, applications and protocols. When the discovery process is completed a results screen appears showing the parameters.

Note: Some systems use a large number of protocols and the time span for the discovery process can take several minutes.

Note: Use the *Modify* function to add a host(s) to an IXP subsystem.



[View Results](#)

Note: If there is a problem with the position, application or protocols, the color of the check mark will be yellow.

Figure 34: Subsystem Results Screen



Figure 35: Results Screen With Error Symbol

8. Click View Results.

The Results screen opens shown below.

The screen has four tabs:

- a) Host - Shows the host parameters and status (added successfully or not)
- b) Application - Shows a summary of the number of applications discovered
- c) xDR Builders - Opens another screen with five tabs that lists the following parameters:

Note: xDR Builders are discovered and are the same for the entire subsystem.

- Added - shows the xDR Builders that added to the subsystem from the last synchronization
- Removed - shows the number of xDR Builders removed from the system from the last synchronization

- Modified - shows any xDR Builders that have been modified from the last synchronization
 - No Change - shows any xDR Builders that have not been changed from the last synchronization
 - Errors - shows a list of any errors that occurred during the discovery process or synchronization
- d) Synchronize IXP - shows if the synchronization was successful or not.

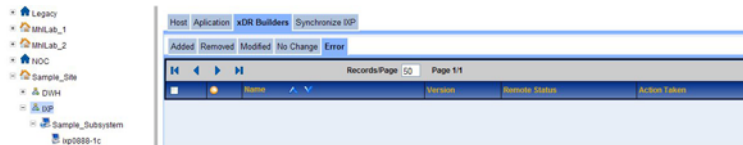


Figure 36: Object Tree Showing Added Subsystem With Results Screen

Note: You must apply changes to the subsystem for the changes to take effect.

Deleting a Storage Server

Complete these steps to delete a storage server in a storage pool.

1. Select the **equipment registry > site > subsystem > server** to be deleted.
2. Make the sever **inactive**.
3. Select **mediation > site > ixp subsystem > server > application**.
4. Delete the **application**.
5. Select **equipment registry > site > subsystem > server**.
6. Select **Delete** from the tool bar.
7. Click **OK** at the prompt.

The server is deleted

Note: You must apply changes before the changes take place.

About xMF (PMF) Subsystems

You have the ability to discover PMF subsystem information. Once the subsystem has been created and hosts discovered you must go to the Acquisition perspective to configure the subsystem.

Note: You can only have one PMF subsystem per site. To add another PMF subsystem, you need to create another site.

Adding a PMF Subsystem to a Site

After you have created a site, complete these steps to add a PMF subsystem to a site.

Note: Each site can only have one PMF subsystem.

1. Select **Equipment Registry > Site > xMF**.
2. From the xMF subsystem right-click menu select **Add**.

Table 26: xMF Subsystem Add Screen Field Descriptions

Field	Description
Subsystem Name	Name is identical to site name since only one xMF subsystem can exist on a site.
VIP Address	This is the Virtual IP address of the server where the PMF subsystem resides. Note: The VIP address is established when the PMF subsystem is initially installed and integrated into the customer network. The assignment of the VIP address can be the default of the broadcast address (broadcast-1) for the subnet, or it can be manually assigned to an address in the subnet.
IP Address	The IP address of xMF server where the PMF subsystem resides.
Add button	Adds the IP address, to the list (you can have more than one IP address for a subsystem).
Delete button	Deletes the subsystem parameters from the list.
Reset button	Resets all settings to default.
Cancel button	Cancels the current process and returns back to original screen.
Create button	Adds the subsystem to the site.

3. Enter the **VIP Address**.
4. Enter an **IP Address** for the PMF host.
5. Click **Add**.
6. Click **Create**.

The system discovers the hosts and cards that belong to the PMF subsystem. All successful discoveries are shown with a check mark beside it. See the figure below.

Note: If there is an error, a red x will appear beside the host or application that could not be discovered.

Note: E1/T1 Span cards are not auto-discovered, they are manually added to the PMF subsystem.

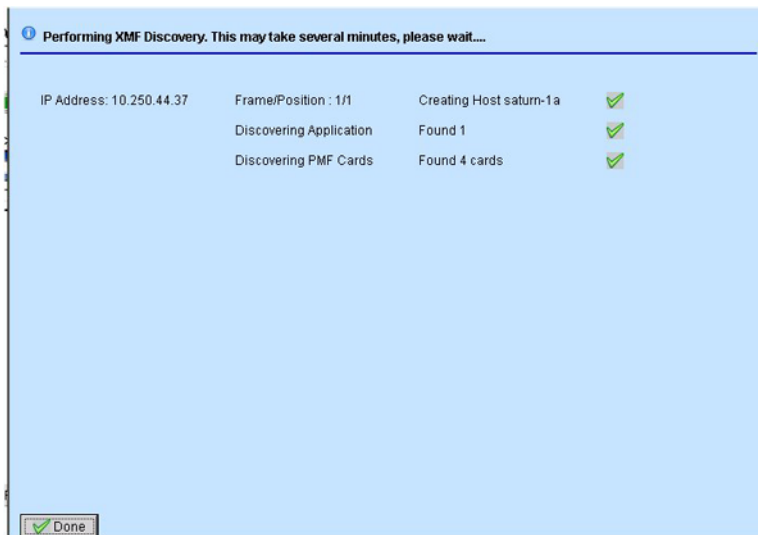


Figure 37: PMF Results Summary Screen

7. Click **Done** to close the Results Summary screen and view the discovery summary. The screen has the following tab information shown in the figure shown here:
 - a) Host tab - showing the IP addresses of the discovered hosts and the result
 - b) Application - showing the applications that were discovered
 - c) PMF Card Discovery - showing the cards installed on the host



Figure 38: Discovery Summary Screen - Hosts Tab



Figure 39: Discovery Summary Screen - Application Tab

Note: The Results screen only opens when the discovery process has been completed.

Note: If this is the first discovery process, all the tabs will be empty except for Added and Error. The other tabs are only populated when the discovery process is repeated after there has been some modification to the host (see how to modify hosts.).

		Page 1/1		Total Records: 0	
Slot	Type	Mode	Adm. State	Actions	
1	SPAN	SS7-E1	Enable	[Action Icons]	
2	NIC 4-Port	-	-	[Action Icons]	

Figure 40: Discovery Summary Screen - PMF Card Discovery

8. Select the **subsystem** again to see the newly created hosts and applications.

If there is an E1/T1 card for the PMF, open the Acquisition perspective to configure the card.

Note: Network cards and NGP cards are automatically discovered and do not have to be manually added.

Modifying a PMF Subsystem Host

Once a PMF subsystem has been created, you can modify the hosts that belong to the subsystem. Complete these steps to modify a host in a PMF subsystem.

1. Select the **Site > xMF subsystem** to be modified from the object tree.
The *List* screen opens.
2. Select the **Host** to be modified.
3. Select **Modify** from the toolbar.
4. Make necessary **modifications**.
5. Click **Modify** after you have made the necessary modifications.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Deleting a PMF Subsystem

Note: You can only delete a subsystem if there are no dependent hosts or applications to the subsystem. You must delete all hosts and applications before deleting the subsystem.

Complete these steps to delete an xMF subsystem.

1. Select **Site > xMF > PMF subsystem** to be deleted.
(Or select the subsystem from the *Site List* screen.)
2. Delete all **hosts and applications** that belong to the PMF subsystem.
3. Select the **PMF subsystem**.
4. Click **Delete**.
5. Click **OK** at the prompt.

The subsystem is deleted. You must now *apply changes* for the changes to take effect.

Chapter 7

Network Element Configuration

Topics:

- *About Network Elements.....80*
- *Filtering Network Elements.....80*
- *About Nodes.....81*
- *About Non-node Network Elements.....82*

About Network Elements

The term, Network Elements, refers to customer network IP elements. The perspective is divided into two categories:

- IP nodes
- IP Elements that include signaling points, cards and application servers.

In addition, each network element has a child table showing all dependent elements down to the link level.

For quick reference, a query can be performed for specific network elements such as nodes or signaling points. This function is very helpful in large networks.

Filtering Network Elements

The search option enables you to search for specific elements using the network element filter (query) wizard. Complete these steps to filter a network element.

1. Select the **Network Element (Node, Linkset, Link, SP)** category from the object menu.
The list screen opens.
2. Click the **Filter** icon on the tool bar (magnifying glass icon).
The network element filter screen opens.

LinkSets Filter	
The query has been loaded.	
Operator	Value
<input type="button" value="Add"/> <input type="button" value="Delete"/>	
Operator: <input checked="" type="radio"/> And <input type="radio"/> Or <input type="checkbox"/> Use Brackets	
Expression: <input type="text"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 41: Network Element Filter Screen (Linkset shown)

3. Click **Add**.
The screen changes to show fields, operators and values.
4. Select a **Field**.
5. Select an **Operator**.

6. Select a **Value**.

Note: To create a filter that has multiple expressions, repeat steps 3 thru 6 and select the proper Operator (and, or, use brackets).

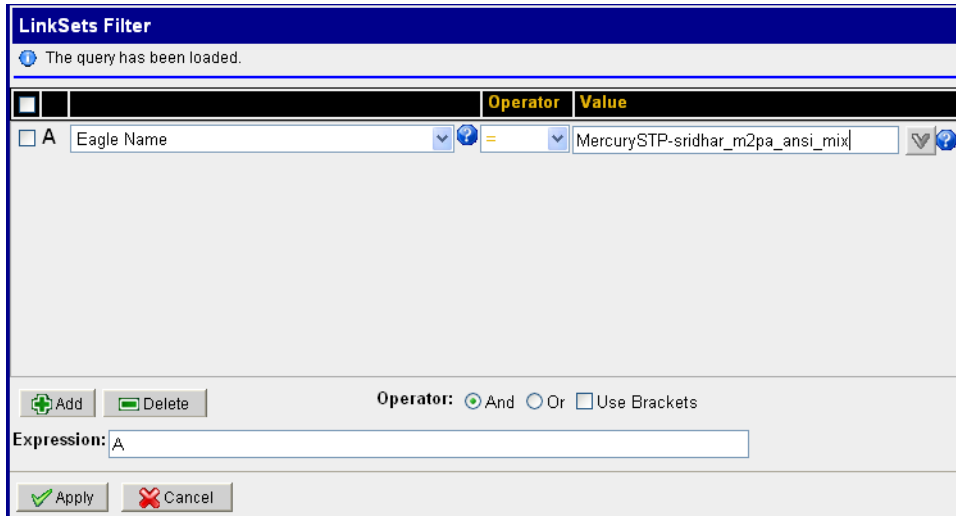


Figure 42: Filter Screen Filled

7. Click **Apply**.

The found network elements appear in the list table.

About Nodes

Nodes are the containers for linksets and links. Using CCM, you can create SS7, GPRS and IP nodes.

Creating a Node

Complete these steps to add a node.

1. Select **Network Elements > Nodes > Node Type (SS7, GPRS, IP) > Add Node**.

The *Add Node* screen opens shown below.

Table 27: Add Node Screen

Field	Description
Name	The name of the node
Description	Optional field to describe the node
Add button	Saves the record to the system and the node shows up in the object tree
Reset button	Resets the screen to default settings

Field	Description
Cancel button	Cancels the procedure

Name

Description

Figure 43: Node Add Screen

2. Type in the **Name** of the Node.
3. (Optional) Type in a **description** of the node.
4. Click **Add**.
 The node is added to the object tree.

Modifying a Node

Complete these steps to modify a node.

1. Select **Network Elements > Nodes > Node Type (SS7, GPRS, IP) > Node** to be modified.
2. Select **Modify**.
3. Make the necessary modifications.
4. Click **Modify**.
 A prompt appears stating that the node was modified.

Deleting a Node

Complete these steps to delete a node.

Note: You must delete the Signaling Points (SPs) associated with the node before deleting it.

1. Select **Network Elements > Nodes > Node Type (SS7, GPRS, IP) > Node** to be deleted from the list.
2. Select **Delete** from the popup menu.
3. Click **OK** at the prompt, the node is deleted.

About Non-node Network Elements

The non-node network element menu has three main categories:

- SS7 which is subdivided into
 - Linksets

- Associations
- Links
- Signaling Points (SPs)
- GPRS which is subdivided into:
 - Gb links
 - Signaling Points (SPs)
- IP which is subdivided into:
 - Signaling Points (SPs)

The differentiation between nodes and non-node network elements enables greater flexibility in working with linksets, links and associations.

Because network elements are so fundamental to the rest of the provisioning process, it is recommended that they be setup right after a site has been created.

About IP Network Elements

The IP network elements include: signaling points, IP cards, associations, application servers and application process servers. These signaling points enable the proper flow of IP packets.

Because network elements are so fundamental to the rest of the provisioning process, it is recommended that they be setup right after a site has been created .

About IP Signaling Points

The IP network element menu contains IP signaling points. These signaling points enable the proper flow of IP packets.

The differentiation between nodes and non-node network elements enables greater flexibility in working with linksets and links and associations.

Because network elements are so fundamental to the rest of the provisioning process, it is recommended that they be setup right after a site has been created .

Creating an IP Signaling Point

Complete these steps to create an IP signaling point for a node.

1. Select **Network Elements >Nodes > IP** . The Node List screen opens showing the node list table with signaling point table.

#	Node Name	Description of Node	Owner	State	Created
1	Test IP Node	This is an example of an IP Node	tekelec	N	16/09/2009 11:54:37

IP Signalling Points list for Node Test IP Node

#	SP	Description	Node Name	IP Id	OID	Owner	State	Created
---	----	-------------	-----------	-------	-----	-------	-------	---------

Figure 44: Add Signaling Point Screen

2. Click **Add** on the signaling point tool bar to open the IP signling point screen.
3. Enter the **Name** of the IP signaling point
4. (Optional) Enter a **Description**.
5. Click **Add**.

The IP signaling point is added to the Node.

Modifying an IP Signaling Point

Complete these steps to modify a IP signaling point.

1. Select **Network Elements >IP >SPs**
2. Select the **IP signaling point** to be modified.
3. Select **Modify**
4. Make the necessary modifications.
5. Click **Modify**.

A prompt appears stating that the signaling point was modified.

Deleting an IP Signaling Point

Complete these steps to detete an IP signaling point.

Note: When deleting an association, all mappings to that association will be broken.

1. Select the **IP signaling point** to be deleted.
2. Select **Delete**.
3. Click **OK** at the prompt.

The signaling point is deleted.

About IP Cards

CCM supports E5-ENET card running IPSG or IPGW for either STC or FastCopy capability. Cards can support either STC-style monitoring or FastCopy monitoring but not both. Cards configured on CCM show this information on the Card list screen.

- Card Number - shows the order that the card was configured. The first card configured on the system would have the number "1", the second "2" and so on.

- Card Name - a text field that provides the name of the card.
- Capacity - shows the capacity in TPS that the card can handle. This information is utilized in the SigTran ProDiag Application for monitoring purposes.

Adding an IP Card

Complete these steps to add an card to the system.

1. Select **Network Elements >IP > Cards** . The Card list screen opens showing the cards configured for the system.
2. Click **Add** on the tool bar.
3. Enter the **Name** of the IP card
4. (Optional) Enter the **Capacity** of the card in (TPS).
5. Click **Add**.

The card is added to the system.

Note: Apply Changes to have the card become functionally available for monitoring by the SigTran Prodiag application.

Modifying an IP Card

Complete these steps to modify an IP card.

1. Select **Network Elements >IP >Cards**
2. Select the **Card** to be modified from the list.
3. Click **Modify** from the tool bar.
4. Make the necessary modifications.
5. Click **Modify**.

A message appears stating that the card was modified.

Deleting an IP Card

Complete these steps to delete an IP card.

Note: When deleting an association, all mappings to that association will be broken.

1. Select the **Card** to be deleted.
2. Select **Delete**.

Note: A prompt will appear stating the following:

This action will delete the third party card from the Associations mapped with it. Please review the following:

The card (name) can not be deleted, mapped with # association(s)

Are you sure you want to delete this Card?

3. To delete the card, click **OK**.

About Application Servers

CCM allows for the configuration of IP Application Servers (AS). An AS is a logical entity serving a specific Routing Key. An example of an Application Server is a virtual IP database element handling

all requests for an SCCP-user. The AS contains a set of one or more unique Application Server Processes (ASPs), where one or more is normally actively processing traffic.

Note: PMF subsystems are manually discovered and their network elements must be created manually.

Adding an Application Server

Complete these steps to add an application server (AS) to the system.

Note: For each AS, the associations mapped to in can also be managed from the bottom table.

1. Select **Network Elements >IP > Application Servers**. The Application Server List screen opens showing the AS list table on top with its mapped associations table on the bottom.
2. Click **Add** from the tool bar.
The add screen opens.
3. Enter the **Name** of the AS
4. (Optional) Enter a **Description**.
5. Enter a valid **Routing Context** for the AS.
6. Click **Add**.

The association server is added to the system.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Mapping Associations to an Application Server

Complete these steps to map an association to an application server (AS).

1. Select **Network Elements >IP > Application Servers**. The Application Server List screen opens showing the AS list table on top with its mapped associations table on the bottom.
2. Select the **AS** to have the association.

Note: If the AS needs to be added, first click **Add** on the tool bar and follow the steps to add an AS.

3. Click **Show Details** on the tool bar.
4. From the bottom table, click **Add** on the tool bar.
5. Enter the **Name** of the Association.
6. Select the **Protocol** (SUA, M2UA or M3UA).
7. Select the **PMF Server** that houses the association.

Note: You must add a PMF server. See Adding a PMF server.

8. Enter the **Maximum Capacity** for the association.
9. Enter the **End Points**
 - a) Enter the **Source Port**.
 - b) Enter the **Distination Port**
10. Enter the **Source IP Address(es)**
11. Click **Add to List**.

Repeat steps 10-11 to add multiple addresses.

12. Enter the **Destination IP Address(es)**.

13. Click **Add to List**.

Repeat steps 12-13 to add multiple addresses.

14. Click **Finish**.

Note: For the changes to take effect, click **Apply Changes**.

Modifying a Mapped Association

Complete these steps to modify an Application Server (AS).

1. Select **Network Elements > IP > Application Servers**.

2. Select the **AS** to be modified.

3. Click **Modify** on the tool bar.

4. Make the necessary modifications.

5. Click **Modify** at the bottom of the screen.

A prompt appears stating that the signaling point was modified.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Deleting an Association Mapped to an Application Server

Complete these steps to delete an association mapped to an application server.

Note: The links and application servers will no longer exist if the association is deleted.

1. Select **Network Elements > IP > Application Servers**

2. Select the **Application Server** that has the association.

3. From the bottom table, select the **association** to be deleted..

4. Click **Delete** from the tool bar.

5. Click **OK** at the prompt. The association is deleted.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Modifying an Application Server

Complete these steps to modify an Application Server.

1. Select **Network Elements > IP > ApplicationServer**.

2. Select the **Application Server** to be modified.

3. Select **Modify**

4. Make the necessary modifications.

5. Click **Modify**.

A prompt appears stating that the Application Server was modified.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Deleting an Application Server

Complete these steps to delete an application server.

Note: When deleting an association, all mappings to that association will be broken.

1. Select **Network Elements > IP > Application Server**.
2. Select the **Application Server** to be deleted.
3. Select **Delete**.
4. Click **OK** at the prompt.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

About Associations

Associations refer to SCTP associations. An association provides the transport for the delivery of SCCP-User protocol data units and SUA layer peer messages. In their simplest form, they are combinations of links that can exist as PMF (utilizing traffic classifications) elements. Network element associations are discovered as part of the site creation process.

Note: On the other hand, all elements on a PMF subsystem require manual creation.

Showing Details of an Association

Complete these steps to show the details endpoints, associations or links mapped to a PMF.

1. Select **Network Elements > IP > Associations > PMF**.
2. From the list screen, select the **Association** to be viewed.
3. Click **Details** from the tool bar. The mappings for that association appear in the bottom table.

Deleting Associations

Complete these steps to delete a PMF association.

Note: When deleting an association, all mappings to that association will be broken.

1. Select **Network Elements > IP > Associations > PMF**.
2. From the list screen, select the **Association** to be deleted.
3. Click **Delete** from the tool bar.
4. Click **OK** at the prompt.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

About Application Servers Processes

CCM allows the monitoring of Application Server Processes. An Application Server Process (ASP) serves as an active or backup process of an Application Server, for example as a distributed signaling node or database element. Examples of ASPs are MGCs, IP SCPs, or IP-based HLRs. An ASP contains an SCTP endpoint and may be configured to process traffic within more than one Application Server.

Note: All elements on a PMF subsystem require manual creation.

Viewing Application Server Processes

The list screen for configured application server processes (ASPs) can be viewed in the ASP list screen. Selecting **Network Elements > IP > Application Server Process** opens the list page. The ASP table contains the following information.

- ASP Name - the name of the process
- Association Name - the name of the association mapped to the ASP
- Application Server Name - the name of the Application Server that the association is related to.
- Removed - shows the date and time that the process was removed through synchronizing the system.

Chapter 8

Network View Configuration

Topics:

- [About Network Views.....91](#)
- [About Link-based Network Views.....95](#)

About Network Views

You can access Session and Link Network Views sby selecting the Network View perspective from the directory tree. Then expand the tree to view these three objects. Session views can be hierarchical and can be one of two types:

- Network Views - A network, hierarchy or networks or session view.
- Link Network Views - A network view containing one or more links of the type - SS7 linkset, Gb links and Input streams.

The Network Views perspective provides a means of logically grouping SS7 linksets, Gb links, Input streams and xDR sessions used by other configuration operations as well as those operations used by applications.

Network views are hierarchical in that one network view can contain other network views, for example, a network view of a country could contain regional networks that contain state networks that contain city networks.

The figure shows the Network View Perspective object tree.



Figure 45: Network View Perspective

Creating Network Views

Network views function as an organizing entity. In complex networks, you can have several levels of networks (for more information, see [Nesting Network Views](#)). Complete these steps to create a network view.

1. Select **Network View > Session Views > Add** from the *Object tree*.

The *Initial Setup* screen opens shown in the figure below.



Figure 46: Initial Setup Screen

2. Type in **Network View Name**.
3. (Optional) Type in a **Description**.
4. Click **Next**.

The *View Type Selection* screen opens shown below.

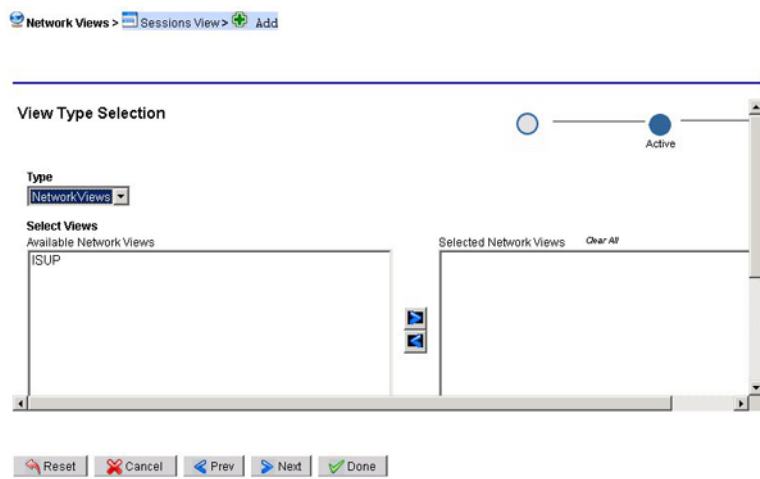


Figure 47: View Type Selection Screen

5. Select **Network Views** from the *Type* drop-down menu.
6. Click **Done** without selecting any available networks.

You have created a container network view that is empty and can function as a container for other networks within it.

Note: See [Nesting Network Views](#) for steps to include existing networks in the view.

Creating Network Session Views

You can access Session and Link Network Views by selecting the Network View option from the directory tree. Then expand the tree to see these three objects.

Like Container Network views, session views can also be hierarchical. Complete these steps to create a session view

1. Select **Network Views > Sessions View**.
2. Click **Add** from the tool bar.
3. Type in **Network View Name**.
4. (Optional) Type in a **Description**.
5. Click **Next**.
6. From the Type drop-down menu select **Sessions**.
7. Click the **Session Selector Filter** icon on the far right of the tool bar.
8. From the Session Selector Filter screen, select one or more **Dictionaries**.
9. Select the **Site(s)**
10. Click **Apply Filter** to filter on specific sessions and/or sites.
11. Click **Select**.

The system searches the dictionaries and sites. Any matches for the filter are shown in the Filtered Sessions field.

12. Click **Close** to close the screen.
13. Click **Done** without selecting any available networks.

You have created a session view.

Nesting Network Views

Container-based network views function as a shell that contains other networks. This type of network is helpful in organizing very large networks that contain other networks. For example, one might have a region network that contains several state networks which in turn contain city networks. Creating a container network enables you to create hierarchies for greater specificity in analysis and troubleshooting.

Complete the steps in [Creating Network Views](#) to create your parent (container) view. Once you have created the networks for your system. You can begin to “nest” the networks to form hierarchies. Follow these steps to create children of the parent.

1. **Network View > Session Views > List**.

The *Network View List* screen opens.

	Name	Type	Description	Actions
<input checked="" type="checkbox"/>	Sample_Session_View	sessionnetworkview	This is an example of a Session View	[Edit] [Delete]
<input type="checkbox"/>	TEST_NV	sessionnetworkview		[Edit] [Delete]
<input type="checkbox"/>	Test1	sessionnetworkview		[Edit] [Delete]
<input type="checkbox"/>	Test1_1	sessionnetworkview		[Edit] [Delete]
<input type="checkbox"/>	Test1_1_1	sessionnetworkview		[Edit] [Delete]

Figure 48: Network View List Screen

2. Select the **Parent Network View** from the list.
3. Click **Modify**.
The *Network View* screen opens.
4. Click **Next** to open the View Type Selection screen.

View Type Selection

Type: NetworkViews

Select Views

Available Network Views

- Sample_Session_View
- TEST_NV
- Test1_1
- Test1_1_1

Selected Network Views [Clear All](#)

[Right Arrow] [Left Arrow]

Reset Cancel Prev Next Done

Figure 49: View Type Selection Screen

5. Select a **network(s)** that will belong to the container network.
6. Click the **right-arrow** to place the networks into the Selected Networks field.
7. Click **Done**.
You created a nested or hierarchical network view.

About Network Views that Separate xDR Sessions

You can access Session and Link Network Views by selecting the Network View perspective from the directory tree. Then expand the tree to view these three objects. Session views can be hierarchical and can be one of two types:

- Network Views - A network, hierarchy or networks or session view.

- Link Network Views - A network view containing one or more links of the type - SS7 linkset, Gb links and Input streams.

The Network Views perspective provides a means of logically grouping SS7 linksets, Gb links, Input streams and xDR sessions used by other configuration operations as well as those operations used by applications.

Network views are hierarchical in that one network view can contain other network views, for example, a network view of a country could contain regional networks that contain state networks that contain city networks.

The figure shows the Network View Perspective object tree.



Figure 50: Network View Perspective

About Link-based Network Views

Link-based network views (IP) can be grouped together to create a view of the network that a system administrator uses for routing link data to the IXP. If a linkset is part of a network view and a new link is added to that linkset either manually or through discovery, the new link also automatically becomes part of the network view.

Configuring link Views

You can add Traffic Classifications (IP streams) to a link-based network view using CCM.

Note: Link views contain only linksets and are the lowest level of network view that can be created.

Creating Link-based Network Views

Complete these steps to add a leaf network view.

1. Select **Network View > Link View > Add**.

The *Initial Setup* screen opens shown in the figure shown below.

Network Views > Links View > List

Initial Setup

Active

Network View Name
Sample_Link_View

Description
This is an example of a lnk view

Reset Cancel Next

Figure 51: Link Network View Create Info-Initial Setup

2. Type in **Network View Name**.
3. (required) Type in a **Description**.
4. Click **Next**.
The *View Type Selection* screen opens shown in the figure.
5. Select **Links** from the drop-down menu. The *link type* screen opens shown below.

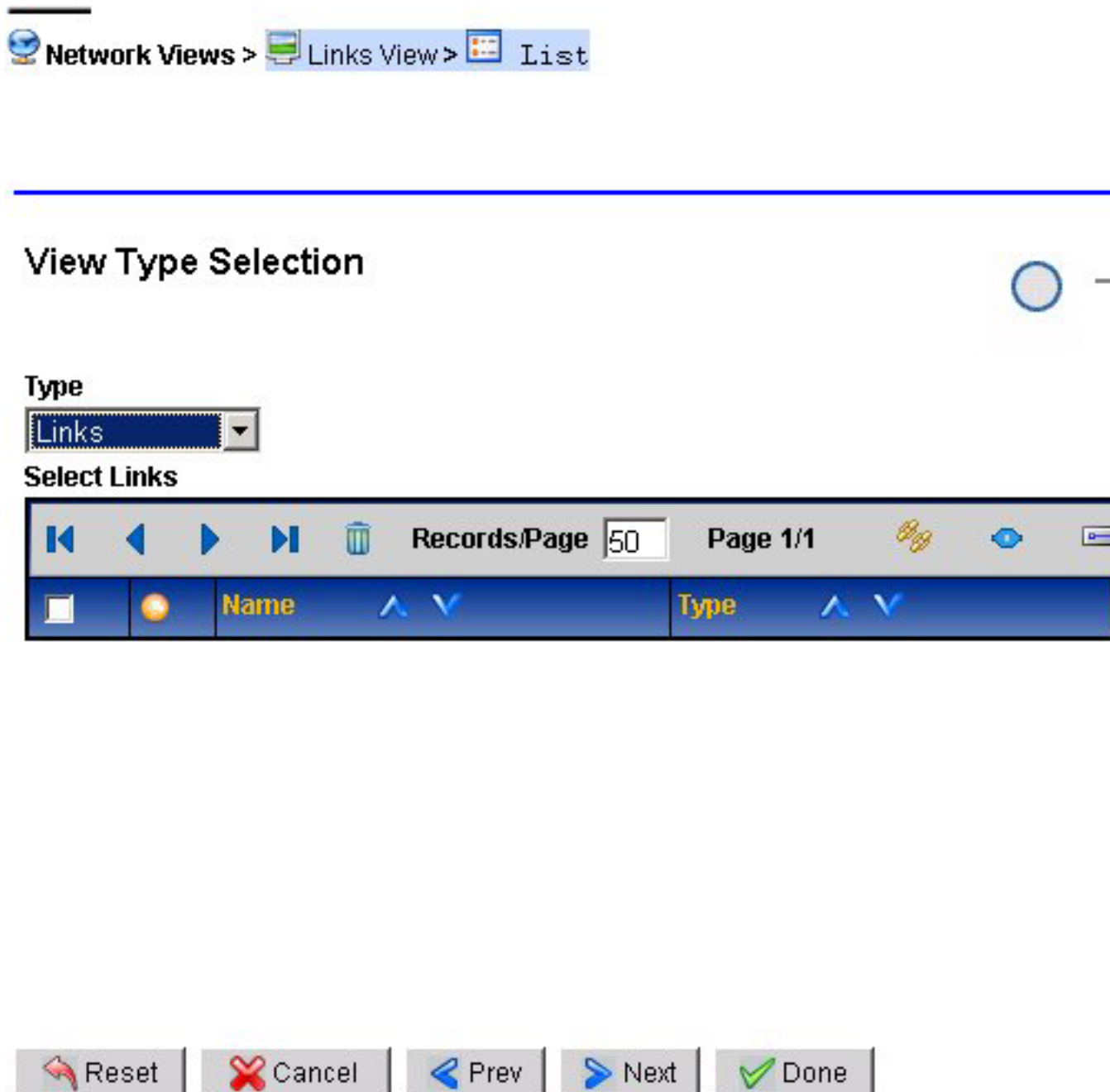


Figure 52: View Type Selection Screen

6. Click a **link type** from the toolbar.

Note: To add a specific linkset or link type, click on this link. [Selecting Traffic Classifications](#)

7. After you have added the links you need, click **Next**.
The *Add Link Network View* screen opens shown below.

Table 28: Link Network View Fields

Item	Option	Description
Field		
	Type	Pull-down menu to select between Network or Links
Toolbar		
	Delete	Deletes a existing link that is selected
	Select SS7 Linksets	Opens Add SS7 Linkset screen
	Select Gb Links	Opens Add Gb link screen
	Select IP Streams	Opens Add IP Stream screen
	Select SS7 Linksets & Gb Links	Opens Add SS7 Gb link screen

Selecting Traffic Classifications

Complete the following steps to select a Traffic Classification.

1. Click **Select Traffic Classifications** from *View Type Selection* screen tool bar shown below.

The *Traffic Classification* screen opens.

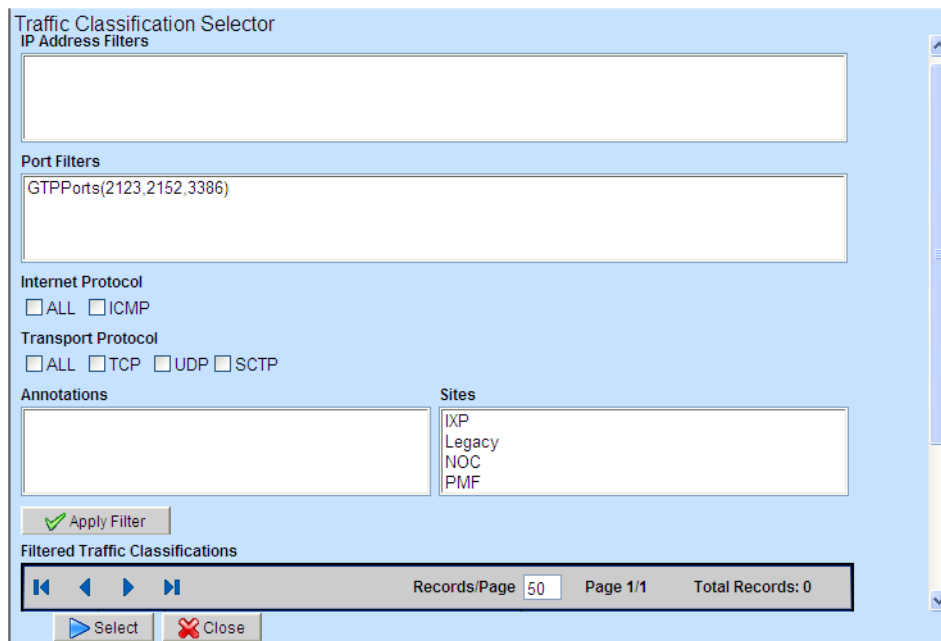


Figure 53: View Type Classification Screen

Table 29: IP Stream Selector Filter Fields

Item	Description
IP Address Filters	Lists available IP Addresses
Port Filters	Lists available Port Filters
Protocols	Check boxes for the following protocols Internet Protocol <ul style="list-style-type: none"> • All • ICMP Transport Protocol <ul style="list-style-type: none"> • All • TCP • UDP • SCTP
Annotations	A specific label or title you add for identification
Sites	The site for the filter
Apply Filter	Begins search for Input streams
Traffic Classification List	Lists Traffic classifications found in search
Select	Selects chosen links
Close	Closes the screen

2. Select **IP Address Filters** from the list.
3. Select the **Port Filters** from the list.
4. Select the **Protocol(s)** (either Internet or Transport) for the filter.
5. (Optional) An **annotation** about the filter
6. Select the **site(s)** for the filter.
7. Click **Apply Filter** to begin the search for available traffic selections.
8. Select the **traffic classification** from the list.
9. Click **Save** to save the selection to the link view.
10. Click **Close** the screen closes.

Modifying Link-based Network Views

Complete these steps to modify a link-based network view.

1. Select the **a network view** to be modified.
2. Select **Modify** from the popup menu.
3. Make the necessary modifications.

4. Click **Done**.

The network view record is updated.

Deleting Link-based Network View

Complete these steps to delete a link-based network view.

1. Selecting the **a network view** to be deleted.
2. Selecting **Delete** from the popup menu.
3. Click **OK** at the prompt.

Chapter 9

xMF Acquisition

Topics:

- *About the Acquisition Perspective.....102*
- *About PMF Subsystem Management.....102*
- *About PDU Filters.....120*
- *About PDU Dataflows.....138*
- *About Alarms.....142*

About the Acquisition Perspective

Once an xMF (PMF) subsystem is created and its applications and network elements are discovered, you configure the subsystem in the Acquisition perspective.

In the Acquisition perspective, only the sites that have xMF (PMF) subsystems are visible in the Acquisition object tree (shown in the figure below). In this perspective you can:

- Modify or delete applications
- Manage PDU Dataflows for an application
- Configure IP Cards
- Manage PMIA Settings
- Create PDU Filters
- Manage Traffic Classifications
 - Set System to Diameter Mode
- Configure Alarms

About PMF Subsystem Management

The general maintenance and configuration options for a specific PMF subsystem are accessed by right-clicking on the selected PMF subsystem. (Select **Sites > subsystem.**) The pop-up menu opens. The functions are briefly described in the table.

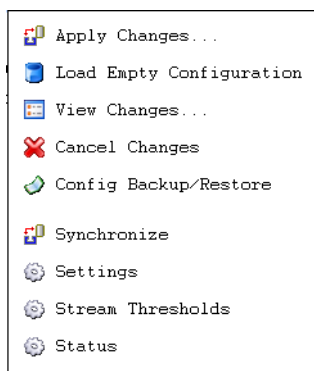


Figure 54: PMF Subsystem Pop-Up Menu

Table 30: PMF Subsystem Pop-Up Menu Options

Option	Description
Apply changes	enables you to apply any changes that have been made to the particular PMF subsystem. You are notified if there are any changes to the system and you use this option to accept the changes.
Load Empty Configuration	enables you to remove the existing configuration for the subsystem.

Option	Description
View changes	enables you to view any changes that have occurred in the subsystem in order to accept the change or cancel them.
Cancel changes	enables you to cancel any changes that have been made to the subsystem. Note: Routing is also deleted after this operation is performed.
Config backup/restore	enables you to backup or restore a previous backup configuration in case of system failure. Note: Routing is also deleted after this operation is performed.
Synchronize	enables you to discover (or re-discover) any applications or network elements on the subsystem.
Settings	enables you view and set some PMF parameters, such as PDF Idb Storage and Threshold Kbps, on a per-subsystem basis.
Stream Thresholds	enables you to set the limit for traffic passing through different destinations within an PMF subsystem.
Status	enables you to view the status of the system

Viewing Changes to an PMF Subsystem

Complete these steps to view the most recent synchronization and any pending changes on an PMF subsystem.

1. Select **Acquisition > Site >PMF subsystem**.
2. From the subsystem right-click menu select **View Changes**.

The screen shows the time and date of the last synchronization and any pending changes in the bottom table.

Loading an Empty Configuration on to an PMF Subsystem

Complete these steps to load an empty configuration on an PMF subsystem.

1. Select the **Acquisition > Site >PMF subsystem**.
2. From right-click menu select **Load Empty Configuration**

Note: A warning appears stating that loading an empty configuration un-route PDU dataflows at the associated PMF subsystem. (For more information, see Avoiding Lost PDU Routes Due to Cancel Changes on an PMF subsystem.)

3. To continue to load an empty configuration, click **OK**.

Note: For changes to take effect, click **Apply Changes** from the subsystem right-click menu.

Canceling Changes to an PMF Subsystem

You can cancel changes to a subsystem by using the *Cancel Changes* option.

Note: Choosing "Cancel Changes" on an PMF subsystem removes the existing configuration (any changes that have occurred) of that subsystem and restores the latest applied (active) configuration which includes Card/Port/Link Mapping and Traffic Classifications (TCs) for PMF. Feeder Thresholds, PMF subsystem parameters and PDU dataflows are preserved (but the PDU routes are not preserved). This action also enables the "Apply Changes" banner for that PMF subsystem. PDU dataflow routing can be restored either by modifying the Build DFPs on the IXP subsystem in order to re-associate the dataflows with the DFPs, or by restoring the last applied configuration on the IXP subsystem that contains the Build DFPs (see next note for constraints on restoring IXP).

Note: Care must be taken in restoring the last applied IXP subsystem configuration because any un-applied configurations to that IXP subsystem will be lost.

Complete these steps to cancel changes for a subsystem. Again, if any changes have occurred, you are prompted with this message:

Configuration has occurred on the following IXP subsystems: *IXPSubsystemName*, changes must be applied or cancelled.

Note: To apply changes to a subsystem you need to be assigned the role *NSPConfigManager* or *NSPAdministrator*.

1. Select the **subsystem** that needs to have the changes cancelled.
2. Right-click and select **Cancel changes** from the pop-up menu.
CCM displays the configuration changes that will be applied to the selected PMF subsystem. At this point, you are prompted if you want to continue, cancel, or undo.
3. Click **Undo**.
The last configuration that was applied to the PMF subsystem is reloaded.
4. Click **Apply Changes** for the PMF subsystem.
To avoid loss of PDU Routes on the IXP subsystems associated with the PMF subsystem follow steps 5-8.
5. Select the **IXP Subsystem** associated with the PMF subsystem.
6. From the right-click menu on the IXP subsystem, select **Config Backup / Restore**.
7. From the screen select the last **Active** backup.
8. Click **Restore** from the tool bar.
If prompted, click **Apply Changes**.

Avoiding Lost PDU Routes Due to Cancel Changes on an xMF Subsystem

How to avoid losing PDU routes when "Cancel Changes" option has been used on IXP and xMF (see Losing PDU Routes Due to Cancel Changes).

Complete one of these two actions to avoid losing PDU routes.

Either:

Click **Cancel Changes** only for the IXP subsystem leaving the associated xMF subsystem unchanged.

or

After clicking **Cancel Change** on an xMF subsystem, select the IXP subsystem(s) that is receiving the data from the xMF and complete the Config Backup/Restore procedure.

Restoring Lost PDU Routes Due to Cancel Changes on an xMF Subsystem

How to restore PDU routes lost when "Cancel Changes" option has been used on IXP and xMF (see Losing PDU Routes Due to Cancel Changes).

Complete these steps to restore lost PDU routes.

1. Select the **Mediation > Sites > IXP Subsystem > Config Backup/Restore** that is receiving traffic from the xMF subsystem.

Note: The backup configuration must be in a state labeled as "Active."

2. Select the **Configuration** that is to be restored from the backup list.
3. Click **Restore** from the tool bar.
The configuration that was selected is reloaded.
4. Apply changes to all **IXP** and **xMF** subsystems affected.

About xMF Subsystem Settings

The settings option for a specific xMF subsystem is accessed by right-clicking on the selected xMF subsystem. (Select **Acquisition > Sites > Subsystem > Settings**.) The subsystem settings list screen opens.

The settings option has five default parameters described in the table.

- **CountUploadFreq** - PMF uses the set value as the frequency for uploading to the IXP. It is measured in seconds, 1 (default) - 2147483647 (max java int).
- **LowThresholdKbps** - PMF parameter holding default value for Low threshold (default value is 320,000 kbps). The PMF will clear the overload alarm and resume forwarding all traffic when the traffic rate falls below the low threshold.
- **NoDataAlarmThreshold** - MSU Feed no activity alarm threshold in minutes. All connections are working, but no activity on the network. Threshold is defined in minutes between 1 min and 24 hours, with default of 5 min (Range: 1-1440).
- **PDUStorage** - saves monitored IP RAW data to RAM or disk
- **PDUStorageAssoc** - saves monitored IP RAW data to RAM or to disk
- **SigtranMonitor** - has three setting values 0=Off (if Sigtran is not utilized), 1=On if there are configured associations and application server processes, 2=ON (All).

Note: Not applicable when system is set to Diameter mode.

- **ThresholdKbps** - PMF parameter holding value for high threshold (default value is 360,000 kbps). The PMF will generate an overload alarm, stop forwarding and discard all traffic when the incoming traffic rate exceeds the overload threshold.
- **UseGTPFilters** - Enables and disables GTP post filtering on PMF. It has two setting values, 0=Disable and 1=Enable. (Enable is the default.)

Note: Not applicable when system is set to Diameter mode.

In addition you can create additional settings for your subsystem.

Note: You cannot delete the default setting parameters only those parameters that you have created.

CCM provides the capability to view and edit some xMF parameters on a per-subsystem basis. Initially, the following are the ranges for pre-defined parameters.

Table 31: Ranges for Pre-defined Subsystem Parameters

Parameter	Default Values	Comment
Pdu Idb Storage	0	PDU IDB Storage = 0, means data is buffered only in memory and has limited recover after network outage, but has higher speed. Recommended for PMF/IP
Threshold Kbps	360,000 kbps	ThresholdKbps = maximum allowed throughput of PMF AFTER PMIA filtering. If exceeded, the system will start to drop MSUs to protect itself. Minimum threshold is 320,000kbps.
Pdu Idb Storage	1	PDU IDB Storage = 1, means data is buffered on disk in case of network outage to be able to recover up to six hours. Recommended for PMF/E1T1

About xMF Subsystem Parameter Settings

There are two considerations when enabling or disabling PDUStorage and PDUStorageAssoc.

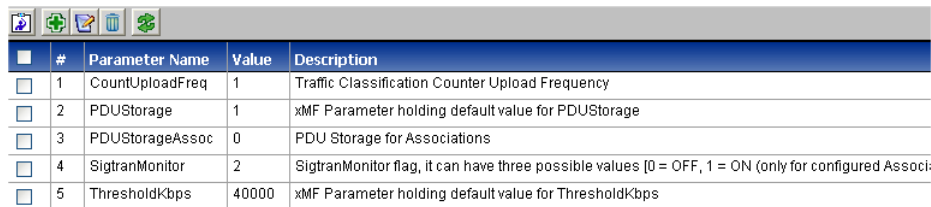
- PDUStorage - the default setting is *enabled*. When enabled, monitored data is stored to the disk.
Note: If IP RAW data should be stored to the disk, then both PDUStorage and PDUStorageAssoc must be enabled. If disabled, the monitored dat is stored only to RAM.
- PDUStorageAssoc - the default setting is *disabled*. If this parameter is *enabled*, then IP RAW data is stored to the disk.
Note: This parameter is valid only if PDUStorage is enabled. If it is disabled (default setting), then the monitored IP RAW dat is stored only to RAM.

Creating a Subsystem Parameter

Complete these steps to create a subsystem parameter for an xMF application.

1. Select **Acquisition > Sites > xMF subsystem** .
2. Right click and select **Settings**.

The Settings List screen opens.



#	Parameter Name	Value	Description
1	CountUploadFreq	1	Traffic Classification Counter Upload Frequency
2	PDUStorage	1	xMF Parameter holding default value for PDUStorage
3	PDUStorageAssoc	0	PDU Storage for Associations
4	SigtranMonitor	2	SigtranMonitor flag, it can have three possible values [0 = OFF, 1 = ON (only for configured Associ
5	ThresholdKbps	40000	xMF Parameter holding default value for ThresholdKbps

Figure 55: xMF Subsystem Settings List Screen

- Click **Add** on the tool bar.

The add creen opens.

Name

Value

Description

Figure 56: xMF Subsystem Parameter Add Screen

- Enter the **Name** of the parameter.
- Enter the **Value** (integer).
- (Optional) Enter the **Description**.
- Click **Add**.

The parameter is added.

Note: The subsystem must be synchronized for the changes to be incorporated into the system.

Modifying a Subsystem Parameter

Complete these steps to modify an xMF subsystem parameter..

- Select **Acquisition > Sites > xMF subsystem** that needs modification.
- Right click and select **Settings**.
The Settings List screen opens.
- Select the **parameter** to be modified.

Note: You can only modify the values of the three default parameters.

- Click **Modify** on the tool bar.
The Modify screen opens.
- (Optional) Modify the **Value**.

Note: You can also reset the value of the parameter to default settings only if you are modifying one of the three default parameters.

6. (Optional) Modify the **Description**.
7. Click **Modify** to save the settings.
The parameter is modified.

Deleting a Subsystem Parameter

Complete these steps to delete an xMF subsystem parameter..

1. Select **Acquisition > Sites > xMF subsystem**.
2. Right click and select **Settings**.
The Settings List screen opens.
3. Select the **parameter** to be deleted.
Note: You can only modify the values of the three default parameters.
4. Click **Delete** on the tool bar.
5. Click **OK** at the prompt.
The parameter is deleted.

Viewing PMF Subsystem Status

Complete these steps to view the status of subsystem applications.

1. Select **Acquisition > Sites > PMF Subsystem** that is needed.
2. Select **Status** from the pop-up menu.

The *Status List* screen opens.

You can view the:

- Application
- Monitoring group associated with the subsystem
- Application role
- Location

About Feeder Thresholds

Feeder thresholds provide limits that trigger alarms for different kinds of traffic (MSU, Gb, IP, MF) passing through the xMF system. xMF thresholds can be set thresholds in the Acquisition perspective of CCM.

Note: If you have any questions as about feeder alarms, please contact your *Tekelec* representative.

Feeder Threshold Values

Table 32: Threshold Values

Threshold Name	Description	Value
hiThreshold	High Threshold for PDU Stream	95%
holdOn	Hold for PDU Stream	5%
loThreshold	Low Threshold for PDU Stream	80%
maxThroughput	Max Throughput (Kbps) for PDU Stream	3000
msuInMaxThroughput	MSU Max Throughput (Kbps) for Incoming Traffic	50000
msuInHiThreshold	MSU High Threshold for Incoming Traffic	95%
msuInLowThreshold	MSU Low Threshold for Incoming Traffic	80%
msuInHoldOn	MSU Hold for Incoming Traffic	5%
msuOutMaxThroughput	MSU Max Throughput (Kbps) for Outgoing Traffic	50000
msuOutHiThreshold	MSU High Threshold for Outgoing Traffic	95%
msuOutLowThreshold	MSU Low Threshold for Outgoing Traffic	80%
msuOutHoldOn	MSU Hold for Outgoing Traffic	5%
gbInMaxThroughput	Gb Max Throughput (Kbps) for Incoming Traffic	80000
gbInHiThreshold	Gb High Threshold for Incoming Traffic	95%
gbInLowThreshold	Gb Low Threshold for Incoming Traffic	80%
gbInHoldOn	Gb Hold for Incoming Traffic	5%
gbOutMaxThroughput	Gb Max Throughput (Kbps) for Outgoing Traffic	150000
gbOutHiThreshold	Gb High Threshold for Outgoing Traffic	95%
gbOutLowThreshold	Gb Low Threshold for Outgoing Traffic	80%
gbOutHoldOn	Gb Hold for Outgoing Traffic	5%

Threshold Name	Description	Value
ipInMaxThroughput	IP Max Throughput (Kbps) for Incoming Traffic	400000
ipInHiThreshold	IP High Threshold for Incoming Traffic	95%
ipInLowThreshold	IP Low Threshold for Incoming Traffic	80%
ipInHoldOn	IP Hold for Incoming Traffic	5%
ipOutMaxThroughput	IP Max Throughput (Kbps) for Outgoing Traffic	150000
ipOutHiThreshold	IP High Threshold for Outgoing Traffic	95%
ipOutLowThreshold	IP Low Threshold for Outgoing Traffic	80%
ipOutHoldOn	IP Hold for Outgoing Traffic	5%
mfInMaxThroughput	Message Feeder Max Throughput (Kbps) for Incoming Traffic	150000
mfInHiThreshold	Message Feeder High Threshold for Incoming Traffic	95%
mfInLowThreshold	Message Feeder Low Threshold for Incoming Traffic	80%
mfInHoldOn	Message Feeder Hold for Incoming Traffic	5%
mfOutMaxThroughput	Message Feeder Max Throughput (Kbps) for Outgoing Traffic	150000
mfOutHiThreshold	Message Feeder High Threshold for Outgoing Traffic	95%
mfOutLowThreshold	Message Feeder Low Threshold for Outgoing Traffic	80%
mfOutHoldOn	Message Feeder Hold for Outgoing Traffic	5%

Setting a feeder Threshold

Complete these steps to set the feeder threshold of an xMF application.

1. Select **Acquisition > Sites > Server > xMF Application** that needs the thresholds set.
2. Right click and select **Feeder Thresholds**.

The *Feeder Thresholds List* screen opens.

#	Threshold	Value	Description
1	hiThreshold	95%	High Threshold for pdu stream
2	holdOn	5%	Hold for pdu stream
3	loThreshold	80%	Low Threshold for pdu stream
4	maxThroughput	500	Max Throughput (Kbps) for pdu stream

Figure 57: Feeder Thresholds List Screen

3. Select the **feeder** to be modified.
4. Click **Modify** the screen changes to show the threshold, value and description.

Acquisition > Sites > IMF-900 > IMF-900>MF > Servers > swit-imf-1a > swit-imf-1a (IMF NG) > Feeder Thresholds

Threshold	Value	Description	Actions
1 gblnHiThreshold	95%	Gb High Threshold for Incoming traffic	[Edit] [Delete]
2 gblnHoldOn	5%	Gb Hold On for Incoming traffic	[Edit] [Delete]
3 gblnLoThreshold	80%	Gb Low Threshold for Incoming traffic	[Edit] [Delete]

Figure 58: Feeder Thresholds Modify Screen

5. Set the **Value** (percentage).

Note: You can also reset the value of the parameter to default settings only if you are modifying one of the three default parameters.

Note: Feeder Thresholds set limits for different kinds of traffic passing through the xMF system.
6. (Optional) Modify the **Description**.
7. Click **Apply** located at the bottom left corner of screen (not shown).
The feeder threshold is modified.

About PMF Applications

Once an PMF subsystem and its applications have been discovered, you can manage the following application functions:

- Modify an application
- Delete an application
- Manage applications

Modifying PMF Applications

Note: You can only modify the description of an application once the application has been discovered.

Deleting PMF Applications

Complete the following steps to delete an PMF application.

Note: You cannot delete an PMF application that has a configuration. You must delete the dependent elements first before deleting the application.

1. Select **Acquisition > Site > PMF subsystem > Host > Application**.
2. Select the **application** from the PMF to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.

The application is deleted. You must then click **apply changes** the subsystem for the changes to take effect in the system.

About PMF Traffic Classifications

A Traffic Classification on PMF is used by to process the captured MSUs/PDUs received from the network. These captured MSUs/PDUs are forwarded to the IXP for processing/storage. The forwarding is based on PDU Data Flow Configurations, filters on the PMF and Dataflow Processing Configurations on IXP.

A Traffic Classification on PMF is also used to process the captured MSUs/PDUs received from the IP probe.

Note: Only when CCM has been set to DIH mode, can traffic classifications capture both IPv4 and IPv6 traffic using specific filters and protocols. See topics about configuring traffic classifications to capture IPv6 and IPv4 traffic

A Traffic Classification is a filter-like construct that is applied on an IP probe (NIC). Each input stream (IP stream) selects a part of the traffic from one or more IP probes. The basic idea is that each IP stream splits the traffic into manageable partitions that are used by downstream applications hence the term "traffic classifications". These captured MSUs/PDUs are forwarded to the IXP for processing/storage. The forwarding is based on PDU Data Flow Configurations, filters on the PMF and Dataflow Processing Configurations on IXP.

DIH when monitoring DSR, filters IP traffic on the Diameter protocol.

DIH filters IP traffic on these protocols.

- ICMP
- SCTP
- RTP
- FTP
- SFTP

Note: All Traffic Classification counts are reset in Diagnostic Utility. For more information, see the Diagnostic Utility Administration online help.

About Chunk and Packet Forwarding

Stream Control Transmission Protocol (SCTP) packets contain a common header and variable length blocks (chunks) of data. The SCTP packet structure is designed to offer the benefits of connection-oriented data flow (sequential) with the variable packet size and the use of Internet protocol (IP) addressing.

A packet represents a whole IP packet. When at least one chunk in a packet matches the filter, then the whole IP packet is sent. When forwarding packets it is best to use IP raw filters.

A chunk represents a common format where contents can vary. In chunk forwarding, only the chunk that matches the filter is forwarded along with the IP and SCTP header.

Note: When collecting statistical information only packets provide accurate size information. If chunk forwarding is selected, only the chunk size is used so statistical information will not be accurate. Therefore, avoid the activation of the SCTP stats and all the other SigTran stats (M2PA, M2UA, M3UA & SUA) on the SigTran builders (IPTransport & SS7Transport) when using chunk forwarding.

Listing a Traffic Classification (PMF)

You can view the list of traffic classifications (Input streams) for a PMF subsystem by selecting **Acquisition > Sites > PMF subsystem > Servers > Application > Traffic Classifications**.

The Traffic Classification screen has a tool bar and table.

The tool bar enables you to manage (add, modify, delete, refresh and set privileges) as well as activate or deactivate one or more input streams.

The table provides this specific information:

Table 33: Traffic Classification Fields

Field	Description
Traffic Classification Name	An alphanumeric field 30 characters max. Name can contain underscores, spaces and hyphens. An example of a traffic classification name is: 1_Traffic Class-Gb.
Description	Text field 225 characters max.
Internet Protocol	Lists the protocols filtered by traffic classification (All or ICMP).
Transport Protocol	Lists the transport protocols filtered by traffic classification (All, SCTP, TCP, UDP)
Application Layer	Lists the application layer (GTP-C or GTP-U) used by the traffic classification.
Forwarding	Lists the forwarding constraints (packets alone or packets and counters) for filtering the stream
Policy	Lists what IDM (intelligent data monitoring) policy, if any, is used in the traffic classification.
Annotations	Text field that lists any annotations for the stream.
Status	NA
Owner	Lists what user has created the traffic classification.

Adding a Traffic Classification (PMF)

Complete these steps to add a traffic classification (IP stream).

1. Select **Acquisition > Sites > PMF subsystem > Servers > Application > Traffic Classifications**.
The List screen opens.

2. Click **Add** on the tool bar to open the wizard.
3. Enter the **Name** of the traffic classification.
4. (Optional) Enter a **Description**.
5. Select an **Internet Protocol** from the pull-down list.
Note: When IPv6 is selected both transport protocol and filters options are disabled.
6. Select a **Transport Protocol** from the pull-down menu.
Note: If SCTP is selected, then all application layers are also selected by default (see step 7).
7. Select an **Application Layer** from the pull-down list.
8. Select a **Filter**.
Note: The list of filters presented is dependent upon the Transport Protocol selected.
9. Select the **Forwarding** method.
Note: If SCTP is selected as transport protocol, then the chunks or packets can be sent.
 - If chunk is selected as the forwarding mechanism, then only matched chunks are sent (as well as the IP and SCTP header).
 - If packet (IP Raw) is selected as the forwarding mechanism, then the whole IP packet is sent when at least one chunk in the packet matches the filter.
10. Select an **Association** to be associated with the TC.
 - a) If SCTP is selected, click **Association Selector** from the Association Selector tool bar.
 - b) Select one or more **Associations** from the Association Selector pop-up screen.
 - c) Click **Select** to add the associations to the traffic classification.
11. Click **Next** to open the probe assignment screen.
12. Select one or more **probes** from the available options field.
13. Click the **right arrow (>)** to move them to the selected options field.
14. Click **Next** to open the Annotation screen.
15. Enter an **Annotation**.
16. (Optional) Click **Add To List**.
The annotation is added to the *Selected Annotations* list.
Note: You can also select existing annotations by typing the first letter and select from the list that appears.
Note: To remove an annotation, select the annotation and click **Remove From List**.
17. Click **Create**.
The traffic classification is added to the list .
Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Configuring TC to Capture all IPv6 Traffic from Network

Note: Only when CCM has been set to DIH mode, can traffic classifications capture both IPv4 and IPv6 traffic using specific filters and protocols. See topics about configuring traffic classifications to capture IPv6 and IPv4 traffic

Complete these steps to configure a traffic classification (TC) for PMF to capture all IPv6 traffic from the network.

1. Select **Acquisition > Sites > PMF subsystem > Servers > Application > Traffic Classifications**.
The List screen opens.

2. Click **Add** on the tool bar to open the wizard.

3. Enter the **Name** of the traffic classification.

4. (Optional) Enter a **Description**.

5. Select **IPv6** from the pull-down list as the **Internet Protocol**.

Note: When IPv6 is selected both transport protocol and filters options are disabled.

6. Select **All** from the pull-down list as the Application Layer.

7. Select **Packets** as the Forwarding method.

8. Click **Next** to move to the Assign Probes screen.

9. Select one or more **probes** from the available options field.

10. Click the **right arrow (>)** to move them to the selected options field.

11. Click **Next** to open the Annotation Info screen.

12. Enter an **Annotation**.

13. (Optional) Click **Add To List**.

The annotation is added to the *Selected Annotations* list.

Note: You can also select existing annotations by typing the first letter and select from the list that appears.

Note: To remove an annotation, select the annotation and click **Remove From List**.

14. Click **Create**.

The traffic classification is added to the list that captures all the IPv6 traffic from the network.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Configuring TC to Capture All Incoming IPv4 Traffic Coming from the Network

Note: Only when CCM has been set to DIH mode, can traffic classifications capture both IPv4 and IPv6 traffic using specific filters and protocols. See topics about configuring traffic classifications to capture IPv6 and IPv4 traffic

Complete these steps to configure a traffic classification (TC) for PMF to capture all incoming IPv4 traffic coming from the network.

1. Select **Acquisition > Sites > PMF subsystem > Servers > Application > Traffic Classifications**.
The List screen opens.

2. Click **Add** on the tool bar to open the wizard.

3. Enter the **Name** of the traffic classification.
4. (Optional) Enter a **Description**.
5. Select **IPv4** as the Internet protocol.
6. Select either (according to the need) **All, TCP or UDP** as the Transport Protocol.
7. Select **All** as the Application Layer.
8. Select **No Filter** as the Filter.
9. Select **Packets** as the Forwarding method.
10. Click **Next** to move to the Assign Probes screen.
11. Select one or more **probes** from the available options field.
12. Click the **right arrow (>)** to move them to the selected options field.
13. Click **Next** to open the Annotation Info screen.
14. Enter an **Annotation**.
15. (Optional) Click **Add To List**.

The annotation is added to the *Selected Annotations* list.

Note: You can also select existing annotations by typing the first letter and select from the list that appears.

Note: To remove an annotation, select the annotation and click **Remove From List**.

16. Click **Create**.

The traffic classification is added to the list that captures all the IPv6 traffic from the network.

Note: For the changes to take effect, right-click on the PMF subsystem and select **Apply Changes** from the menu.

Modifying Traffic Classifications

1. Select **Acquisition > Sites > PMF subsystem > Server > Application > Traffic Classifications**.
The List screen opens.
2. Select the specific **Traffic Classification (IP Stream)** .
3. Click **Modify** from the tool bar.
4. Modify the appropriate information in the record.
5. Click **Modify** at the bottom of the screen.

Note: You must apply changes to the PMF subsystem for the changes to take affect.

Deleting Traffic Classifications

Complete these steps to delete an IP Stream record from a PMF Traffic Classification.

1. Select **Acquisition > Sites > PMF subsystem > Host > Application > Traffic Classifications**.
The List screen opens.
2. Select the **Traffic Classification(s)** to be deleted.
3. Click **Delete** on the tool bar.

4. Click **OK** at the prompt.

The traffic classification(s) is deleted from the list.

Note: You must apply changes to the PMF subsystem for the changes to take affect.

Setting System to Diameter Mode

Complete these steps to select Diameter mode for a system.

Note: The default setting is "standard" for a system where mode where a variety of traffic classifications (TCs) are created and filters are chosen for those TCs. In Diameter mode there are predefined traffic classifications and filters are chosen just for those pre-defined TCs.

1. Select **Acquisition > Sites > PMF Site > Servers > xMF Server > Traffic Classifications** from the object menu.

The Traffic Classifications (TC) list screen opens.

2. From the tool bar, select **Diameter Mode** from the drop-down list at the right-hand side of the tool bar.

3. Click **OK** at the prompt to deactivate TCs in standard mode.

The three Diameter Traffic Classifications are listed in table format shown in this table.

Column Heading	Description
Selection	This column is for selecting specific TCs.
Record #	This shows the numerical order of the TC in the table.
Traffic Classification Name	Provides the Name of the TC. For Diameter Setting there are only three TCs. They are: <ul style="list-style-type: none"> • Diameter_Exception • Diameter_Frag • Diameter_Trace Note: None of the TCs can be deleted. The only TC that can be modified is Diameter_Trace
Description	(Optional) This column shows any description of the TC.
Internet Protocol	Shows the Internet protocol used (default is ALL).
Transport Protocol	Shows the transport protocol used (default is ALL).
Application Layer	Shows the application layer (ID) used (default is ALL).
Forwarding	Shows the forwarding medium (default is Packets).

Column Heading	Description
Policy	Shows the policy used for the TC.
Annotation	Shows any annotation used for the TC.
Status	Shows the status (shows green for active or red for inactive)
Owner	Shows the name of the user that created the TC.

Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

About PMIA (for PMF Subsystems)

This option supports PMIA means Pattern Matching IP Algorithms (PMIA) configuration for PMF.

For monitoring IP traffic, CCM provides a traffic classification for each xMF (PMF) server. Each PMF server can be run in two modes either normal mode or expert mode.

In normal mode, you define IP Filters using CCM and optionally can apply on traffic classification.

In expert mode, you browse the file which can be interpreted by PMF server. While server running in expert mode, all predefined IP filters will be disabled for this server.

Note: All PMIA counts are reset in the Diagnostic Utility application using a command line. For more information, see the Diagnostic Utility Administration Guide.

Using Normal and Expert Mode (PMF)

For each PMF server, you have an option to switch from normal mode to expert mode and back from expert mode to normal mode. Complete these steps to switch between *normal* and *expert* modes.

1. Select **Acquisition > xMF subsystem > PMF server > Application.**

The PMIA screen opens.

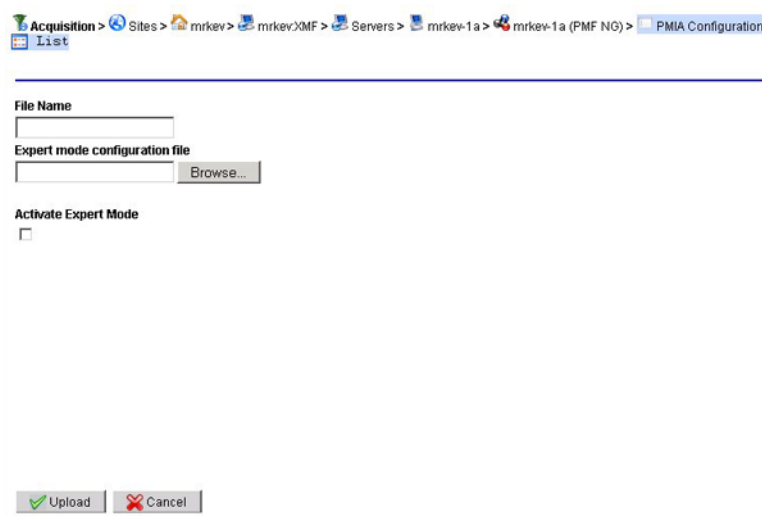


Figure 59: PMIA Screen

2. Enter the **File Name**.
3. Select the **Activate Expert Mode** field.
Note: Before using this option, consult with Tekelec personnel.
4. Browse the **file** that can be interpreted by xMF server.
5. Click **Upload** to upload the selected file and place the PMIA into expert status.

PMIA (PMF) Activating and De-activating a Configuration

1. Select **Acquisition > xMF subsystem > PMF server > Application**.
The *PMIA List* screen opens.
2. Select the **PMIA** to be converted.
3. Select **Modify**.
The *Modify* screen opens.
4. Select the **Activate Expert Mode** field to de-activate the PMIA.
5. Click **Modify**.
The *PMIA* is modified.
Note: You can use the alternate method by select the PMIA from the List, and clicking *De-activate* from the toolbar.

Deleting a PMIA (in a PMF Subsystem)

1. Select **Acquisition > xMF (PMF) subsystem > server > Application**.
The *PMA List* screen opens.
2. Select the **PMIA** to be deleted.
3. Click **Delete**.

4. Click **OK** at the prompt.
The PMIA is deleted.

About Data Transport Service (DTS)

You can use DTS to pull data from an xMF datasource (PMF) to IXP. You create a DTS transport that defines the route (the IP address and protocol derived from the DTS datasource and IP address and port on the PMF).

Creating a Route for a DTS Transport

Complete these steps to create a route for a DTS transport.

1. Select **Acquisition > Sites > Server > xMF Application** that needs the DTS.
2. Right click and select **DTS transport**.

The *DTS List* screen opens.

Protocol	Primary IP Address	Alternate IP Address	Actions
SCTP	000.000.000.000		[Edit] [Delete]

Figure 60: Dts List Screen

3. Click **Add** the *DTS Add* screen opens shown below.

Protocol:
 Primary IP Address:
 Alternate IP Address:

Figure 61: Dts Add Screen

4. Select the **Protocol** (SCTP) to be used.
5. Select the **Primary IP Address**.
6. (Optional) Select the **Alternate IP Address**.
7. Click **Create**.

The new DTS appears in the *List screen*.

About PDU Filters

The PDU dataflows that are configured in the acquisition (xMF) perspective can have filters applied to them. These filters provide a way to route selective data from an xMF subsystem to the IXP

subsystem. The filters are broadly categorized into two PDU family types, IP and Diameter. These family provide greater efficiency in data analysis and manipulation. This is a list of protocols and their filter types.

Note: There can be an unlimited number of filters in DIH, but only one filter can be associated with a dataflow at one time.

Note: The maximum size of any filter is 4000 bytes. If the filter exceeds this constraint, an error message appears stating that the filter has exceeded the size limit.

- IP protocol filters include:
 - PORT
 - IP Address
 - Combination
 - SAPI
 - VLAN

xMF MSU and EMP Correspondance Values

This list provides the corresponding EMP message type with an xMF MSU type.

xMF MSU Type	EMP Message Type
2	LSSU
3	MTP2 LSL / HSL
5	SS7_Layer3
6	ISDN_Layer3
10	RAS
11	Q9331
12	H245
13	SIP
14	RTCP
40	SigTran_M3UA
41	SigTran_M2UA_MTP3
42	SigTran_M2PA_MTP3
43	SigTran_SUA
60	MTP2a HSL
61	SS7_MTP3
69	SS7_MTP2A_LSSU
70	SS7_M2PA_MTP3_ANSI_NoSCTP_NoIP
71	SS7_M2UA_MTP3_ANSI_NoSCTP_NoIP

xMF MSU Type	EMP Message Type
72	SS7_M3UA_NoSCTP_NoIP
73	SS7_SUA_NoSCTP_NoIP
74	SS7_M2PA_MTP3_ITU_NoSCTP_NoIP
75	SS7_M2UA_MTP3_ITU_NoSCTP_NoIP

About IP PDU Filters

IP filters are used to filter based on IP addresses. IP filters allow you to limit the data forwarded by a dataflow to the IP addresses included in the filter. There are five types of IP filters:

- IP address filters - Filters based on its IP Address
- Port filters - Filters based on the port numbers (PMF only). When creating a Port filter, you should include only those port numbers you want to obtain information about. This will filter out all Port numbers not included in your filter.

Note: The range for port numbers is 1-65535. You have the option of selecting all, even, odd ports within a specified range. Port filters have the ability to combine any overlap of ranges.

Note: There is a limitation of 20 entries for a port filter. An individual port number or a range are counted as one entry.

- VLAN filters - Filters
- SAPI filters - Filters based on the stream control transmission protocol numbers
- Combination filters - Filters based on a combination of one or more of the other filters

About IP Address PDU Filters

IP Address filters allow you to filter for IP addresses. When you create an IP filter, you should include the IP addresses you want information about. This will filter out all IP addresses not included in your filter. To create filters that filter out specific IP addresses only, you must use Combination Filters.

The add IP Filter screen is used for adding IP address filters.

Figure 62: Add IP Address Filter Screen

Table 34: Add / Modify Port Filter Screen Fields

Field	Description
Filter Name	User assigned name of filter. The filter name is used to identify the filter when setting up dataflows or combination filters.
Description	(Optional) Enables you to add information about the filter.
Location	Select one of the following from the drop-down menu: <ul style="list-style-type: none"> • Destination: Outgoing IP ports. • Source: Incoming IP ports.
Enter IP Address	Where you can add a valid IP address.
Add button	Adds the IP address to the IP Address List.
IP Address List	Shows the IP addresses that the filter uses.
Create button	Create: Creates and saves the Port Filter information.

Adding an IP Address PDU Filter

Complete these steps to add an IP Address.

1. Select **Acquisition > PDU Filters** from the object menu.

- The PDU Filter list screen opens.
2. Click **Add** from the tool bar.
The PDU Filter Family screen opens.
 3. Select **IP - Internet protocol**.
The IP tab opens.
 4. Select **IP Address filter**.
The IP Filters screen opens.

The screenshot shows a web-based form for configuring IP filters. It contains the following elements:

- Filter Name:** A text input field.
- Description:** A large text area for entering details about the filter.
- Location:** A dropdown menu currently set to 'Destination'.
- Address Type:** A dropdown menu currently set to 'Host-Address'.
- Enter IP Address:** A text input field next to an 'Add' button.
- IP Address List:** A list area with a 'Remove' button.

Figure 63: IP Filters Screen

Table 35: IP Filter Screen Fields

Field	Description
Filter Name	User assigned name of filter. The filter name is used to identify the filter when setting up dataflows or combination filters.
Description	(Optional) Enables you to add information about the filter.
Location	Select one of the following from the drop-down menu: <ul style="list-style-type: none"> • Destination: Outgoing IP ports. • Source: Incoming IP ports.
Address Type	Select one of the following from the drop-down menu <ul style="list-style-type: none"> • Host-Address : Specific address of a host • Network-Address: An address of a network
Enter IP Address	Where you can add a valid IP address.
Add button	Adds the IP address to the IP Address List.

Field	Description
Remove button	Removes the IP address from the list.
IP Address List	Shows the IP addresses that the filter uses.
Finish button (Not shown)	Creates and saves the Port Filter information.
Previous button (Not shown)	Takes you back to the previous (IP)screen
Cancel button (Not shown)	Cancel the procedure with no information saved.

5. Type in the **Filter Name**.
6. (Optional) Type in a **Description** of the IP Address.
7. Select a **Location** from the *pull-down* menu.
8. Select the **Address Type** from the *pull-down* menu.
9. Type in an **IP Address** in the *Enter IP Address* field.
10. Click **Add** to add the port to the *Port List*.
11. Click **Finish**.

The filter is added to the *IP Address filter object tree* in alphanumerical order.

Removing an IP Address from the List

To remove an IP Address, Complete these steps.

1. Select the **IP Address record** that needs modification.
2. Click **Edit**.
3. Select the **IP Address** from the *IP Address List*.
4. Click **Remove**.

The IP Address is removed.

5. Click **Done** to save the changes.

Modifying an IP Address PDU Filter Record

Complete these steps to modify an IP Address filter.

1. Select the **IP Address filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.

The changes are saved.

Deleting an IP Address PDU Filter

Complete these steps to delete a IP Address filter.

1. Select the **IP Address filter** to be deleted.
2. Select **delete** from the menu.
3. Click **OK** at the prompt.

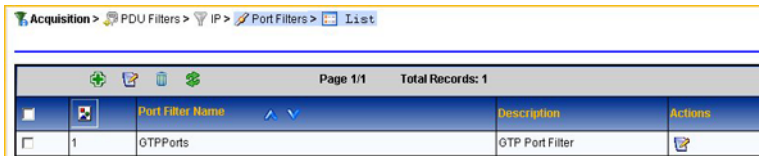
The filter is deleted.

About IP Port PDU Filters

IP Port filters provide a means of filtering through specific ports (all, odd or even). This helps in distributing traffic to the system.

Listing IP Port Filters to Show Default GTP Port Filter

There is a default GTP port filter provided in the *IP port filters list* screen shown in the figure below.



The screenshot shows a web-based interface for listing IP Port Filters. The breadcrumb navigation at the top reads: Acquisition > PDU Filters > IP > Port Filters > List. Below the navigation is a toolbar with icons for adding, deleting, and refreshing. The main content area displays a table with the following data:

Port Filter Name	Description	Actions
1 GTPPorts	GTP Port Filter	[Edit]

Page 1/1 Total Records: 1

Figure 64: IP Port Filter Screen With GTP Port Filter Default

This filter comes with three default GTP ports. They are:

- 2123
- 2152
- 3386

There may be network configurations that use more GTP port filters or different GTP filters than the defaults provided. In this case you can modify the default filter by completing the steps described in [Modifying a Port Record](#) and [Removing a Port from the List](#).

Removing a Port from the List

To remove a Port, Complete these steps.

1. Select the **Port record** that needs modification.
2. Click **Edit**.
3. Select the **Port** from the *Port List*.
4. Click **Remove**.
The Port is removed.
5. Click **Done** to save the changes.

Adding IP Port PDU Filters

Complete these steps to add an Port filter.

1. Select **Acquisition > PDU Filters** from the object menu.
The PDU Filter list screen opens.
2. Click **Add** from the tool bar.
The PDU Filter Family screen opens.
3. Select **IP Filters**.
4. Click **Next**.
The IP screen opens.
5. Select **PORT - IP Port Filter**.

The Port Filters screen opens.

Figure 65: Add Port Filter Screen

This table describes the fields on the Add Port Filter screen.

Table 36: Port Filter Screen Fields

Field	Description
Filter Name	User assigned name of filter. The filter name is used to identify the filter when setting up dataflows or combination filters.
Description	Enter pertinent information for this filter.
Location	Select one of the following from the drop-down menu: <ul style="list-style-type: none"> • Destination: Outgoing IP ports. • Source: Incoming IP ports.
Selected ports	This is a drop-down menu option with the following selections: <ul style="list-style-type: none"> • Even: All even port numbers. • Odd: All odd port numbers. • All: Both odd and even port numbers.
Enter Port or Port range	Allows you to enter individual port numbers or a range of port numbers to be monitored.
Add	Adds the number typed in the Enter Port box to the Port List box.
Port List	Shows all of the chosen Ports being filtered.

Field	Description
Remove	Deletes highlighted values from the Port List box. Multiple entries can be removed at the same time.
Finish button (Not Shown)	Saves the Port Filter information to the system.

6. Type in the **Filter Name**.
7. (Optional) Enter a **Description**.
8. Select a **Location** from the *pull-down* menu.
9. Select a **Port** from the *Selected Ports pull-down* menu.
10. Type in a **Port** in the *Enter Port* field.
11. Click **Add** to add the port to the *Port List*.
12. Click **Finish**.

Modifying a Port Record

Complete these steps to modify a Port filter.

1. Select the **Port filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
The changes are saved.

Deleting a Port Filter

Complete these steps to delete a port filter.

1. Select the **Port filter** to be deleted.
2. Select **delete** from the menu.
3. Click **OK** at the prompt.
The filter is deleted.

About IP VLAN PDU Filters

VLAN filtering is a user-defined filter based on VLAN ID in the ethernet layer. It allows a user to filter IP packets of a matching VLAN tag in the ethernet layer.

A list of up to 10 VLANS can be identified and entered during configuration. If a VLAN list is empty, then no filtering is applied for VLAN.

If the traffic is using 802.1Q VLAN tagging, then you must use a VLAN filter to pass the traffic through to an IP dataflow. This can be done using a combination filter. Conversely, if a VLAN filter is used to filter a dataflow, than any traffic that does not use VLAN tagging will not pass through the dataflow.

Adding an IP VLAN PDU Filter

Complete these steps to add an IP VLAN filter.

1. Select **Acquisition > PDU Filters** from the object menu.

The PDU Filters list screen opens.

2. Click **Next**.

PDU Filter Family screen opens.

3. Select **IP - Internet Protocol**

4. Click **Next**.

The IP screen opens.

5. Select **Vlan filter**.

6. Click **Next**.

The VLAN filters screen opens.

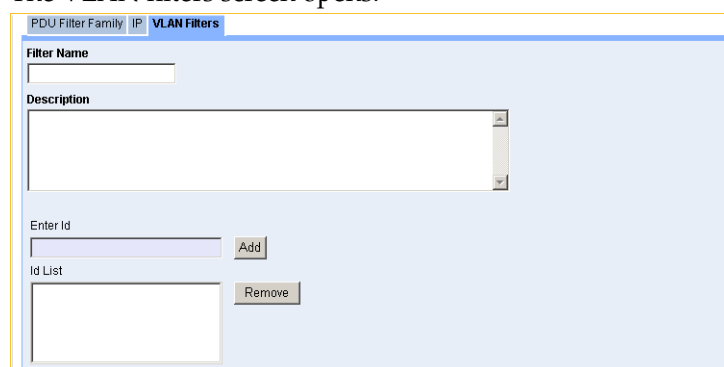


Figure 66: Add IP VLAN Filter Screen

The table describes the fields on this screen.

Table 37: VLAN Filter Screen Fields

Field	Description
Filter Name	User-defined name for filter.
Enter Id	Type in the VLAN Id.
Add	Adds the Id information entered to the ID List.
ID List	Moves highlighted filter into Filter Expression box.
Remove	Data must match all filters tied together with this operation.
Finish button	Saves filter settings based on the information shown in the Filter Expression field.

7. Type in the **Filter Name**.

8. (Optional) Type in a **Description** of the VLAN filter.

9. Type in an **ID** in the *Enter ID* field.

10. Click **Add**.

The ID appears in the *ID List* field.

11. Click **Finish**.

The filter is added to the *VLAN filter object tree* in alphanumerical order.

Removing an ID from the List

To remove an ID, Complete these steps.

1. Select the **VLAN** record that needs modification.
2. Click **Edit**.
3. Select the **ID** from the *ID List*.
4. Click **Remove**.
The ID is removed.
5. Click **Done** to save the changes.

Modifying an IP VLAN Filter Record

Complete these steps to modify an IP VLAN filter.

1. Select the **IP VLAN filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
The changes are saved.

Deleting a IP VLAN PDU Filter

Complete these steps to delete an IP VLAN filter.

1. Select the **IP VLAN filter** to be deleted.
2. Select **delete** from the menu.
3. Click **OK** at the prompt.
The filter is deleted.

About SAPI Filters

SAPI filtering is a user-defined filter based on in the ethernet layer. It allows a user to filter IP packets of a matching VLAN tag in the ethernet layer.

Adding a IP SAPI Filter (PMF)

Complete these steps to add a IP SAPI filter.

1. Select **Acquisition > PDU Filters** from the object menu.
The PDU filters list screen opens.
2. Click **Add** on the tool bar .
The PDU Filter Family tab appears.
3. Select **IP** from the list.
4. Click **Next**.
The IP tab appears.
5. Select **SAPI filter** from the list.
6. Click **Next**

The SAPI Filters tab appears.

Figure 67: Add SAPI for Gb over IP Filter Screen

This table describes the fields in the Gb SAPI filter screen.

Table 38: Add SAPI Filter for GP over IP Screen Fields

Field	Description
Filter Name	User assigned name for the SAPI Filter.
Description (Optional)	Provides a description of the SAPI filter
Selected SAPI numbers	Drop-down menu to Include or Exclude a range of SAPI numbers.
SAPI filter	Radio button to select a SAPI filter. The range for a SAPI filter can be from 0-16.
No SAPI filter	Radio button to select if there is no SAPI filter.
Previous / Finish / Cancel (not shown)	<ul style="list-style-type: none"> • Finish: Creates and saves the SAPI Filter information. • Previous: Takes you back to the previous screen. • Cancel: No information is saved for this filter.

7. Type in the **Filter Name**.
8. (Optional) Enter the **Description**.
9. Select a **SAPI number function** from the *pull-down* menu (include or exclude).
10. Select to use or not use a **SAPI filter**.
11. Click **Finish**.

The filter is added to the PDU filter list screen.

Modifying a SAPI Filter for Gb over IP

Complete these steps to modify a Gb over IP PDU filter.

1. Select the **SAPI Gb over IP filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.

The changes are saved.

Deleting a SAPI Filter for Gb over IP

Complete these steps to delete a SAPI for Gb over IP filter.

1. Select the **Gb SAPI for Gb over IP filter** to be deleted.
2. Select **delete** from the menu.
3. Click **OK** at the prompt.

The filter is deleted.

About IP Combination Filters

Combination filters are for using the existing IP and Port (Gb) filters to filter for information. The various operators can be used to filter in or filter out information.

Note: The maximum size of any filter is 4000 bytes. If the filter exceeds this constraint, an error message appears stating that the filter has exceeded the size limit.

Adding an IP PDU Combination Filter

Complete these steps to add an IP Combination filter..

1. Select **Acquisition > PDU Filters** from the object menu.
The PDU Filters screen opens.
2. Click **Add** from the tool bar.
The PDU Filter Family screen opens.
3. Select **IP-Internet Protocol** .
4. Click **Next**.
The IP screen opens.
5. Select **IP Combination Filter**
The *Combination Filters* screen opens.

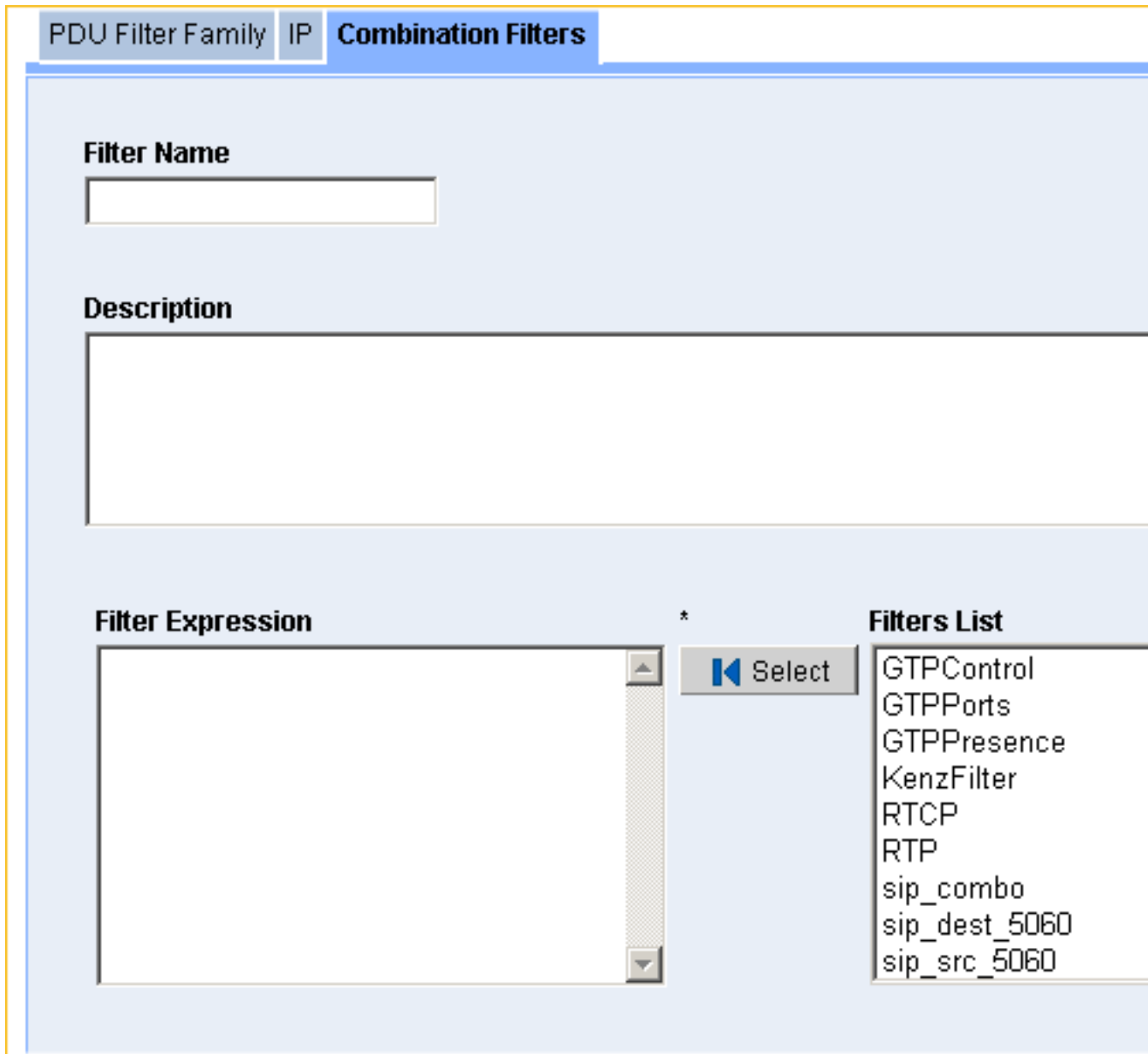


Figure 68: Combination Filters Screen

The table describes the fields on this screen.

Table 39: Combination Filter Screen Fields

Field	Description
Filter Name	User-defined name for filter.
Filter Description	Enter pertinent information for the combination filter.

Field	Description
Filter Expression	Provides a view of the combination filter value as it is created. Selected filters and logical operators appear in this window. When the Accept button is clicked, the information in the Filter Expression window becomes the new Combination filter.
Filter List	List of existing filters a user can combine.
Select button	Moves highlighted filter into Filter Expression box.
And button	Data must match all filters tied together with this operation.
Or button	Data can match both or any one of the filters tied together by this operation.
Not button	Data must match the first filter, but cannot match the second filter tied together by this operation.
GTP button in GTP Operations Section	Using GTP operations allows you to filter IP packets that contain a GTP layer by performing one of the following GTP operations within the GTP layer. <ul style="list-style-type: none"> • GTP Presence: Can be defined, if the GTP layer is contained in the packet. • GTP Control: Can be defined, if the GTP layer contains control plane or data plane.
Finish button (not shown)	Saves the information to the system.

6. Type in the **Filter Name**.
7. (Optional) Type in a **Description** of the Filter.
8. Type in or select a **Filter Expression** in the *Filter Expression* field.
9. Click **Select**.
The expression is added to the *Filters List*.
10. Select a **Logical Operator** (And, Or, Not), by clicking the appropriate *Operator*.

From the *pull-down* menu.

Note: IF you use a GTP filter in a combination filter, you may want to specify the “OR” condition with the GTP Control filter in order to pass GTP-C-PDUs.

Note: The VLAN filter can be used in the filter expression, but is limited to use of only 1 VLAN filter an expression. As an example, v1 and v2 are VLAN filters; f1 filter: Correct: v1 and f1 Correct: not (v1) and f1 Incorrect: f1 and v1 Incorrect: not (v1 and f1)

10. If applicable, click to select a GTP operation and specify the GTP expression within the parenthesis.

Note: An example of a correct GTP combination filter: GTP(src5000 and dest500) or GTPControl.

Note: An example of an incorrect GTP combination filter GTP(src5000 and dest500 and GTPControl)
The correct GTP filter has GTPControl outside of the GTP expression contained within the parenthesis.

11. Click **Done**.

The Combination filter is added to the *object tree* in alphanumerical order.

Modifying an IP Combination Filter

Complete these steps to modify an IP Combination filter.

1. Select the **IP Combination filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.

The changes are saved.

Deleting an IP Combination Filter

Complete these steps to delete an IP Combination filter.

1. Select the **IP Combination filter** to be deleted.
2. Select **delete** from the menu.
3. Click **OK** at the prompt.

The filter is deleted.

About Diameter Protocol Filters

Diameter PDU filters are used only when the Traffic Classification for a specific server is set to Diameter. (See "Setting System to Diameter Mode" for more information.)

Multiple Diameter filters can be created but only one filter can be used at a time. The specificity of the filter is based on a combination of any or all of the four components listed at the end of this topic.

Note: When adding a Diameter PDU filter, if the system recognizes Application, Command Code and Host (AND/OR logic) or Realm (OR logic), then the filter will pass the packet to IXP for correlation and storage.

Note: Diameter PDU filters can also be used when creating Combination Filters. (See About IP Combination Filters for more information.)

- Application
- Command Code
- Host
- Realm

Adding a Diameter PDU Filter

Note: When adding a Diameter PDU filter, if the system recognizes any of four components (OR logic filtering), then the filter will pass the packet to IXP for correlation and storage. The four components are represented in the following fields: Enter ApplicationID, Enter Command Code, Enter Host, Enter Realm.

Note: Diameter PDU filters can also be used when creating Combination Filters. (For more information, see "About IP Combination Filters.")

Complete these steps to add a Diameter PDU filter.

1. In CCM, select **Acquisition > PDU Filters** from the object menu.
The PDU Filters list screen opens.
2. Click **Add** on the tool bar (green + sign).
PDU Filter Family screen opens.
3. Select **Diameter - protocol**
4. Click **Next**.
The Diameter Filters screen opens.
The table describes the fields on this screen.

Table 40: Diameter Filter Screen Fields

Field	Description
Filter Name	Alphanumeric field providing name of the filter
Description	(Optional) Alphanumeric field for short description of the filter
Enter ApplicationID	Provides the numeric ID for the Application for the diameter filter Numeric field with range of 0- 4294967295
Enter Command Code	Numeric field that provides numeric ID for the 24-bit command code Numeric field with range of 0- 16777215
Enter Host To match Origin-Host or Destination-Host	Provides the Host ID for either the Origin or the Destination An alphanumeric field with no constraints Note: The name must be a Fully Qualified Domain Name (FQDN) For example: 123.xyz.com (where 123 = HSS or MME and xyz = domain)
Enter Realm To match Origin-Realm or Destination-Realm	Provides the Host ID for either the Origin or the Destination An alphanumeric field with no constraints Note: Just a Domain Name (DN) For example: xyz.com
Add button	Adds the a value of the parameter to the list Note: There can be multiple values of each parameter
Remove	Removes the value from the parameter list

Note: Any combination of the fields, ApplicationID, Command Code, Host and Realm can be used.

Note: The fields ApplicationID, Command Code and Host utilize both AND/OR functionality in order to make a filter more specific. The Realm field uses only OR functionality for inclusion.

For example, a simple filter with Command Code (C1) and Host (H1) would filter out all other possibilities that do not contain both of those fields (C1 AND H1). The same filter could include Realm (R1) along with Command Code and Host since the Realm field uses the OR functionality

(C1 AND H1) OR (R1). If there are multiple entities for a field (for example Command Code such as C1, C2), then the filter equation would be ((C1 or C2) and (H1)) or (R1)

5. Enter the **Filter Name**.
6. (Optional) Enter a **Description** of the Diameter filter.
7. Enter the **Application ID** (if one is used).
8. Click **Add** to add it to the Application list.
9. Enter a **Command Code** (if one is used).
10. Click **Add** to add it to the Command Code list.
11. Enter the **Host** (if one is used).
12. Click **Add** to add it to the Host (Origin or Destination) list.
13. Enter the **Realm** (if one is used).
14. Click **Add** to add it to the Command Code list.
15. Click **Finish**.

The filter appears in the PDU filter list.

Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

Modifying a Diameter PDU Filter

Complete these steps to modify a Diameter PDU filter.

1. Select the **Diameter filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.

Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

Deleting a Diameter PDU Filter

Complete these steps to delete a Diameter PDU filter.

1. Select the **Diameter filter** to be deleted.
2. Select **delete** from the tool bar.
3. Click **OK** at the prompt.

Note: To apply changes and update the xMF (PMF) system, select **Apply Changes...** from the Host right-click menu.

About PDU Dataflows

PDU Data Flows are used to group Linksets and/or Associations that are being captured on the PMF and deliver them to the IXP for protocol analysis and storage. The MSUs/PDUs are packaged and shipped to the IXP over an input stream (IP Stream). Once configured, the PDU Data Flows can be used by the IXP for processing xDR storage.

PDU dataflows are created for each specific PMF subsystem to route both filtered and unfiltered data to IXP for xDR creation. The PDU dataflows contain linksets which can belong to different servers across a subsystem or all together different subsystems. There are different categories of PDU dataflows defined to route different types of data.

CCM provides the capability to configure PDU Dataflows for each xMF subsystem. The capability allows for greater flexibility and quicker search capabilities when creating dataflows.

About IP Dataflows

PMF

When you create an IP dataflow, you select one or more ethernet devices connected to a selected PMF server. When an ethernet device, referred to as an IP device in the user interface, is assigned to a dataflow, the dataflow will forward all IP traffic related to the selected ethernet device to the IXP upon dataflow creation. If you wish to limit the IP traffic that is sent to the IXP, you must define and assign a filter to your dataflow filters.

Note: Way Management only provides directional information for IP addresses added to the IP address list. IP traffic data for unspecified IP addresses associated with the selected ethernet device(s) will still be forwarded to the IXP without the directional information.

XOR is a mechanism for load distribution of the messages to different ICPs and IXPs. The groups can comprise of exactly 2, 4, or 8 IXPs, hence XOR_2, XOR_4, and XOR_8. A dataflow with XOR_4 needs to be routed to destinations on the routing screen. Selecting any more or less than 4 would cause an error.

XOR preserves the call context. All messages belonging to one call are always forwarded to the same destination in order for correlation to be successful.

XOR allows a dataflow with higher throughput of traffic to be load shared to a group of IXPs.

Note: To create an IP data flow, IP filters have to be already defined and the link-based network views used for specifying the IP source has also to be defined.

Adding an IP Dataflow

Complete these steps to create an IP dataflow.

1. Select **Acquisition > Site > PDU DataFlows > IP**.

The IP Dataflow list screen opens.



Figure 69: IP DataFlow List Screen

2. Click **Add**.
The Add screen opens.

IPDataFlow Info

Name

Description

Figure 70: IP DataFlow Add Screen

3. Type in the **Name** of the IP dataflow
4. (Optional) Type in a **Description** of the dataflow record.
5. Click **Next** to move to the IP Data Flow Load Share Configuration screen.

Table 41: Add / Modify IP DataFlow Screen Fields

Section	Field	Description
Load Sharing	Is a set of fields where you can set number of destinations and utilize either GTP user plane, GTP control plane or both for load sharing.	
	Load Sharing Across "N" destinations	Pull-down field (0, 2-8) <ul style="list-style-type: none"> • 0 is default and no load sharing is available. • 2 or greater enables you to load share.
	Utilize GTP User Plane For Load Share Algorithm	Check box - must have minimum of two destinations for load sharing
	Send GTP Control Plane To All Load Share Destinations	Check box - must have a minimum of two destination for load sharing
Send Traffic Classification Counters Only		Check box to select if only counters are used. Use this when not load sharing.
Enter IP Address for Way Management		Allows you to define a list of IP addresses you want directional information for. When selected, IP packet data forwarded to an IXP will include information about the direction of the packet in relation to IP addresses defined in the Ip List.

Section	Field	Description
		<p>If this is not selected, IP address directional information is not be included in the information sent to the IXP.</p> <ul style="list-style-type: none"> • Host-Address: Point-to-point. For example, 10.25.130.22 • Network-Address: Monitors whole network. For example, entering 10.254.100.32/27 includes all IP addresses between 10.254.100.32 - 10.254.100.63.
Add to list button		When clicked, adds value in Ip Address field to the Ip List field.
IP Address List		Shows the IP addresses subject to Way Management for this dataflow. You can add to or remove IP addresses from this list. If Way Management is not selected, then this field is irrelevant to the dataflow.
Remove from list button		Deletes IP addresses from the Ip List field. When an IP address is deleted from the IP List, it is no longer subject to Way Management.
Reset / Cancel Previous / Next		<p>Click on one of the following:</p> <ul style="list-style-type: none"> • Reset: Restores original settings. • Cancel: Information is not saved. • Previous: Returns you to the Add IP Dataflows screen. • Next: The Add IP Dataflows Network View screen opens.

- (Optional for Load Sharing) Select the number of **Destinations** that will be used in load sharing (must be two or more).
- (Optional) Select whether the system should utilize the **GTP User Plane** for load sharing action.
- (Optional) Select (or not) whether the system should utilized the **GTP Control Plane to all shared destinations**.
- Type in a valid **IP Address(es)**.
- Click **Add to list** to add the IP address is added to the IP Address list.
- Click **Next** to move to the IP Data Flow Truncation Configuration screen.
- Enter a **Packet Truncation** value (integer).
- (Optional) Select any **Annotations** you want to be associated with the dataflow.
- Click **Next** to move to the IP Data Flow Stream Configuration screen.
The Traffic Classifications screen opens.

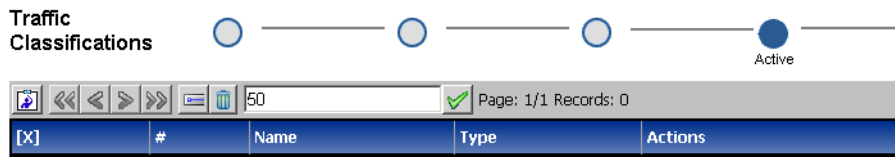


Figure 71: Traffic Classifications Screen

15. Click **Select Traffic Classifications** on the tool bar.

The Traffic Classification Selector screen opens.

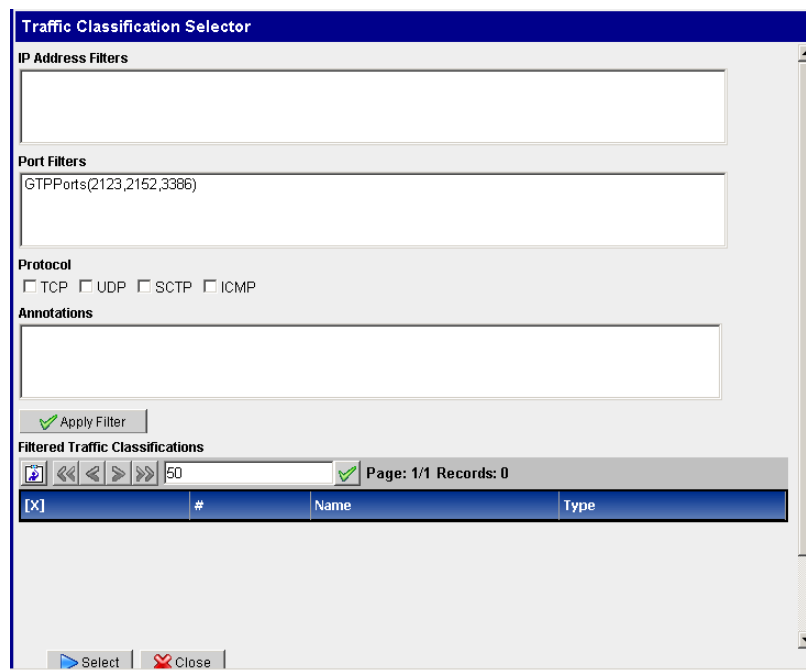


Figure 72: Traffic Classifications Selector Screen

16. Select either an **IP Address Filter** or a **Port Filter**.
17. Select a **Protocol**
18. Select an **Annotation**.
19. Click **Apply Filter**.
The Filter appears in the bottom table.
20. Click **Select**.
The Traffic Classification is added to the dataflow.
21. Click **Add**.
The IP Dataflow is added to the system.
22. You must now **apply changes** for the changes to take effect in the subsystem.

Modifying an IP Dataflow

Complete these steps to modify an IP dataflow.

1. Select the **IP dataflow** record to be modified.
2. Click **Modify**.
The *Modify* screen opens.
3. Make the necessary modifications.
4. Click **Modify**.
The changes are saved.
5. You must now **synchronize** the subsystem.

Deleting an IP Dataflow

Complete these steps to delete an IP dataflow.

Note: You must de-select any IP stream that is associated with an IP dataflow before deleting it.

1. Select the **IP dataflow** record to be deleted.
2. Click **routes**.
The bottom table changes to show the Input streams for the dataflow.
3. Click **streams**.
The streams selection screen opens.
4. De-select all the **selected streams**.
5. Click **Apply**.
6. Click **Delete** on the selected dataflow.
7. Click **OK** at the prompt.
The record is deleted.
8. You must now **synchronize** the subsystem.

About Alarms

Various types of alarm-related parameters are managed through CCM. Alarm management includes enabling/disabling alarms, setting threshold levels as well as other functions. The DIH system receives alarms from the monitored network as well as the various applications generate alarms based on PDUs received, traffic condition, etc. In addition, users can configure ProTraq statistical sessions and set alarm thresholds. This release of CCM supports the management of alarms that are either received by or generated by the PMF subsystem. This release of CCM supports these operations at a global level. For example, if the user enables or disables a particular type of alarm, the action takes effect for all sites. By default all the alarms are enabled. You have to explicitly disable alarms.

Managing Platform Alarms

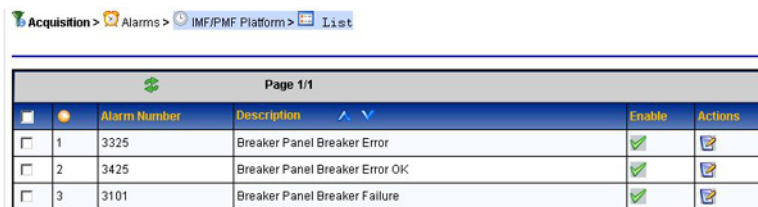
This section describes how the platform alarms are enabled or disabled by the CCM application. The PMF server comes with system-level software that can detect hardware and operating system-level failure and report them to the PMF system. You can enable or disable forwarding of such alarms globally.

Enabling and Disabling Platform Alarms

Complete these steps to enable or disable a Platform alarm.

1. Select **Acquisition > Alarms > PMF Platform > List**.

The *Alarms Configuration* screen opens shown below.



Page 1/1					
		Alarm Number	Description	Enable	Actions
<input type="checkbox"/>	1	3325	Breaker Panel Breaker Error	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2	3425	Breaker Panel Breaker Error OK	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	3	3101	Breaker Panel Breaker Failure	<input checked="" type="checkbox"/>	

Figure 73: Alarms Configuration Screen

2. Select the **Alarm** to be enabled or disabled.
3. Click **modify** the *Modify Platform Alarm Configuration* screen opens with the alarm record details.
4. Enable or disable the alarm.
 - a) Enable - select the **Enable** check box.
 - b) Disable - click on the **Enable** check box to remove check mark.
5. Click **Done**.

The modifications are saved and you are returned to the alarm list.

Note: To update the alarm list, click the *Refresh* button on the toolbar. The list is updated to show the latest changes.

Chapter 10

IXP Mediation

Topics:

- *About Mediation Perspective.....145*
- *About Managing each IXP Subsystem.....145*
- *About IXP Storage Servers.....152*
- *Configuring Servers in an IXP Subsystem.....154*
- *About Streams.....155*
- *Configuring xDR Dataflow Processings.....159*
- *About Distributions.....195*
- *Managing Multiple IXP Subsystems.....198*
- *About Dictionaries.....198*
- *About xDR Filters.....206*
- *About Sessions.....209*
- *About Enrichment Files.....216*

About Mediation Perspective

The *Mediation* perspective enables you to manage the IXP, (and Data Warehouse (DWH)), subsystems. The entire configuration in this perspective is designed to configure dataflow processings, data sources, input streams, xDR filters, distributions, platform parameters of xDRs in either a DWH or IXP subsystem.

About Managing each IXP Subsystem

The Mediation perspective object tree has the Site object where you can manage IXP subsystems belonging to a particular site. Once you have discovered all the elements of each IXP subsystem, you go to the *Mediation* perspective to configure the subsystem.

In addition, once the subsystem is discovered, you can click on the subsystem in the Mediation perspective to view a platform overview of the system.

Properties		Value			
Subsystem name		ixp0777			
User Information		Auto-generated sub-system			

Host Name	Type	IP Address	Last Update	User Information
ixp0777-1a	Primary	10.250.42.166	2009-07-20 04:12:44.0	
ixp0777-1b	Secondary	10.250.42.167	2009-07-20 04:13:56.0	
ixp0777-1c	Spare	10.250.42.168	2009-07-20 04:13:57.0	

DWH Server Name	IP Address	State
ixp0777-1a_DWH	10.250.42.166	ACTIVE

Server	Dataflow Processing	Type	Active	Input Stream(s)	Output Stream(s) / Session
ixp0777-1a	StreamMonitor	Storage	✓	ixp0777StreamMonitor	ixp0777StreamMonitor
	BuildMonitor	Storage	✓	ixp0777BuildMonitor	ixp0777BuildMonitor
	OperateMonitor	Storage	✓	ixp0777OperateMonitor	ixp0777OperateMonitor
	StoreMonitor	Storage	✓	ixp0777StoreMonitor	ixp0777StoreMonitor
ixp0777-1b	de_test_isup_ansi	Building	✓	DE_TEST_ISUP_ANSI	B_de_test_isup_ansi_7
	BSS_RANCC_DF	Building	✓	BSS_STREAM	B_BSS_RANCC_S_9
	BSS_TDR_DF	Building	✓	BSS_STREAM	B_BSS_TDR_S_10
	FCT-328	Building	✓	FCT-328_FCT-328_ixp0777	B_FCT_328_M2PA_STAT B_FCT_328_M2PA_SUDR
	BSS_RANCC_S_11	Operation	✓	B_BSS_RANCC_S_9	O_BSS_RANCC_S_12 K_KPI_BSS_RANCC_S_C K_KPI_BSS_RANCC_S_C
	BSS_TDR_S_17	Operation	✓	B_BSS_TDR_S_10	O_BSS_TDR_S_18 K_KPI_BSS_TDR21July_S K_KPI_BSS_TDR21July_S
	S_de_test_isup_ansi	Storage	✓	B_de_test_isup_ansi_7	de_test_isup_ansi
	S BSS RANCC S	Storage	✓	O BSS RANCC S 12	BSS RANCC S

Figure 74: IXP Subsystem Overview

Note: You must explicitly apply all IXP configuration changes to each IXP subsystem. You are prompted if there is any change to the subsystem by a message banner at the top of the screen.

About IXP Subsystem Functions

The general maintenance and configuration options for a specific IXP subsystem are accessed by right-clicking on the selected IXP subsystem. (Select **Sites > subsystem**.) The pop-up menu opens, shown below. The options are described in the table and sections below.

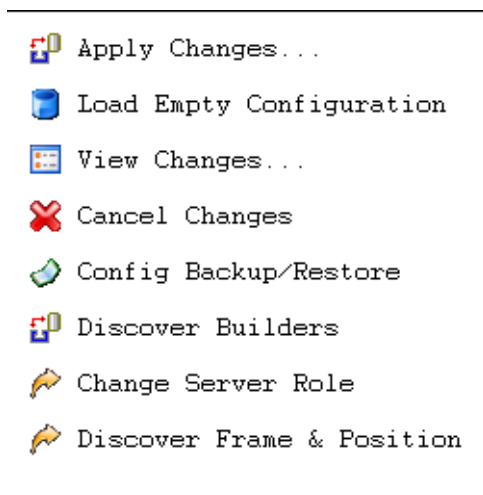


Figure 75: Subsystem Pop-Up Menu

Table 42: IXP Subsystem Pop-Up Menu Options

Option	Description
Apply changes	enables you to apply any changes that have been made to the particular IXP subsystem. You are notified if there are any changes to the system and you use this option to accept the changes.
Load Empty Configuration	enables you to configure an IXP subsystem by using a template configuration.
View changes	enables you to view any changes that have occurred in the subsystem in order to accept the change or cancel them.
Cancel changes	enables you to cancel any changes that have been made to the subsystem.
Config backup/restore	enables you to backup or restore a previous backup configuration in case of system failure.
Discover Builders	enables you to discover xDR builders for the subsystem if upgrades to builders have been installed on the system.
Modify server roles	enables you to change the role of a server
Synchronize Frame and Position	enables you to sychronized the subsystem after you have modified the frame and position of a host in the IXP subsystem.

About Applying Changes to an IXP Subsystem

Note: To apply changes to a subsystem you need to be assigned the role *NSPConfigManager*.

Anytime you add, modify or delete an object in an IXP subsystem, you need to synchronize the subsystem so that the changes are recognized by the DIH system. CCM has a IXP subsystem prompt option that alerts you to any changes that have occurred.

Configuration has occurred on the following IXP subsystems: *IXPSubsystemName*, changes must be applied or cancelled.

Complete these steps to apply changes to a subsystem.

1. Select the **subsystem** that has been modified.
2. Right-click and select **apply changes...** from the pop-up menu.
CCM displays the configuration changes that will be applied to the selected IXP subsystem. At this point, you are prompted if you want to continue, cancel, or undo.
3. Click **Continue**.
The configuration is validated and any warning messages are displayed.
Note: If there are warnings, you are prompted if you still want to apply changes.
4. To apply changes, click **Apply**.

Viewing Changes to an IXP Subsystem

Complete these steps to view the most recent synchronization and any pending changes on an IXP subsystem.

1. Select **Mediation > Site > IXP subsystem**.
2. From the subsystem right-click menu select **View Changes**.
The screen shows the time and date of the last synchronization and any pending changes in the bottom table.

Enabling and Disabling IXP Subsystem Automatic Failover

Complete these steps to enable or disable the automatic failover for an IXP subsystem.

1. Select **Mediation > Site > IXP subsystem**.
2. Right-click and select **Enable / Disable Auto Failover**.
Note: Enabling and disabling an IXP subsystem can also be performed from the Actions column in the IXP list screen.
3. Select either **Enable** (default setting) or **Disable**.
4. Click **Done**.
Note: For the changes to take affect, click **Apply Changes**.

Loading an Empty Configuration on to an IXP Subsystem

Complete these steps to load an empty configuration on an xMF subsystem.

1. Select the **Acquisition > Site > xMF subsystem**.

2. From right-click menu select **Load Empty Configuration**

Note: A warning appears stating that loading an empty configuration un-route PDU dataflows at the associated PMF subsystem. (For more information, see *Avoiding Lost PDU Routes Due to Cancel Changes on an PMF subsystem.*)

3. To continue to load an empty configuration, click **OK**.

Note: For changes to take effect, click **Apply Changes** from the subsystem right-click menu.

Cancelling Changes to an IXP Subsystem

You can cancel changes to a subsystem by using the *Cancel Changes* option.

Note: Choosing "Cancel Changes" on an PMF subsystem removes the existing configuration (any changes that have occurred) of that subsystem and restores the latest applied (active) configuration which includes Card/Port/Link Mapping and Traffic Classifications (TCs) for PMF. Feeder Thresholds, PMF subsystem parameters and PDU dataflows are preserved (but the PDU routes are not preserved). This action also enables the "Apply Changes" banner for that PMF subsystem. PDU dataflow routing can be restored either by modifying the Build DFPs on the IXP subsystem in order to re-associate the dataflows with the DFPs, or by restoring the last applied configuration on the IXP subsystem that contains the Build DFPs (see next note for constraints on restoring IXP).

Complete these steps to cancel changes for a subsystem. Again, if any changes have occurred, you are prompted with this message:

Configuration has occurred on the following IXP subsystems: *IXPSubsystemName*, changes must be applied or cancelled.

Note: To apply changes to a subsystem you need to be assigned the role *NSPConfigManager* or *NSPAdministrator*.

1. Select the **subsystem** that needs to have the changes cancelled.
2. Right-click and select **Cancel changes** from the pop-up menu.

CCM displays the configuration changes that will be applied to the selected IXP subsystem. At this point, you are prompted if you want to continue, cancel, or undo.

3. Click **Undo**.

The last configuration that was applied to the IXP subsystem is reloaded.

Backup and restoring an IXP Subsystem

CCM has a **backup/restore** function that enables you to backup and archive the IXP configuration per subsystem. CCM also has a option to restore the IXP configuration from an archived backup. This option enables you to bring the configuration of an IXP subsystem to any previously working state.

Complete these steps to backup or restore an IXP subsystem.

Note: To apply changes to a subsystem you need to be assigned the role *NSPConfigManager*.

1. Select the **subsystem** that needs a backup.
2. Right-click and select **Config Backup/Restore** from the pop-up menu.

CCM displays a table of named archived backups.

	BackUp Name	Active	Actions
<input type="checkbox"/>	1 IxpConfig_Mon Jul 28 10:45:30 UTC 2008	Yes	
<input type="checkbox"/>	2 IxpConfig_Mon Jul 28 10:17:51 UTC 2008	No	
<input type="checkbox"/>	3 IxpConfig_Mon Jul 28 09:05:45 UTC 2008	No	
<input type="checkbox"/>	4 IxpConfig_Mon Jul 28 08:43:12 UTC 2008	No	
<input type="checkbox"/>	5 IxpConfig_Mon Jul 28 07:25:20 UTC 2008	No	
<input type="checkbox"/>	6 IxpConfig_Mon Jul 28 06:59:57 UTC 2008	No	
<input type="checkbox"/>	7 IxpConfig_Mon Jul 28 06:37:59 UTC 2008	No	
<input type="checkbox"/>	8 IxpConfig_Mon Jul 28 03:58:34 UTC 2008	No	

Figure 76: Archived List Of Configurations

3. Click **Add**.

CCM automatically names the backup and stores a configuration backup in the NSP database. CCM maintains up to nine backups per subsystem.

Deleting an archived Backup

You can also delete an archived backup file by using the delete function described here. Complete these steps to delete a backup file.

Note: To apply changes or delete a subsystem you need to be assigned the role *NSPConfigManager*.

1. Select the **subsystem** that needs backups deleted.
2. Right-click and select **Config Backup/Restore** from the pop-up menu.
CCM displays a table of named archived backups.
3. Select the **archived version** that you want from the list.
4. Click **Delete**.
5. Click **OK** at the prompt.

The archived backup is deleted from the list.

Discovering xDR Builders

You use the *Discover xDR builders* option if there has been an update to the xDR builders on your IXP subsystem. Complete these steps to discover xDR builders for a specific IXP subsystem.

1. Select and right-click on the **IXP subsystem** that needs the builders.
2. Select **Discover Builders** from the pop-up menu.

The system begins the discovery process. The *Discovery* screen opens shown below.

	Name	Version	Remote Status	Action Taken
<input type="checkbox"/>	1 VoIP MGCP Decoding	1.2.1.3	No Change	Discovered - No Change
<input type="checkbox"/>	2 IP MMS	5.0.1.4	No Change	Discovered - No Change
<input type="checkbox"/>	3 VoIP SIP Decoding	2.4.1.5	No Change	Discovered - No Change
<input type="checkbox"/>	4 VoIP G931 Decoding	1.0.0.6	No Change	Discovered - No Change
<input type="checkbox"/>	5 Initial step	1.1.0.0	No Change	Discovered - No Change
<input type="checkbox"/>	6 IP Smppt Intermediate	1.0.0.0	No Change	Discovered - No Change
<input type="checkbox"/>	7 VoIP H248 Decoding	1.1.1.3	No Change	Discovered - No Change
<input type="checkbox"/>	8 VoIP MEGACO Decoding	1.2.0.7	No Change	Discovered - No Change
<input type="checkbox"/>	9 SS7 Transport	1.1.0.1	No Change	Discovered - No Change

Figure 77: Discovery Results Screen

- The *Results* screen shows any changes to the builders (additions, deletions, errors or builders that showed no change).

Discovering Frame and Port Position

You use the Discover Frames and Position option if there has been an update to the IXP subsystem. Complete these steps to discover the frames and positions for a specific IXP subsystem.

- Select and right-click on the **IXP subsystem** that needs the discovery process.
- Select **Discover Frames and Positions** from the pop-up menu.
The discovery process begins. When completed a prompt appears stating, "Discovered Frame * Position for all hosts under subsystem - name of subsystem."

Modifying a server Role

Server roles (primary/secondary/ancillary server roles) are designated for each IXP server by CCM the subsystem and applications are discovered. CCM assigns primary status only to the server that has *1a* designation. Secondary status is designated to the sever labeled *1b* and ancillary status to the rest if the servers (*1c*, *1d*, *1e*, etc.). The order of discovery of the hosts does not matter. If you need to switch a server role, say, switching a primary to secondary, you are automatically directed to *Apply Changes* screen where changes have to be manually activated on the IXP subsystem.

Changing a Primary Server Role

Complete these steps to change the primary server role.

- Select and right-click on the **IXP subsystem** for the role change.
- Select **Modify Server Roles** option.

The role change screen opens for changing the primary and secondary server roles shown below.

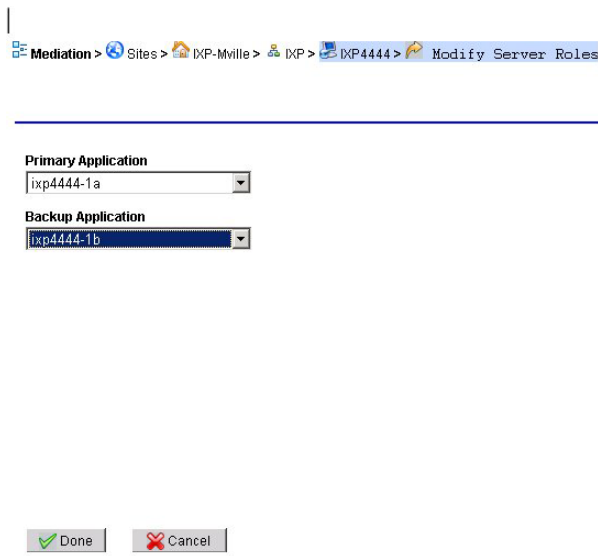


Figure 78: Server Role Change Screen

3. Select the **server** to be the primary application.
4. Select the **server** to be the secondary application.
5. Click **Done**.

The request is submitted to the system and CCM invokes the NSP server to perform the change role process. CCM updates the display indicating that the discovery request was successful.

About IXP Storage Servers

Once you have added an IXP subsystem in the Equipment Registry, that IXP subsystem is visible in the *Mediation* perspective. From this perspective you view the storage servers that have been assigned to that subsystem. By selecting **Mediation > Site > IXP Subsystem > Servers > Storage**. The list of storage servers opens.

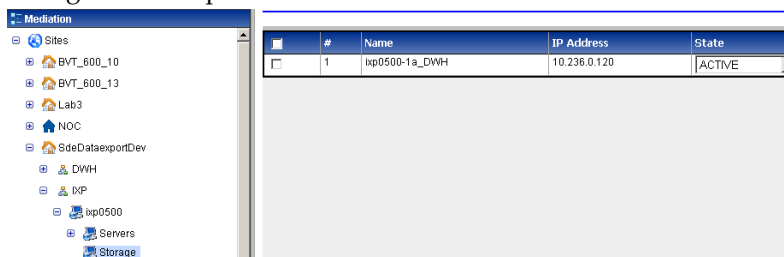


Figure 79: Storage Server Object and List Table

Changing the State of a Storage Server

Complete these steps to change the state of an IXP storage server.

Note: If an IXP storage server is in "Query" state, no configuration actions can be undertaken. All servers must be in "Active" state when sessions are created for queries on such sessions to be successful. Otherwise, if a query is launched in ProTrace on a newly created session, a "Unable to execute query: ORA-00942: table or view does not exist." will appear.

1. Select **Mediation > Site > IXP Subsystem > Server > Storage.**

The storage server list screen opens.

2. Select the **State** from the pull-down menu in the State column.

#	Name	IP Address	State
1	ixp0500-1a_DWH	10.236.0.120	ACTIVE

Figure 80: Add Screen

3. Click **OK** at the prompt.

The state is changed.

IXP Storage Pool States

You can manage an IXP storage pool by managing the state of the server on the specific subsystem. Each state also has an effect on an NSP application. These tables show the states and the effect on specific applications.

Table 43: Storage Pool Server States

State	Description
Active	Normal (default) state. Data being written and read from the server.
Maintenance	This state is designated if there is maintenance being performed on the server, for example, changing disk or upgrading RAM. There is no ability to query or to write any data.
Query Only	This is a transitional state between active and maintenance used for not missing any data. The server will be accessible to be read by applications, such as Data Feed Export and ProTraQ, to gain their information before the state moves to maintenance.

Values associated with each state.

Note: If an IXP storage server is in "Query" state, no configuration actions can be undertaken. All servers must be in "Active" state when sessions are created for queries on such sessions to be successful. Otherwise, if a query is launched in ProTrace on a newly created session, a "Unable to execute query: ORA-00942: table or view does not exist." will appear.

Table 44: Values Associated with each State

Value in Cell	Description
OK	Applications behave normally.
(Warning) Ignore Server	During operation, application will ignore server status and continue to reading, but providing a warning that data could not be accessed from a specific subsystem.
Suspend	Application will suspend any operation and wait until server has restored functionality.
Ignore Server	During operation the application ignores the server (from the storage pool) for reading and provides xDRs from other servers.

Table 45: NSP Applications Effected by Each State

Application	Active	Query Only	Maintenance	Down
ProTrace	OK	OK	Ignore Server (Warning on prompt)	Ignore Server (Warning on prompt)
ProPerf	OK	OK	Ignore Server (Warning on prompt)	Ignore Server (Warning on Prompt)
Data Feed	OK	OK	Ignore Server	Suspend
Historical KPI	OK	OK	Ignore Server	Suspend
Scheduled Export	OK	OK	Ignore Server (Show text warning in the exported archive)	Suspend

Configuring Servers in an IXP Subsystem

Once you have added an IXP subsystem in the *Equipment Registry*, that IXP subsystem is visible in the *Mediation* perspective. From this perspective you can perform the following procedures on servers in that IXP subsystem:

Note: The first two topics in the list are to be accomplished first. For example, you create input streams before you create dataflow processings. The other topics are used to manage the dataflow processings you have created.

- List the servers on an IXP subsystem
- Monitor storage capacity on a DWH server
- Manage the sessions on that IXP subsystem

- Manage the external PDU streams on that IXP subsystem
- Manage input streams on that IXP subsystem
- Manage the dataflow processings on that IXP subsystem
- Manage configuration for Q.752 processing on that IXP subsystem
- Manage the distribution on that IXP subsystem for load balancing or during server maintenance
- Manage the xDR builders on that IXP subsystem
- View software information associated with that IXP subsystem
- Manage the subsystem preferences for that IXP subsystem

About Streams

Streams are the connectors that enable PDUs to be routed from xMFs to IXPs. The two kinds of streams that can be created on an IXP subsystem are:

- PDU - that originate from PDU dataflows, which are created in xDR subsystems, these streams serve as the input streams to xDR Build dataflows
- xDR - that originate from *external* IXP subsystems, legacy or current, and are connected to an XDR input stream.

Note: The XDR input stream name needs to match the stream name of the legacy subsystem.

Note: CCM supports up to 500 streams (including PDU as well as xDR) per IXP subsystem. As soon as user crosses 255 streams per IXP subsystem, CCM places a constraint on each server with in the IXP subsystem that it cannot exceed 127 streams and shows an error message when changes are applied to the subsystem.

Every *unused* stream is counted for each IXP server for the corresponding IXP subsystem. An *unused* stream means streams that are not used by any IXP server. Unused streams are listed in the warning tab when applying changes to the corresponding IXP subsystem.

For example, one IXP subsystem consists of three servers and each server uses 100 streams. If a user has created a stream that is not used by any process, then CCM recognizes this *unused* stream as an extra stream for each server so that *each* server now have 101 streams.

In addition, all monitoring (system generated) and MFP based streams are also counted for each IXP server.

Selecting **Site > IXP Subsystem >Streams** in the object tree shows a list of the streams for that server.

#	Stream Name	Stream Type	User Information	Use RID	Critical
1	K_ixp0456AggSessionMonitor_127	xDR	Created for KPIs		✓
2	O_ixp0456PoolMonitor_126	xDR	Created for KPIs		✓
3	ixp0456BuildMonitor	xDR	Created for BuildMonitor by lxp.		✓
4	ixp0456OperateMonitor	xDR	Created for OperateMonitor by lxp.		✓
5	ixp0456PoolMonitor	xDR	Created for PoolMonitor by lxp.		✓
6	ixp0456StreamMonitor	xDR	Created for StreamMonitor by lxp.		✓

Figure 81: Streams List

Adding a PDU Stream

Input streams are constructs for grouping dataflows for the purpose of routing to one or more xDR builders. The grouping is done so that PDUs belonging to a dataflow are routed over a single communication stream to an xDR generator, resulting in optimized data collection resources.

Complete these steps to add a PDU stream.

1. Select **Mediation > Sites > IXP > IXP Subsystem > Streams**.
2. Click **Add** from the tool bar.

The screenshot shows a web form titled 'Add Streams'. It contains the following elements:

- Stream Name:** A text input field.
- Stream Type:** Two radio buttons, 'Pdu' (selected) and 'xDR'.
- Use RID:** A checkbox.
- Critical:** A checkbox.
- User Information:** A text area with a vertical scrollbar.

Figure 82: Add Streams Screen

3. Type the **Stream Name**.
4. Select the **Stream Type** (PDU).
5. (Optional) Select whether to **Use RID** or not.
6. Select whether the stream is **critical** or not.

Note: The critical field in the stream creation screen is used to indicate the behavior of a given dataflow processing when it is fed by multiple input streams. When the critical box is activated, it designates that the dataflow processing will stop processing PDU's/XDRs if any critical input stream stops having traffic. When the field is not selected, it indicates the dataflow processing will continue to process data even if some of the streams have no traffic.

7. (Optional) Enter any pertinent **User Information**.
8. Click **Create**.

The stream is added to the list.

Adding an xDR Stream

Complete these steps to add an xDR stream from one IXP subsystem to be used for input to an external IXP subsystem.

Note: To add an xDR stream there must be more than one IXP Subsystem available. xDR streams are created when external streams, streams from some other IXP subsystem so that xDRs from one IXP are taken as input on another IXP, are needed.

1. Select **Mediation > Sites > IXP > IXP Subsystem > Streams**.
2. Click **Add** from the tool bar.
3. Select the **xDR** as the stream type.
4. Select the **IXP subsystem** that contains the xDR stream.
5. Select an **xDR Stream** from the list.
6. (Optional) Select if the stream is to **Use RID**.
7. (Optional) Select whether the stream is **critical** or not.

Note: The critical field in the stream creation screen is used to indicate the behavior of a given dataflow processing when it is fed by multiple input streams. When the critical box is activated, it designates that the dataflow processing will stop processing PDU's/XDRs if any critical input stream stops having traffic. When the field is not selected, it indicates the dataflow processing will continue to process data even if some of the streams have no traffic.

8. (Optional) Enter any pertinent **User Information**.
9. Click **Create**. The system creates an external stream with the same name as on the external IXP subsystem.

Click **Apply Changes** for the IXP subsystem for the changes to take effect.

Modifying a Stream

1. Select **Streams > List**.
2. Select the **stream** to be modified.
3. Click **Modify**.

The screen for that stream opens shown below.

Mediation > **Sites** > **TEST** > **IXP** > **ss-27** > **Streams** > **List**

Stream Name
dts0

Stream Type
 Pdu xDR

Use RID

Critical

User Information

Reset Cancel Modify

Figure 83: Stream Modify Screen

4. Make the necessary modifications.
5. Click **Modify**.

The system is updated and you are returned to the *Streams List* screen with the modifications.

Deleting a Stream

Note: You cannot delete a stream that has dataflow processings associated with it. If the stream does have any dependencies, you will get an error message.

Complete these steps to delete a stream.

1. Select **Streams > List**.
The streams list screen opens.
2. Select the **stream** to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.
The stream is deleted from the list.

Configuring xDR Dataflow Processings

The most important aspect of IXP configuration is the creation of xDR Dataflows. An xDR Dataflow is made of interconnected processes referred to as *dataflow processings*.

Dataflow processings are categorized into three types listed in the order that they should be created:

1. Building - this dataflow processing creates or builds xDRs
2. Operation - this dataflow processing generates statistics and applies filters for data enrichment
3. Storage - this dataflow processing stores information on the system

About Dataflow Processings

Dataflow Processing is the receiving end from a PDU Stream or PDU Dataflow as configured on the PMF. The Dataflow Processing configuration is used to build a xDR for storage on the IXP. The configuration is required based on the protocol and type of post-processing prior to storage on the IXP. Once a Dataflow Processing has been configured, the IXP will start receiving MSUs/PDUs from the PMF over the input stream that was created for the PMF PDU Data Flows.

About Dataflow Processing Retention Times

Dataflow Processing chains are the normal sequence of processes that correlation goes through until xDRs are stored in the IXP. Each DFP has a retention period in seconds. The retention time is the duration of PDUs or xDR retention in the chronological sorting list that is used to buffer input to the IxpBuild, IxpOperate and IxpStore processes.

Note: The IxpStore process has an additional turning parameter called a flush timeout. The flush timeout is the frequency of the xDR buffer flushing in the IxpStore process, (xDR writing to Oracle), when the maximum size of a buffer is not reached.

Both the retention time and the flush timeout have a direct impact on the time between the transmission (by xMF) of the PDU opening a transaction and the writing of the corresponding xDR into the Oracle database. The valid range for these parameters is 0-60 seconds. The default value for these parameters is 5 seconds.

These parameters are specific to each DFP instance so that you can fine tune a DFP according to the protocol type it uses. For example, more retention is needed when the sources come from a pair of mated STP (2 sources) and less retention time is needed when the DFP is using a single IP tap.

Note: If the retention time is too small (depending on the network configuration), there is a possibility of an incorrect correlation. The impact can occur when the retention time is acceptable for ProTrace performance but unacceptable for creating valid correlation rates.

Listing xDR Dataflow Processings

To view a list of all the dataflow processings on a server, select **dataflow processings** in the object tree. The list opens in the Table section shown here.

From this screen, you can perform the basic functions of adding, modifying and deleting a dataflow processings. In addition, you are able sort the rows by clicking on a column of interest.

Name	Type	Input Streams	Output Streams (Out Sessions)	Active	Actions
1 S_dfa_store_28_1_8	Storage	S_dfa_store_28_1_7	dfa_store_28_1	<input type="checkbox"/>	
2 dfa-test2	Building	ss166_in	S_dfa_store_5_28_2_9	<input type="checkbox"/>	
3 dfa-1	Building	ss166_in	S_dfa_store_28_1_7	<input type="checkbox"/>	
4 S_dfa_store_5_28_2_10	Storage	S_dfa_store_5_28_2_9	dfa_store_5_28_2	<input type="checkbox"/>	

Figure 84: Dataflow Processings List

Table 46: Dataflow Processings List Table

Column	Description
Select	This column enables you to select a dataflow processing. Use this column when selecting multiple sessions.
Hide/show columns	This column enables you to select the columns you want to view.
Name	Shows the name of the dataflow processing and enables you to sort dataflow processings by ascending or descending order. .
Type	Shows the type of session: Storage Operation Building
Input (streams)	Shows the name of the input stream for the dataflow processing.
Output stream	Shows the name of the output stream for the dataflow processing
Active	Is a check box showing whether the dataflow processing is active or not.
Actions	Provides the appropriate actions (modify, delete, etc.) you can perform on the dataflow processing.

About xDR Dataflow Assistant

The xDR Dataflow Assistant option provides a wizard to help you quickly create a dataflow processing. It is a convenient way to add large numbers of xDR Dataflows. The *xDR Dataflow Processing Assistant* assists you with creation of an xDR Dataflow, a chain of IXP Dataflow Processings more efficiently. The process follows four stages:

- Selecting the input PDU sources
- Selecting the xDR Builders
- (Optional) Enriching the xDRs
- Creating or reusing sessions to store xDRs

About Dataflow Naming Conventions

Depending on the input, the xDR Dataflow created will result in the following types of Dataflow Processings.

- One *Build* dataflow processing,
- Zero or more *Operate* dataflow processings,
- Multiple *Storage* dataflow processings.

All the dataflow processings and the intermediate streams are automatically created and named by CCM. The table shows examples of naming conventions used by CCM.

Table 47: Dataflow Processing Naming Conventions

Dataflow Processing Type	Naming convention
Build dataflow processing	User Input
Operation dataflow processing	< name of the session fed by the main stream>_<dataflow processingId> (mandatory)
Storage dataflow processing	S_<corresponding session name>_<dataflow processingId>
Building dataflow processing output stream	B_<corresponding xDR session name>_<streamId>
Operation dataflow processing main output stream (xDRs)	O_<corresponding xDR session name>_<streamId>
Operation dataflow processing secondary output stream (KPIs)	K_<corresponding KPI session name>_<streamId>

Creating a Dataflow Processing Using xDR Dataflow Assistant

The most important aspect of IXP configuration is the creation of xDR Dataflows. An xDR Dataflow is made of interconnected processes referred to as dataflow processings. Dataflow processings are categorized into three types listed in the order that they should be created:

- Building - this dataflow processing creates or builds xDRs
- Operation - this dataflow processing generates statistics and applies filters for data enrichment

- Storage - this dataflow processing stores information on the system

Note: If you do not have licenses to use specific xDR builders, the builder selection screen will not show them.

Configure dataflow processings using the xDR Dataflow Assistant.

Note: Because Q.752 processings utilize input streams, you must first create your input streams or PDF dataflows before you create your Q.752 processings.

1. Select **IXP subsystem > Subsystem** that needs dataflow processings.
2. Right-click on the **Subsystem**.
The pop-up menu opens.
3. Right-click on **Dataflow Processings**.
4. Select **xDR Dataflow Assistant** from the pop-up menu.

The first screen of the wizard opens in the *Table* section shown here.

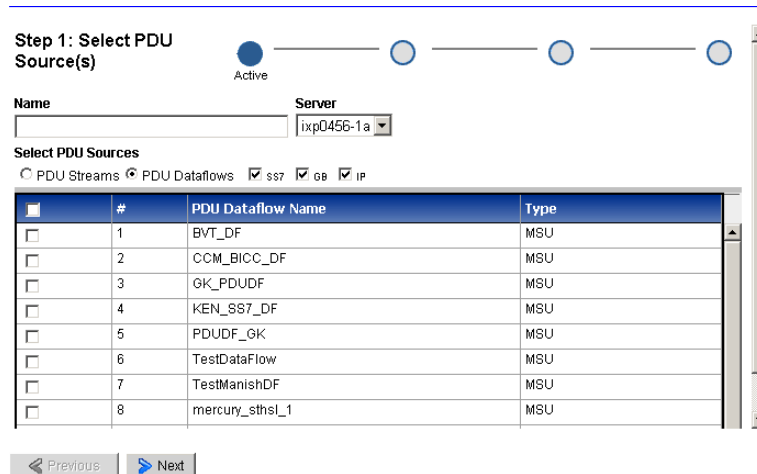


Figure 85: xDR Dataflow Assistant Initial Screen-PDU Sources

5. Type in the **Name** of the Dataflow Process.
6. Select the **server**.
Note: Do not use the DWH as the server for the Dataflow Process.
Note: If multiple dataflow processes are created, it is recommended that more than one server be used to facilitate load balancing.
7. Select a **PDU Source** from the table.
You can filter by selecting what type of source you want to view/use. Whether its a Stream or Dataflow and what category (SS7, Gb, IP)
8. Click **Next** to choose an xDR Builder shown below.

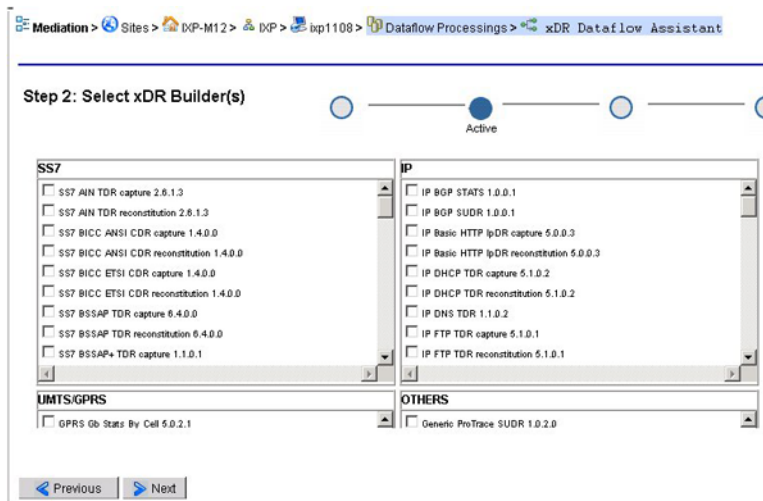


Figure 86: Dataflow Assistant Xdr Builder Selection

9. Select one or more **xDR Builders** from the four categories (SS7, IP, UMTS/GPRS or Others).

Note: You can select multiple builders from one or more of the categories.

10. Click **Next** to open the optional *Enrichment* screen shown here.

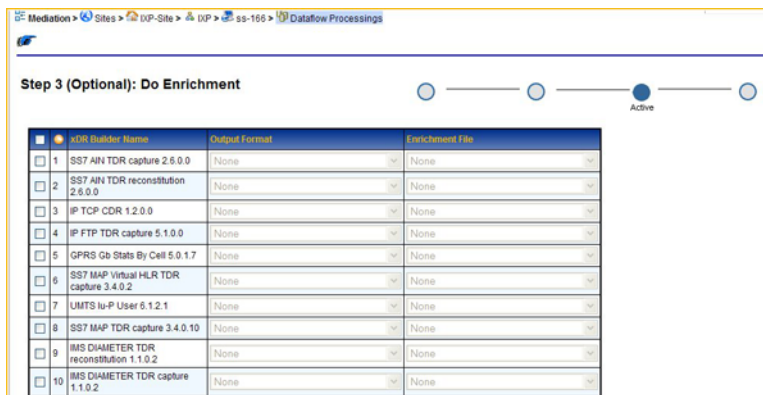


Figure 87: Xdr Assistant - Enrichment Selection

11. (Optional) The *Enrichment* screen enables you to select specific output format and files to be included into the dataflow processing that is to be used in data feed exporting.

To create an enrichment complete these steps.

- a) Select an **xDR Builder**.

The row is highlighted.

- b) From the *Output Format*, select **upload a new format** or select **none** from the pull-down list.

- c) From the *Enrichment* select to **upload a new file** or select **none** from the pull-down list.

- d) Repeat **steps a-c** for each builder.

12. Click **Next** to configure xDR sessions as shown below.

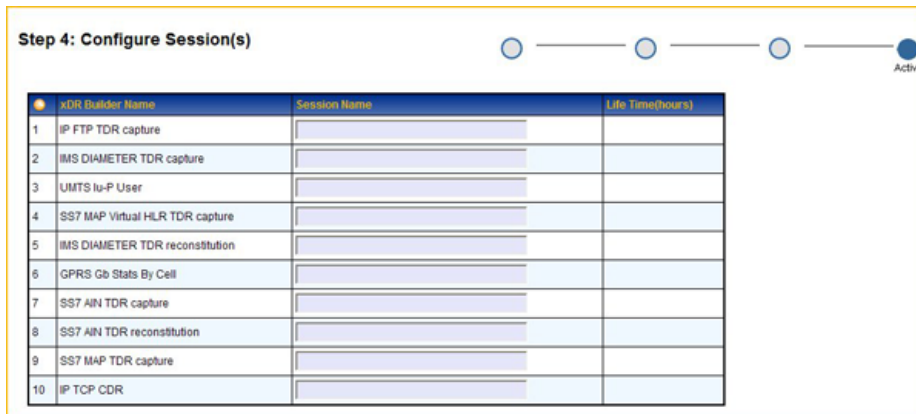


Figure 88: xDR Assistant - Configuring Sessions Screen

13. Type in the **session name**.

14. Type in the **Life Time** (in hours the default is 72 hours).

Note: The Life Time defines how long an xDR is stored. It is a tuning parameter used as a safeguard to conserve disk space and is an important factor in managing your system. After the set amount of time, the xDRs are deleted from the disk. The longer the life time, the longer that disk space is used by the xDRs. It is important to know how much storage you have on your system when setting the Life Time parameter. If the parameter is set too high, then more disk space will be required than is available on the IXP server. Disk space used per xDR will vary from session to session depending upon the number of columns and enrichment settings.

15. Repeat **steps 11-14** for each builder session.

16. Click **Done**.

For changes to take effect, click right-click on the IXP subsystem that has changed, then select **Apply Changes** from the menu.

About Managing Dataflow Processings Manually

Once you have created a dataflow processing, you can modify it manually or if you prefer, you can use this manual method if you want to create a specific dataflow processing. Dataflow processings are categorized into three types:

1. Building - this dataflow processing creates or builds xDRs
2. Operation - this dataflow processing generates statistics and applies filters
3. Storage - this dataflow processing sends data to the IXP subsystem

You can manually add xDR session types using CCM.

Adding an xDR dataflow processing session manually - Build

The building dataflow processing correlates PDUs to create xDRs. This operation is done by one or more xDR builders that create a summary of the values of the signalling.

You can manually add a xDR dataflow procession session by completing these steps.

1. Select **Mediation > Site > IXP > Subsystem >Dataflow Processings**.

2. Right-click on **Dataflow Processings**.
3. Select **Add** from the pop-up menu.

The *Add* screen opens shown here.

The screenshot shows the 'Add' screen for a Dataflow Processing. The 'Definition' tab is selected. The form contains the following fields and options:

- Name:** An empty text input field.
- User Information:** A large empty text area.
- Active:** A checked checkbox.
- Server:** A dropdown menu with 'ixp0888-1e' selected.
- Processing Type:** Three radio buttons: 'Building' (selected), 'Operation', and 'Storage'.
- Retention Time(s):** An empty text input field.

Figure 89: Add Screen

4. Type in the **Name** of the Dataflow.
5. (Optional) Type in any **User Information**.
6. Select whether the dataflow is **active** or not.
7. Select the **Server** for the dataflow.
8. (Optional) Select the **Retention Time** for the process
9. Select **Building**.

(The screen changes to show four more tabs.)

The screenshot shows the 'Dataflow Building Screen'. The 'Definition' tab is selected. The form contains the following fields and options:

- Name:** A text input field containing 'Sample'.
- User Information:** A text area containing the text: 'This is an example of manually creating a Build xDR dataflow processing'.
- Active:** A checked checkbox.
- Server:** A dropdown menu with 'ixp0888-1e' selected.
- Processing Type:** Three radio buttons: 'Building' (selected), 'Operation', and 'Storage'.
- Retention Time(s):** A text input field containing '5'.

Figure 90: Dataflow Building Screen

10. Click **Next**.

The *Input PDUs* tab appears.

Note: If you select PDU Dataflows follow steps 11-12. If you select PDU Streams, go to step 13. You can also use both options.

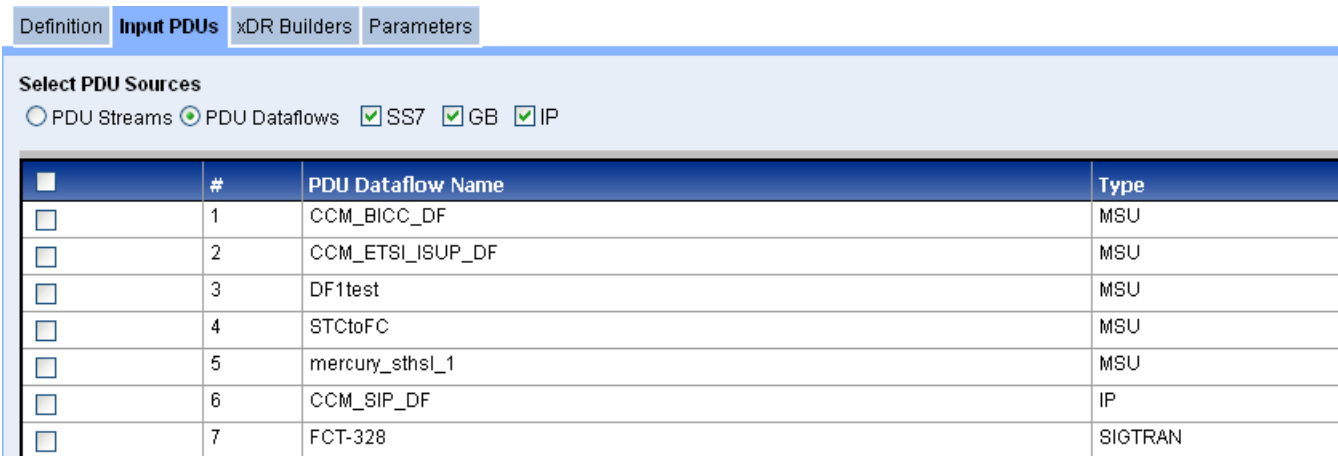


Figure 91: Dataflow Input PDU Tab (PDU Dataflows selected)

11. Select the **Links** you want to use.
12. Select the **PDU Dataflows** you want to use.
13. (For legacy or external PDU streams) Select a **PDU Stream(s)** selection.

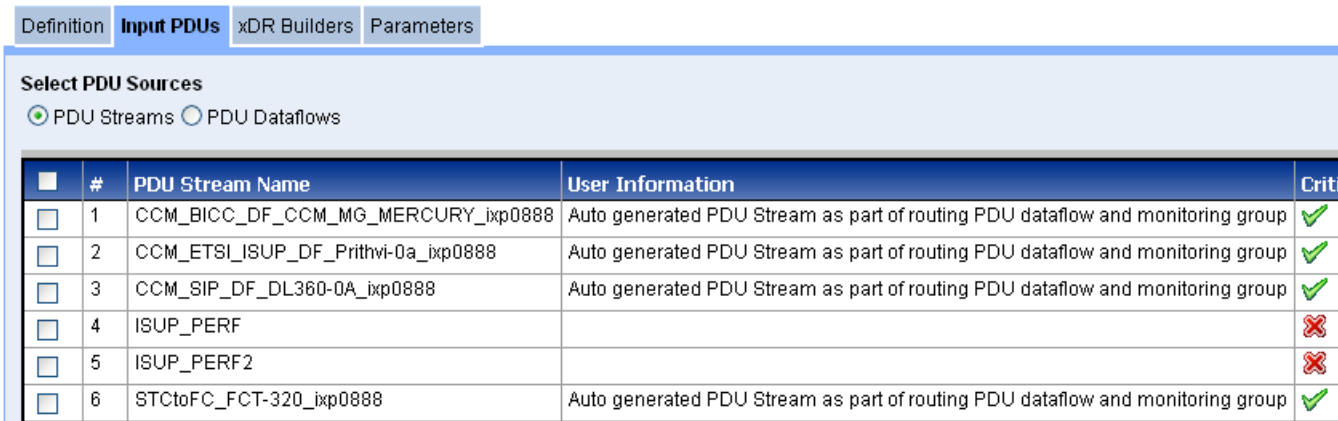


Figure 92: Input PDU Tab (PDU Streams selected if working with external PDU streams)

14. Select the **PDU Stream Name(s)** to be used.
15. Click **Next** to open the *xDR Builders* tab.

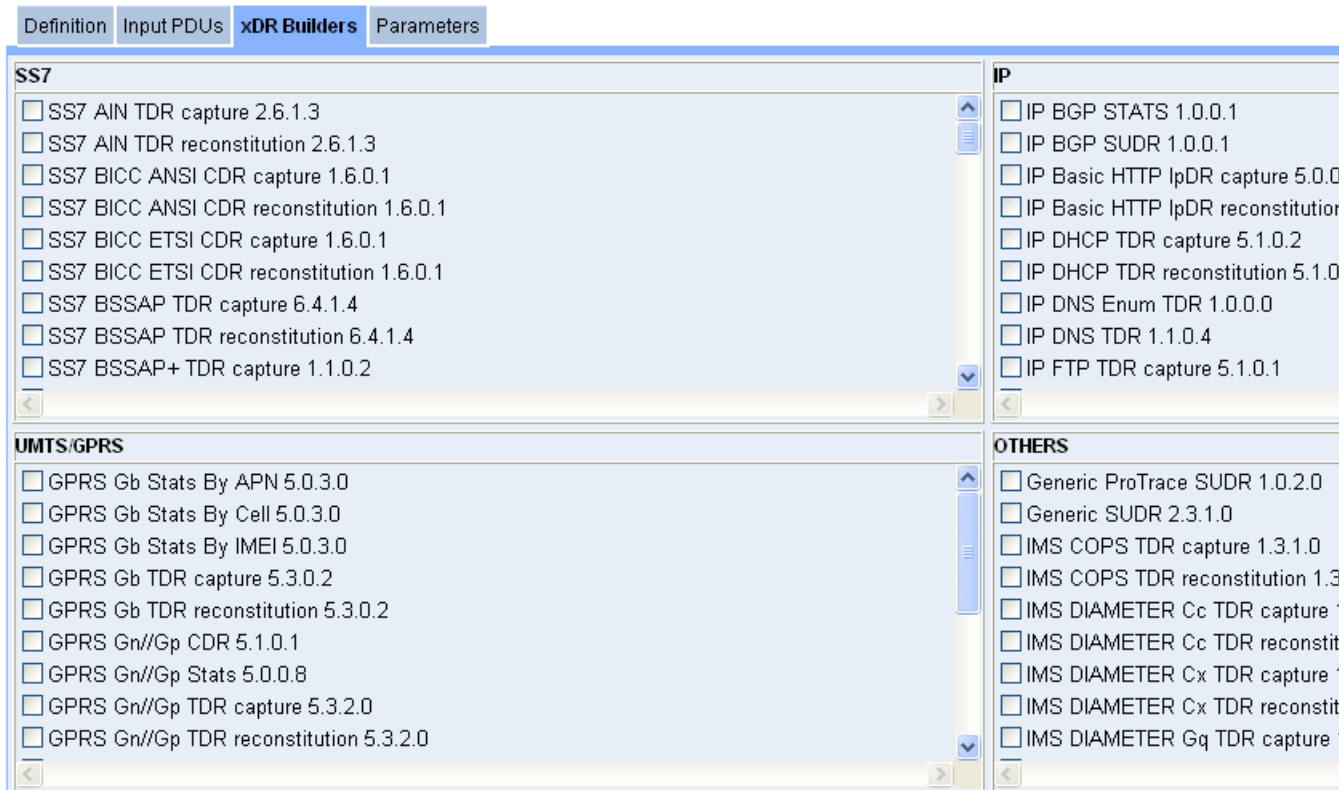


Figure 93: Xdr Builders Tab

16. Select one or more **xDR Builders** from the four categories (SS7, IP, UMTS/GPRS or others).

Note: You can select multiple builders from one or more of the categories.

17. Click **Next** to open the *Parameters* tab shown below.

Note: Based on previously selected builders, CCM displays a series of screens to view and/or change each xDR Builder parameter value. Each xDR Builder selected has a unique set of parameters. The parameters are initialized with default values. For more information on configuring xDR builder parameters, refer to Appendix B, “xDR Builder Parameters,”

The screenshot displays the 'Parameters' configuration page. At the top, there are navigation tabs: 'Definition', 'Input PDUs', 'xDR Builders', and 'Parameters'. Below these, there are sub-tabs: 'Initial step', 'GPRS Gb', 'IP BGP Intermediate', 'IP Transport', and 'IP User Transport'. The main content area is divided into two sections: 'Generic Parameters' and 'Specific Parameters'.
Generic Parameters:
 - No PDU Timeout(s): 600
 - Max transaction duration(s): 86400
 - Garbage period(s): 60
 - Monitored:
Specific Parameters:
 - Maximum authorized frame length acceptable (in KB): 4
 - ATM layer Activation:
 - Send xDRs and frames to the xDR Consumer:
 - Period of flow trace displaying (s): 0
 At the bottom left, there is a 'Defaults' button with a red arrow icon.

Figure 94: Parameters Tab (with SS7, GPRS, IP and Misc xDR Builders selected)

18. You can modify the default values of any parameter.

19. Click **create**.

You must now **apply the change** to save the changes to the subsystem.

About Partial xDRs

The Partial xDR feature in CCM is utilized by ProTrace for processing real-time traces on the SS7 ISUP ANSI, VoIP SIP-T ANSI CDR and VoIP SIP CDR protocols. Using the partial xDR feature you can configure in the build and store process.

Note: You must configure partial ANSI ISUP an dSIP-T/SIP xDRs manually using the build process.

Note: In addition, in configuring partial ANSI ISUP an dSIP-T/SIP xDRs you must also configure xDR filters so that partial and completed xDRs are written to the proper session.

Creating a Partial Build xDR for SS7 ISUP ANSI Protocol

Complete these steps to configure a partial build xDR for SS7 ISUP ANSI CDR reconstitution sessions that can be used by ProTrace for in-progress traces.

1. Select **Mediation > Site > Subsystem > Server > Dataflow Processing** .

The Dataflow processing list page opens.

2. Click **Add** from the tool bar.

The Add screen opens.

Figure 95: Add Screen

3. Type in the **Name** of the Dataflow.
4. (Optional) Type in any **User Information**.
5. Select whether the dataflow is **active** or not.
6. Select the **Server** for the dataflow.
7. (Optional) Select the **Retention Time** for the process
8. Select **Building**.

(The screen changes to show four more tabs.)

Figure 96: Dataflow Building Screen

9. Click Next.

The *Input PDUs* tab appears.

Note: If you select PDU Dataflows follow steps 11-12. If you select PDU Streams, go to step 13. You can also use both options.

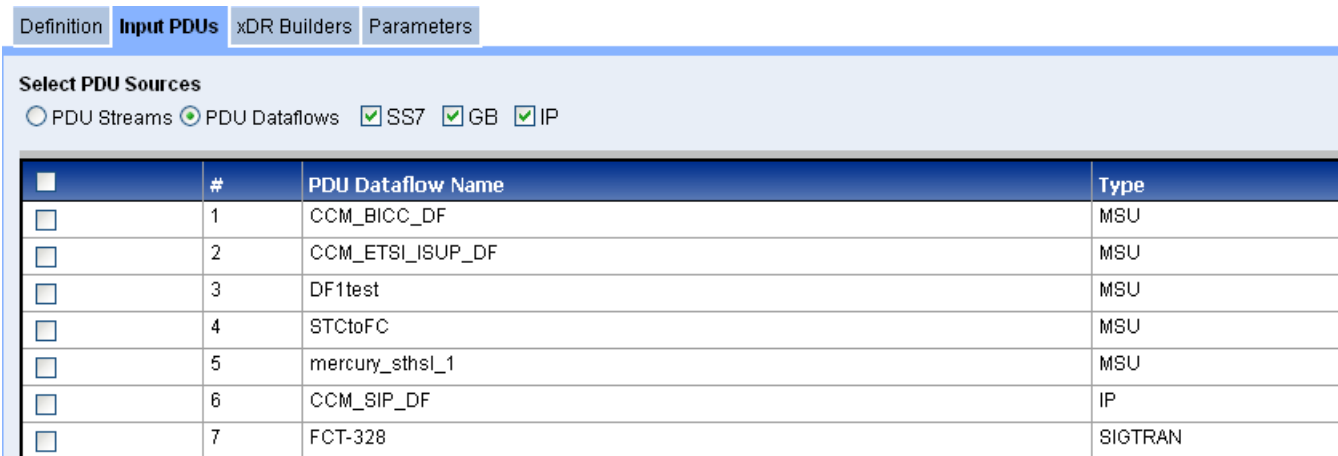


Figure 97: Dataflow Input PDU Tab (PDU Dataflows selected)

10. Select the **Links** you want to use.
11. Select the **PDU Dataflows** you want to use.
12. (For legacy or external PDU streams) Select a **PDU Stream(s)** selection.

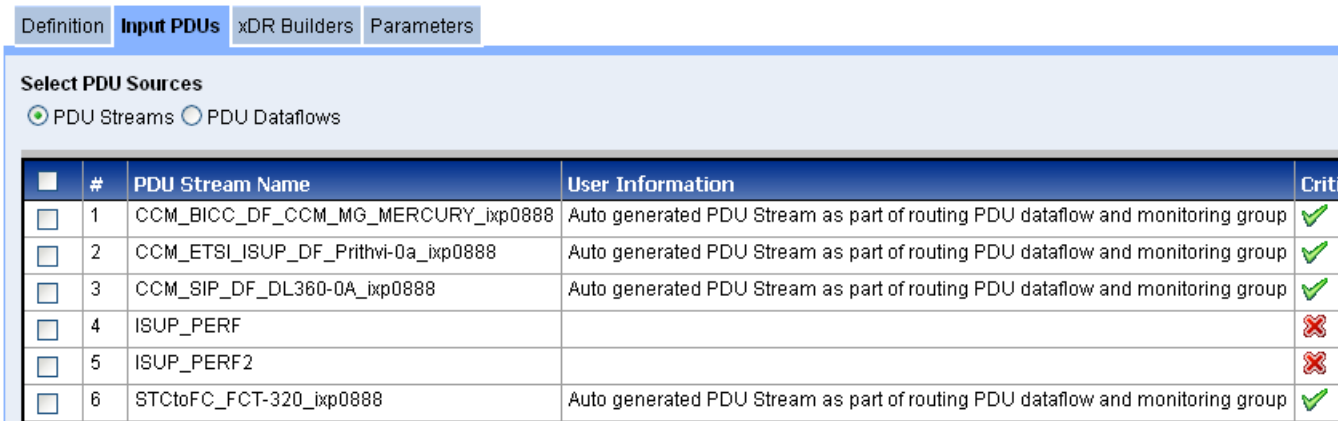


Figure 98: Input PDU Tab (PDU Streams selected if working with external PDU streams)

13. Select the **PDU Stream Name(s)** to be used.
14. Click **Next** to open the *xDR Builders* tab.

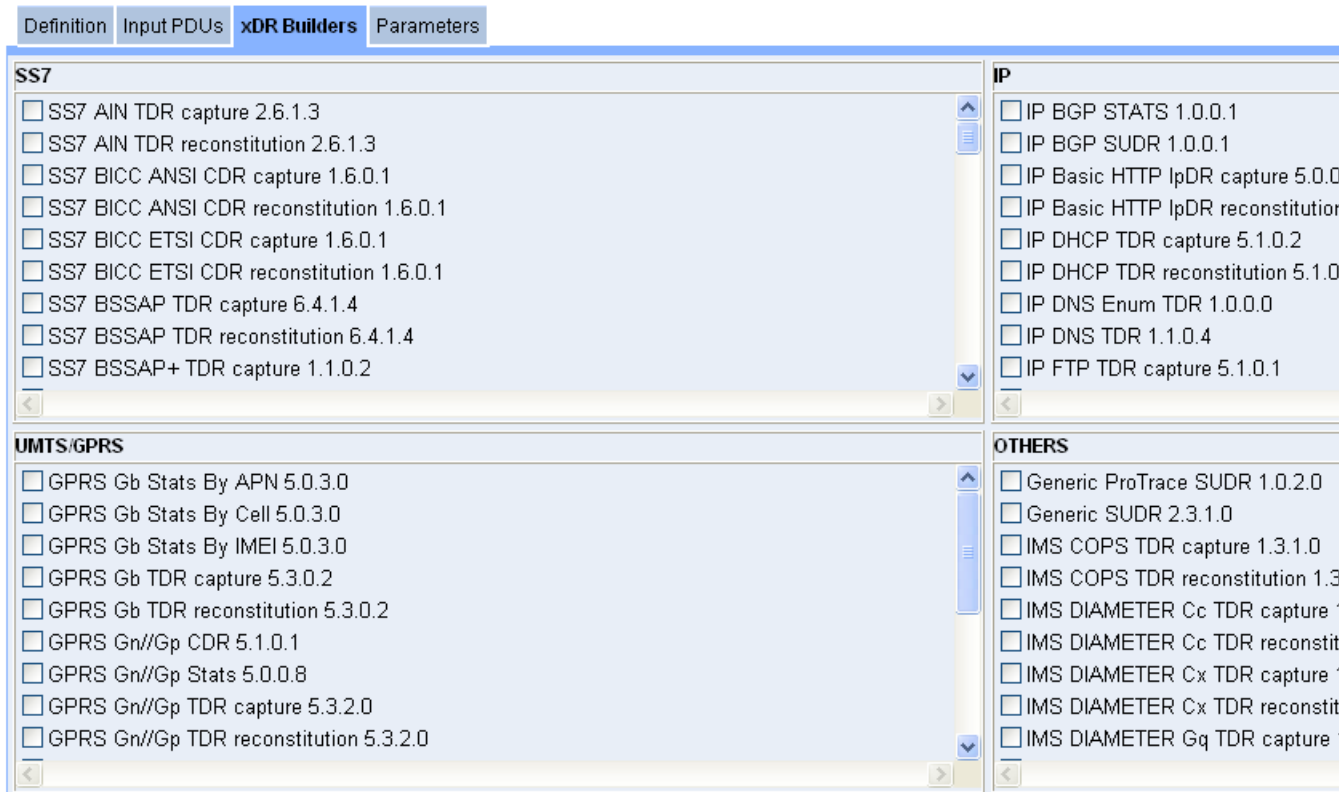


Figure 99: xDR Builders Tab

15. Select one or more **SS7 ISUP ANSI CDR Reconstruction** from the list of (SS7 builders).

Note: You can select multiple builders from one or more of the categories.

16. Click **Next** to open the *Parameters* tab shown below.

Note: Based on previously selected builders, CCM displays a series of screens to view and/or change each xDR Builder parameter value. Each xDR Builder selected has a unique set of parameters. The parameters are initialized with default values. For more information on configuring xDR builder parameters, refer to Appendix B, “xDR Builder Parameters,”

Partial xDR to be sent after Setup	<input type="checkbox"/>
Partial xDR to be sent after Forward	<input type="checkbox"/>
Partial xDR to be sent after Answer	<input checked="" type="checkbox"/>
Partial xDR to be sent after Release	<input type="checkbox"/>
Partial xDR to be sent during conversation	<input type="checkbox"/>

Figure 100: Parameters Tab Showing SS7 ISUP ANSI CDR Tab

17. Click **Create**.

The partial xDR is created.

Apply changes to the IXP subsystem. This partial xDR is now available for in-progress traces used in ProTrace

Creating a Partial xDR for SIP-T/SIP Protocol

Complete these steps to configure a partial build xDR for SS7 SIP-/SIP protocol that can be found in the VoIP SIP-T ANSI CDR reconstitution and VoIP SIP CDR reconstitution sessions used by ProTrace for in-progress traces.

1. Select **Mediation > Site > IXP > Subsystem > Dataflow Processings**.
2. Right-click on **Dataflow Processings**.
3. Select **Add** from the pop-up menu.

The *Add* screen opens shown here.

The screenshot shows a web-based configuration form for adding a new dataflow processing. The form is titled 'Definition' and contains several fields:

- Name:** An empty text input field.
- User Information:** A large empty text area for optional notes.
- Active:** A checked checkbox.
- Server:** A dropdown menu with 'ixp0888-1e' selected.
- Processing Type:** Radio buttons for 'Building' (selected), 'Operation', and 'Storage'.
- Retention Time(s):** An empty text input field.

Figure 101: Add Screen

4. Type in the **Name** of the Dataflow.
5. (Optional) Type in any **User Information**.
6. Select whether the dataflow is **active** or not.
7. Select the **Server** for the dataflow.
8. (Optional) Select the **Retention Time** for the process
9. Select **Building**.

(The screen changes to show four more tabs.)

The screenshot shows the 'Dataflow Building Screen' with the 'Definition' tab selected. The form is populated with the following information:

- Name:** Sample
- User Information:** This is an example of manually creating a Build xDR dataflow processing
- Active:** Checked
- Server:** ixp0888-1e
- Processing Type:** Building (selected)
- Retention Time(s):** 5

 The top of the screen shows four tabs: 'Definition', 'Input PDUs', 'xDR Builders', and 'Parameters'.

Figure 102: Dataflow Building Screen

10. Click Next.

The *Input PDUs* tab appears.

Note: If you select PDU Dataflows follow steps 11-12. If you select PDU Streams, go to step 13. You can also use both options.

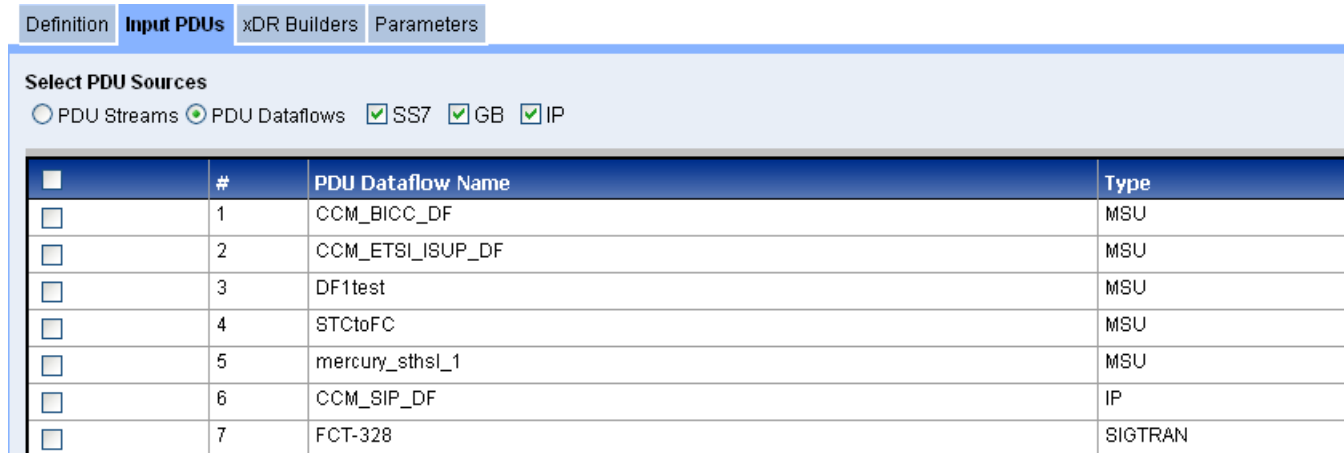


Figure 103: Dataflow Input PDU Tab (PDU Dataflows selected)

11. Select the **Links** you want to use.

12. Select the **PDU Dataflows** you want to use.

13. Click **Next** to open the *xDR Builders* tab.

Select the VoIP SIP

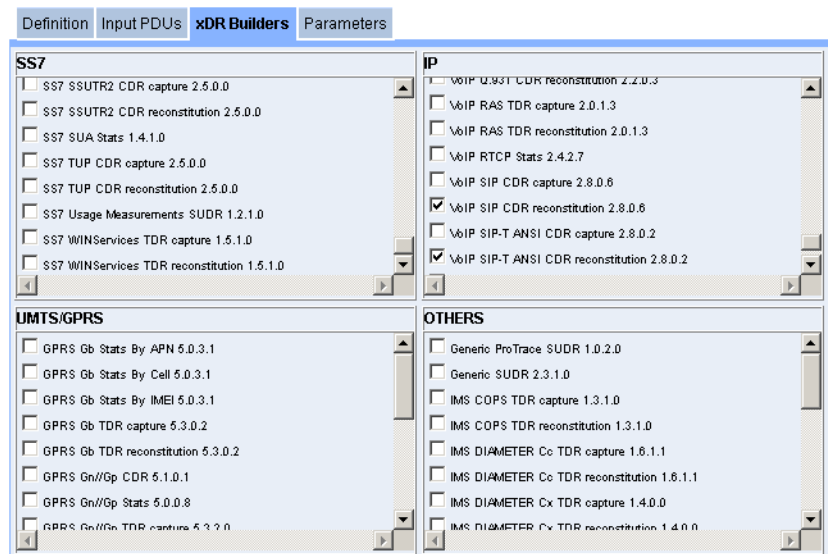


Figure 104: xDR Builders Tab with VOIP SIP Builders Selected

14. Select one or more **xDR Builders** from the four categories (SS7, IP, UMTS/GPRS or others).

Note: You can select multiple builders from one or more of the categories.

15. Click **Next** to open the *Parameters* tab shown below.

Note: Based on previously selected builders, CCM displays a series of screens to view and/or change each xDR Builder parameter value. Each xDR Builder selected has a unique set of parameters. The parameters are initialized with default values. For more information on configuring xDR builder parameters, refer to Appendix B, "xDR Builder Parameters,"

Figure 105: Parameters Tab with VoIP SIP-T ANSI CDR Tab

16. Select **Answer** (move to selected options field) from the CDR Partial section.

Figure 106: VoIP SIP with Answer selected

17. Click **create**.

You must now **apply the change** to save the changes to the subsystem.

Configuring xDR Filters for Store Dataflow Partial xDRs

Partial xDRs for ANSI ISUP and SIP-T/SIP protocols that have been configured for "Answer" must have specifically configured xDR Filters for store dataflows to handle partial and final (after call completion) xDRs. Complete these steps to configure an xDR filter for partial xDR generation.

1. Select **Mediation > Site > IXP > Subsystem > Dataflow Processings**.
2. Right-click on **Dataflow Processings**.
3. Select **Add** from the pop-up menu.

The Add screen opens.

Figure 107: Add Screen

4. Enter the **Name** of the Dataflow.
5. (Optional) Enter any **User Information**.
6. Select whether the dataflow is **active** or not.
7. Select the **Server** for the dataflow.
8. Select **Storage** for the processing type.
9. Enter the **Retention Time(s)** for the DFP. (Default is 5 sec)
10. Enter the **Flush Time(s)** for the DFP. (Default is 5 sec)
11. Click **Next**.

The list of Input Steams appears.

#	Name	Critical	Description
1	B_TC_320_ansi_recon_129	✓	Created as the part of build dfp
2	B_CCM_SIP_CDRS_98	✓	Created as the part of build dfp
3	B_TC_320_ansi_capt_130	✓	Created as the part of build dfp
4	O_POOL_ISUP_PERF1_111	✓	Created for KPIs
5	K_Test_Stats_112	✓	Created for KPIs
6	B_TC_320_etsi_cap_131	✓	Created as the part of build dfp
7	test_sac_buildISUPANSICDRcapture	✓	Created as the part of build dfp
8	O_ixp0888PoolMonitor_89	✓	Created for KPIs
9	ixp0888PoolMonitor	✓	Created for PoolMonitor by Ixp.

Figure 108: Input Streams Screen

12. Select the **Input Steams** to be used in the dataflow processing.

Note: You cannot select Input Streams that belong to different dictionaries. They must all belong to the same dictionary.

13. Click **Next**.

The xDR Filter screen appears.

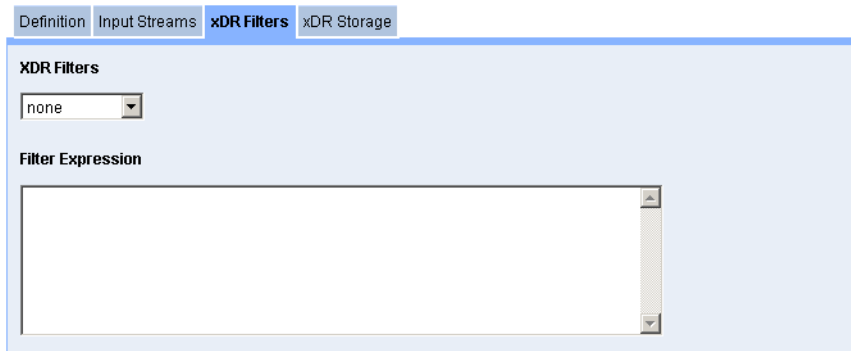


Figure 109: xDR Filter Screen

14. Select **Create Filter** from the drop-down menu.

The Create New xDR Filter opens.

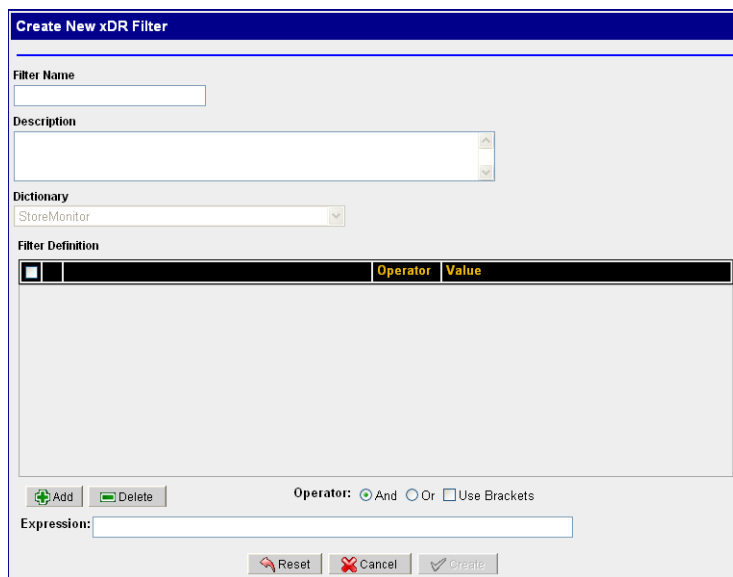


Figure 110: xDR Filter Screen

15. Enter the **Filter Name**.

You can also enter a description. The dictionary has already been selected and is grayed out.

16. Click **Add** to add a condition.

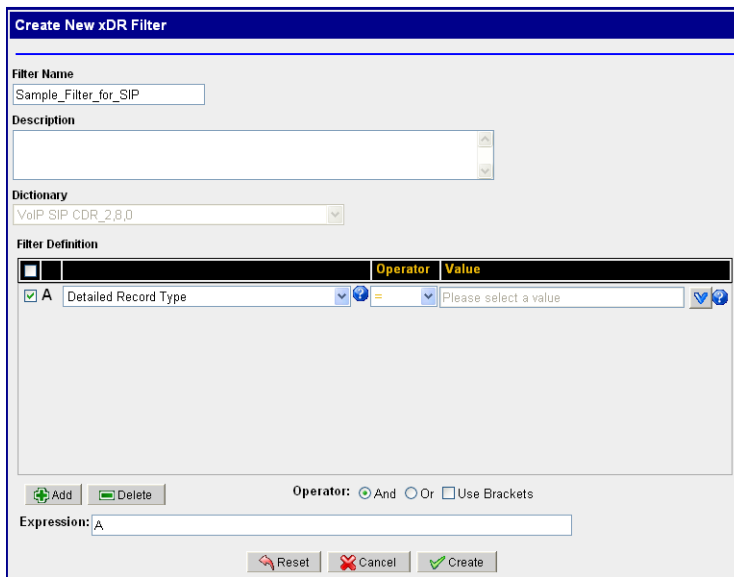


Figure 111: xDR Filter Screen with condition

17. Select **Detailed Record Type** for field.
18. Select **=** for the operator.
19. Select **After Answer Partial xDR** for value.
20. Click **Create**.

The filter is created that allows all types of xDRs including Frame Alone xDRs and Circuit Message to be stored in the *Complete* xDR Session except the ones which are generated as Partial xDRs after Answer message.

21. Select or create a **session**.
Make sure the session lifetime is **24 hours**.
22. Click **Create** to create the storage dfp with special filter.
Apply changes to the IXP subsystem for them to take effect.

Adding an xDR Dataflow Processing Session Manually - Operation

You can manually add a operation xDR dataflow processing session by completing these steps.

Note: Before you create a Operate dataflow process, make sure that you have XdR input streams. These XDR input streams maybe the output of a previously created build dataflow process or a stream from another subsystem.

1. Select **Mediation > Site > IXP > Subsystem > Dataflow Processings**.
2. Right-click on **Dataflow Processings**.
3. Select **Add** from the pop-up menu.

The Add screen opens shown here.

Figure 112: Add Dataflow Processing Screen

4. Type in the **Name** of the Dataflow.
5. (Optional) Type in any **User Information**.
6. Select whether the dataflow is **active** or not.
7. Select the **Server** for the dataflow.
8. Select **Operation**.
9. Click **Next**.

The screen changes to show the *Input streams* screen.

	Name	Critical	Description
<input type="checkbox"/>	B_VoipMgcpCap_010808_2	✓	Created as the part of build dfp
<input type="checkbox"/>	B_Sample_3	✓	Created as the part of build dfp
<input type="checkbox"/>	B_Sample1_4	✓	Created as the part of build dfp
<input type="checkbox"/>	B_Sample2_5	✓	Created as the part of build dfp
<input type="checkbox"/>	B_Sample3_6	✓	Created as the part of build dfp
<input type="checkbox"/>	B_ss7IsupAnsiCap_010808_1	✓	Created as the part of build dfp
<input type="checkbox"/>	ixp0960StreamMonitor	✓	Created for StreamMonitor by lxp.
<input type="checkbox"/>	ixp0960BuildMonitor	✓	Created for BuildMonitor by lxp.
<input type="checkbox"/>	ixp0960OperateMonitor	✓	Created for OperateMonitor by lxp.

Figure 113: IP Streams Screen

10. Select the **Input streams** you want.

Note: What you select will be the *outputs* of the build data process that have been created.

11. Click **Next**.

The *xDR Filters* screen opens shown below.

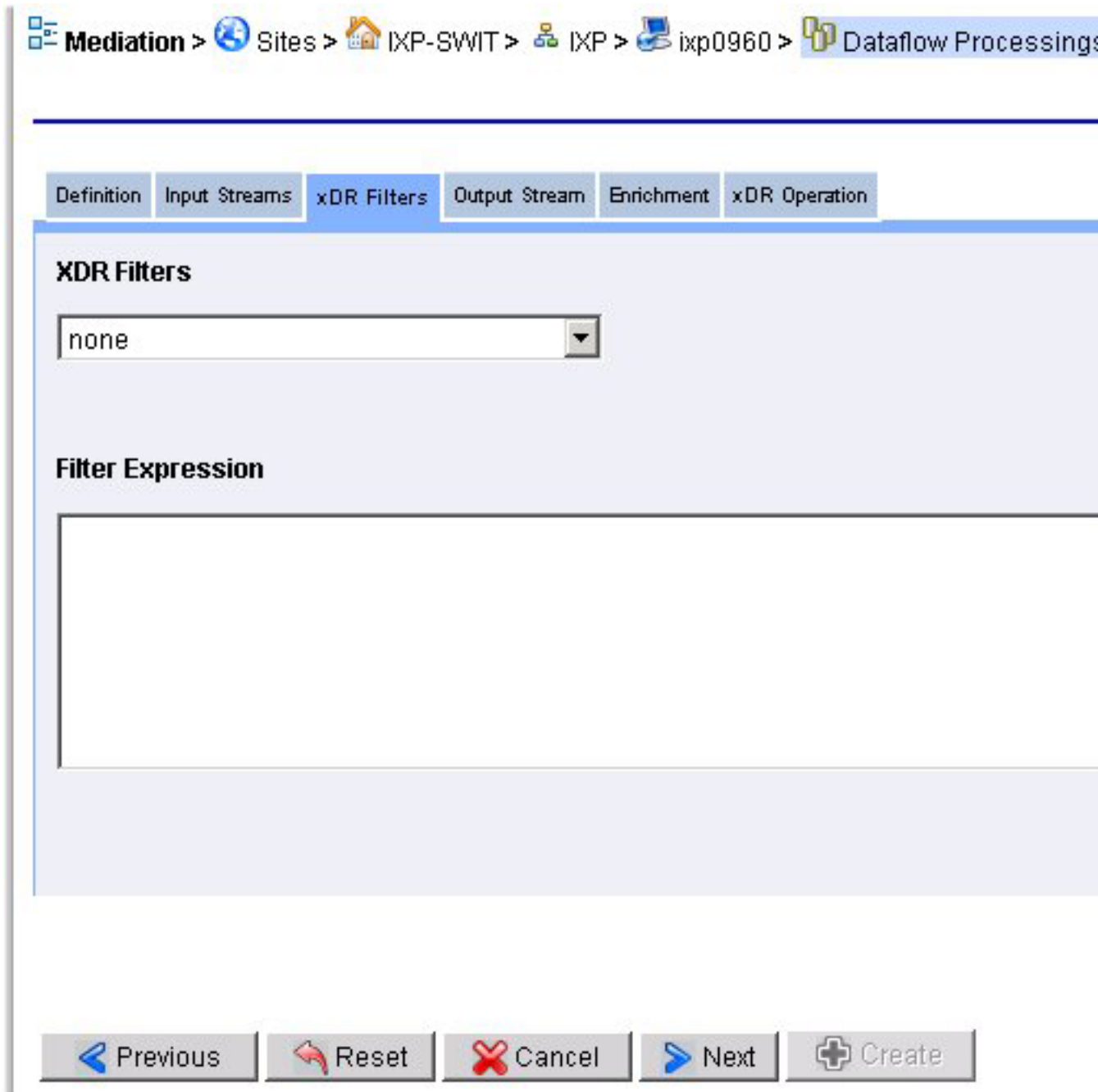


Figure 114: Xdr Filters Screen

12. Select a **xDR Filter** from the pull-down list.

The *Filter Expression* is shown in the field below.

Note: You can also select *Create a new xDR Filter* from the pull-down list. See [Creating an xDR Session for a Dataflow Processing](#) for more information.

13. Click **Next**.

The *Output Stream* screen opens shown below.

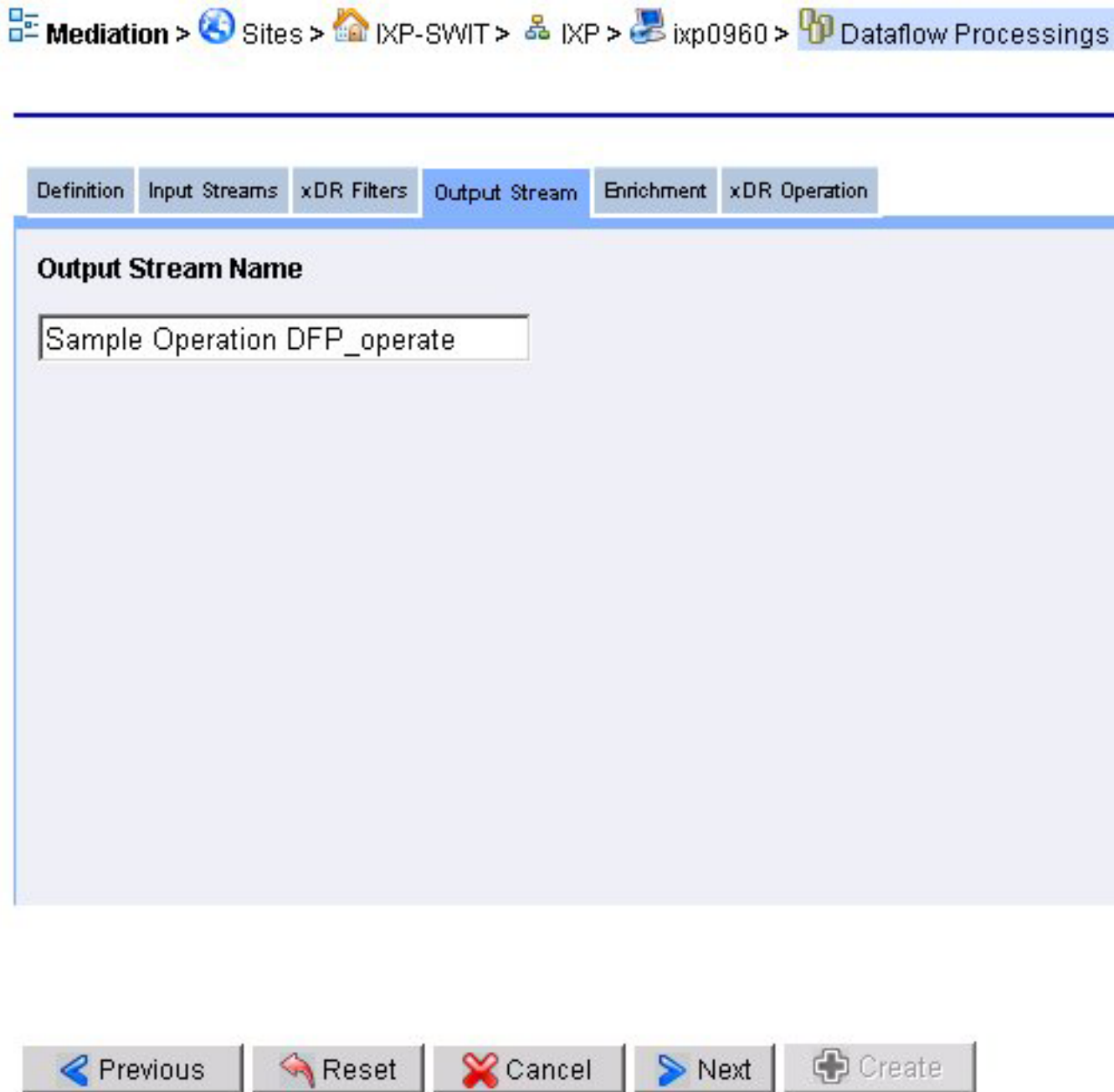


Figure 115: Output Steams Screen

14. (Optional) Modify the **Output Stream Name** from the default name.

15. Click **Next** the *Enrichment* screen opens shown below.

Note: This screen is used exclusively for the IXP xDR static or dynamic enrichment option. The output xDRs from can have extra user-defined fields that are updated by IxpOperate using user-defined mapping tables in *.fse files, and are used by ProTraq. However, the new fields must be defined in a dictionary, referred to as an enriched dictionary. The ASCII dictionary file (*.a7d) are modified manually and loaded into NSP by using the dictionary upload screen. These enriched dictionaries show up in this list.

Mediation > Sites > IXP-SWIT > IXP > ixp0960 > Dataflow Processings

Definition | Input Streams | xDR Filters | Output Stream | **Enrichment** | xDR Operation

Output Format

none

Enrichment File

none

Active

◀ Previous | Reset | Cancel | Next | Create

Figure 116: Enrichment Screen

16. (Optional) Create an **Enrichment** record.

- a) Select an **Output Format**
- b) Select an **Enrichment file**.
- c) (Optional) Select if the enrichment is **Active** or not.
(Active means that the enrichment will happen on this dataflow.)

17. Click **Next**.

The *xDR Operation* screen opens shown below.

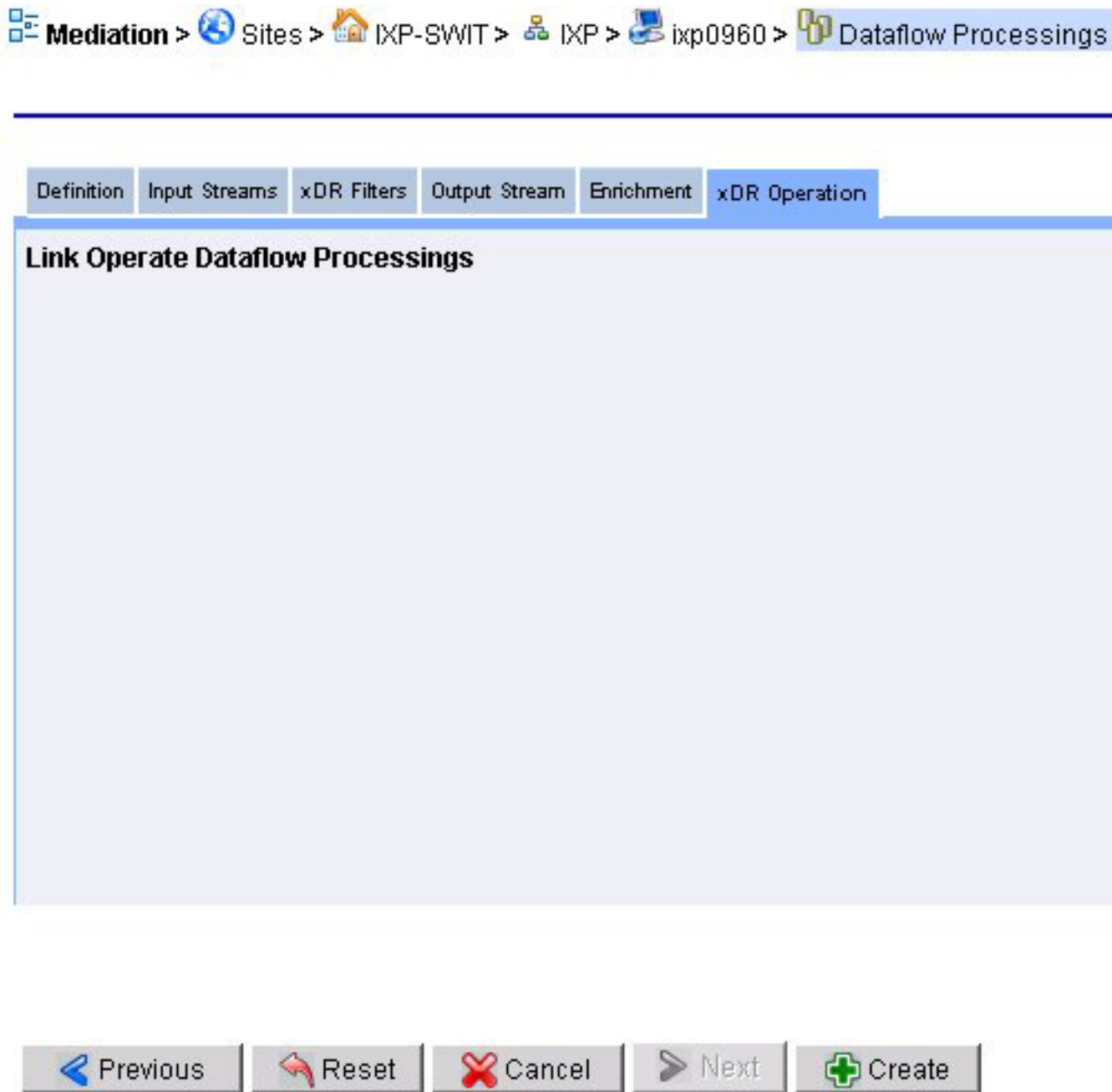


Figure 117: Xdr Operation Screen

18. Select a **link(s)** for the Operate Dataflow Processings.
(not shown here)

19. Click **Create**.

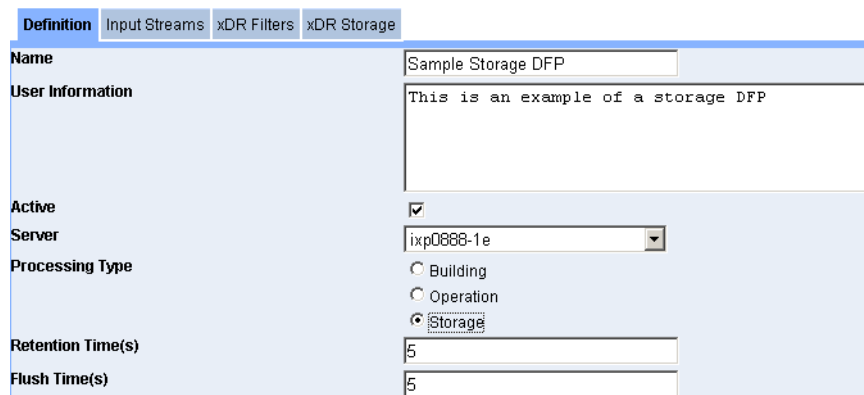
Note: You must apply these configurations to the IXP subsystem for these configurations be used in the system.

Adding an xDR Dataflow Processing Session Manually - Storage

You can manually add a storage xDR dataflow procession session by completing these steps.

1. Select **Mediation > Site > IXP > Subsystem > Dataflow Processings**.
2. Right-click on **Dataflow Processings**.
3. Select **Add** from the pop-up menu.

The Add screen opens.



Field	Value
Name	Sample Storage DFP
User Information	This is an example of a storage DFP
Active	<input checked="" type="checkbox"/>
Server	ixp0888-1e
Processing Type	<input type="radio"/> Building <input type="radio"/> Operation <input checked="" type="radio"/> Storage
Retention Time(s)	5
Flush Time(s)	5

Figure 118: Add Screen

4. Enter the **Name** of the Dataflow.
5. (Optional) Enter any **User Information**.
6. Select whether the dataflow is **active** or not.
7. Select the **Server** for the dataflow.
8. Select **Storage** for the processing type.
9. Enter the **Retention Time(s)** for the DFP. (Default is 5 sec)
10. Enter the **Flush Time(s)** for the DFP. (Default is 5 sec)
11. Click **Next**.

The list of Input Steams appears.

Definition Input Streams xDR Filters xDR Storage				
<input type="checkbox"/>	#	Name	Critical	Description
<input type="checkbox"/>	1	B_TC_320_ansi_recon_129	✓	Created as the part of build dfp
<input type="checkbox"/>	2	B_CCM_SIP_CDRS_98	✓	Created as the part of build dfp
<input type="checkbox"/>	3	B_TC_320_ansi_capt_130	✓	Created as the part of build dfp
<input type="checkbox"/>	4	O_POOL_ISUP_PERF1_111	✓	Created for KPIs
<input type="checkbox"/>	5	K_Test_Stats_112	✓	Created for KPIs
<input type="checkbox"/>	6	B_TC_320_etsi_cap_131	✓	Created as the part of build dfp
<input type="checkbox"/>	7	test_sac_buildISUPANSICDRcapture	✓	Created as the part of build dfp
<input type="checkbox"/>	8	O_ixp0888PoolMonitor_89	✓	Created for KPIs
<input type="checkbox"/>	9	ixp0888PoolMonitor	✓	Created for PoolMonitor by Ixp.

Figure 119: Input Streams Screen

12. Select the **Input Steams** to be used in the dataflow processing.

Note: You cannot select Input Streams that belong to different dictionaries. They must all belong to the same dictionary.

13. Click **Next**.

The xDR Filter screen appears.

Definition Input Streams xDR Filters xDR Storage			
XDR Filters			
none			
Filter Expression			
<div style="border: 1px solid gray; height: 50px;"></div>			

Figure 120: xDR Filter Screen

14. Select the **xDR Filter** to be applied to the dataflow processing.

The filter expression appears in the field at the bottom of the screen.

Note: You can also select *Create Filter* from the pull-down list. .

15. Click **Next**.

The *xDR Storage* screen appears.

Definition Input Streams xDR Filters xDR Storage			
XDR Sessions			
Select Session			

Figure 121: xDR Storage Screen

16. Select or create a **session**.

Note: A list of existing xDR Sessions based on the dictionaries that are associated with the previously selected xDR input streams is provided.

17. Click **Create**.

The storage dataflow processing is created. You are now prompted to synchronize the subsystem to save the changes.

Listing xDR Builders

The builder information is needed for IXP configuration. xDR builders perform various functions from correlating to deciphering information in an xDR. Builders are tracked by CCM on a per-subsystem basis. An IXP subsystem is assumed to have a single version of a particular builder installed on its servers. In addition, dictionaries used by discovered builders are also retrieved and stored in the system.

Complete the following task to list all the xDR builders in an IXP subsystem.

- Select **Mediation > IXP Subsystem > xDR Builders** The *xDR Builder List* screen opens shown below.

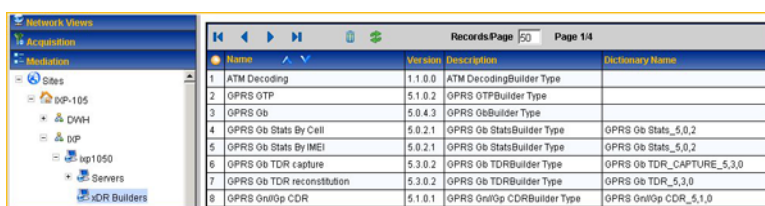


Figure 122: Xdr Builder List Screen

The following information is provided:

Table 48: Xdr Builder List Descriptions

Column	Description
Name	xDR Builder Name
Version	current version of the builder that is stored in the subsystem
Description	brief description of the builder
Dictionary name	the name of the dictionary associated with the builder

About Sessions

You can click on **Sessions** in the object tree to view the list of available sessions. In this screen, you can add, modify, or delete sessions on a server.

Note: The session name must be unique for each IXP subsystem or dataserver, but sessions can have identical names if they reside on separate IXP subsystems.

Adding an xDR Session to a Server

Complete these steps to add a session to a server.

1. Select **IXP Subsystem > Sessions**.
The sessions list screen opens.
2. Click **Add** the *Add Session* screen opens.

The screenshot shows the 'Add Session' form in the IXP Mediation interface. The breadcrumb trail at the top reads: Mediation > Sites > Morrisville > IXP > ixp0500 > Sessions > List. The form has the following fields:

- Session Name:** Sample_Session
- Lifetime (hours):** 72
- Storage:** ixp5001-1a
- Dictionary:** 8951|monica_sess
- Description:** This is an example of a session

At the bottom of the form are three buttons: Reset, Cancel, and Add.

Figure 123: Add Sessions Screen

3. Type a **Session name**.
Note: The session name must be unique for each IXP subsystem or datasever, but sessions can have identical names if they reside on separate IXP subsystems.
4. Type in the **Lifetime** (number of hours the session exists).
5. Select the **Storage** subsystem.
6. Select the **Dictionary** associated with the session.
7. (Optional) Select a **Session Backup**.
(None, xDR only or xDR and PDU) Default is *None*.
8. (Optional) Type in a **Description**. Shown below is a completed session.
9. Click **Add**.
The session is added to the session list shown below.

The screenshot shows a web interface for session management. At the top, there is a breadcrumb trail: Mediation > Sessions > List. Below this is a toolbar with various icons and a status bar indicating 'Records: Page 25', 'Page 1/1', and 'Total Records: 7'. The main content is a table with the following columns: Session, Type, Format, Dictionary, Host, and Lifetime. The table contains seven rows of session data.

Session	Type	Format	Dictionary	Host	Lifetime
1 AG_ISUP_ANSI_28	RECONSTITUTION	SINGLE	SS7 ISUP ANSI CDR_2,4,0	ixp0960-1a	120
2 Sample_Session	STATISTICS	SINGLE	BuildMonitor	ixp0960-1a	150
3 xip0960StreamMonitor	STATISTICS	SINGLE	StreamMonitor	ixp0960-1a	336
4 xip0960BuildMonitor	STATISTICS	SINGLE	BuildMonitor	ixp0960-1a	336
5 xip0960OperateMonitor	STATISTICS	SINGLE	OperateMonitor	ixp0960-1a	336
6 xip0960StoreMonitor	STATISTICS	SINGLE	StoreMonitor	ixp0960-1a	336
7 INAP_Rec_28	RECONSTITUTION	SINGLE	SS7 INAP TDR_2,9,5	ixp0960-1a	100

Figure 124: Completed Session In Session List

Modifying an xDR Session

1. Select **IXP Subsystem > Sessions**.
The sessions list screen opens.
2. Select the **session** to be modified shown here.

This screenshot is similar to Figure 124 but shows a different set of sessions. The 'Sample_Session' row is highlighted in blue, indicating it is selected. The status bar shows 'Total Records: 11'.

Session	Type	Format	Dictionary	Host	Lifetime
1 Sample_Session	CAPTURE	SINGLE	SS7 AIN TDR_CAPTURE_2,6,1	ixp5001-1a	72
2 Sample_Session_1	RECONSTITUTION	SINGLE	SS7 AIN TDR_2,6,1	ixp5001-1a	72
3 xip5001StreamMonitor	STATISTICS	SINGLE	StreamMonitor	ixp5001-1a	336

Figure 125: Selected Session For Modification

3. Click **Modify** on the toolbar.
The session record opens.
4. Make the needed modifications.
Note: You can not select another dictionary for the session. To use another dictionary, you must create a new session.
5. Click **Modify**.
The record is modified.

Deleting an xDR Session

Complete these steps to delete an xDR session.

Note: You can not delete a session that is using a dataflow processing. You must first delete the dataflow processing or modify the dataflow processing to use another session.

Note: You must also apply changes for any changes in the subsystem to take effect.

1. Select **Mediation > IXP > Subsystem > Sessions**.
The sessions list screen opens.
2. Select the **session** to be deleted.

3. Click **Delete**.
4. Click **OK** at the prompt.
The session is deleted.

About Partial xDRs

The Partial xDR feature in CCM is utilized by ProTrace for processing real-time traces on the SS7 ISUP ANSI, VoIP SIP-T ANSI CDR and VoIP SIP CDR protocols. Using the partial xDR feature you can configure in the build and store process.

Note: You must configure partial ANSI ISUP an dSIP-T/SIP xDRs manually using the build process.

Note: In addition, in configuring partial ANSI ISUP an dSIP-T/SIP xDRs you must also configure xDR filters so that partial and completed xDRs are written to the proper session.

Creating an xDR Session for a Dataflow Processing

Complete these steps to create an xDR Session for a dataflow processing. You can create a session for either an Operate or a Storage dataflow processing.

1. In the *xDR Storage* screen, select **Create Session**.

The shown below.

Figure 126: Create Session Screen

2. Type a **Session name**.
3. Type in the **Lifetime** (number of hours the session exists).
4. Select the **Storage** subsystem.
5. Select the **Dictionary** associated with the session.
6. (Optional) Type in a **Description**. Shown below is a completed session.

Session Name	Lifetime (hours)	Storage
Sample_xDR_Session	72	ixp0960-1a

Dictionary: IP DHCP TDR_CAPTURE_5,1,0

Session Backup: None

Description: This is an example of an xDR session.

Buttons: Reset, Cancel, Add

Figure 127: Completed Xdr Session Screen

7. Click **Add**.

The session is created and the session name shows up in the Session field shown below.

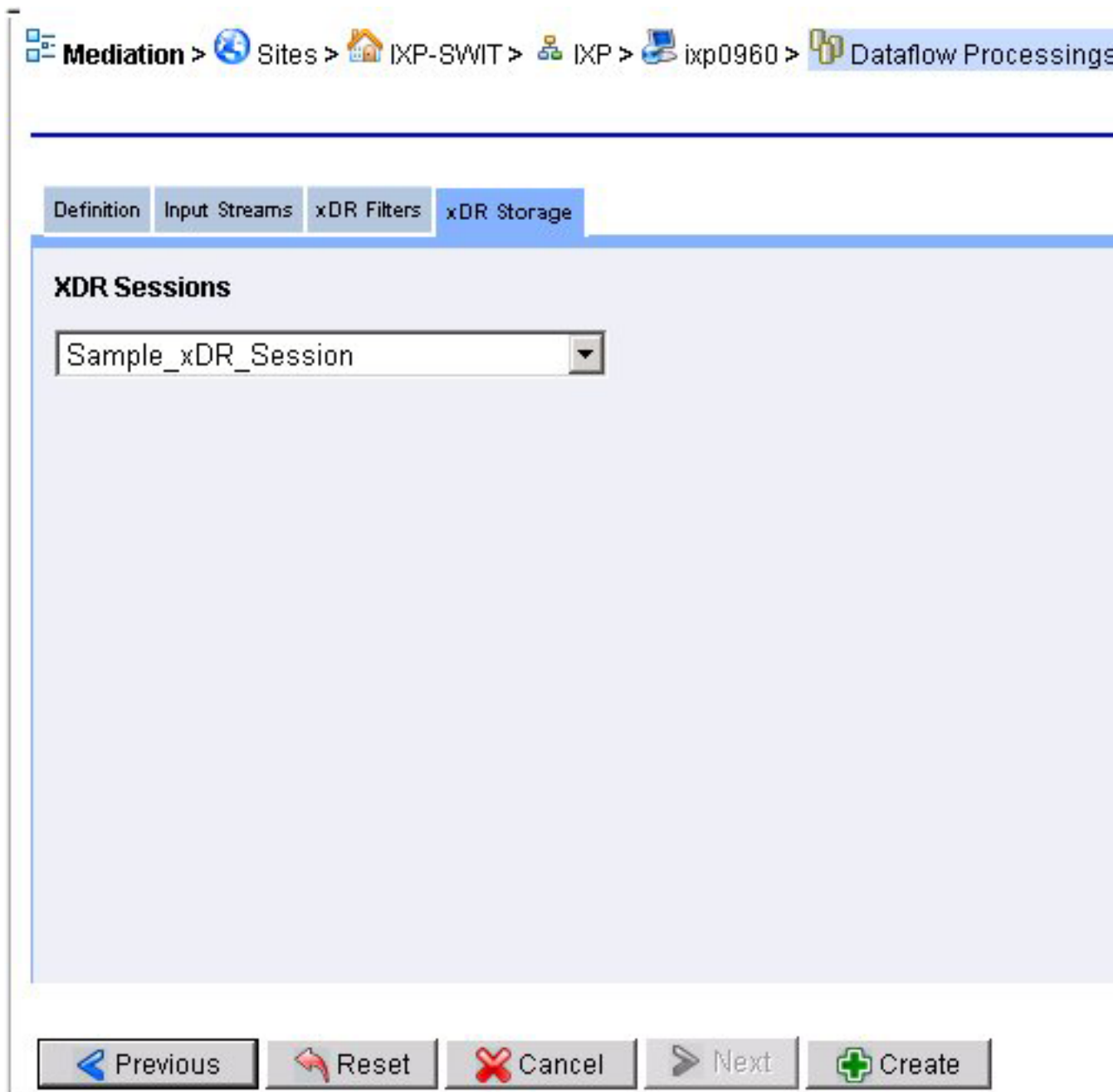


Figure 128: Added Session In Xdr Storage Screen

8. You can now create the storage dataflow processing.

Modifying an xDR session for a dataflow Processing

Complete these steps to modify an xDR session for a dataflow processing.

1. Select **Mediation > Site > IXP Subsystem > Subsystem Name > Dataflow Processings**.

The *dataflow processing List* screen opens.

2. Select the **dataflow processing** to be modified.
3. Click **Modify**.
4. Make the necessary modifications.
5. Click **Modify**.

The dataflow processing is modified. You must now synchronize the subsystem. (See [About Applying Changes to an IXP Subsystem](#))

Deleting an xDR session from a dataflow Processing

1. Select **Mediation > Site > IXP Subsystem > Subsystem Name > Dataflow Processings**.

The *dataflow processing List* screen opens.

2. Select the **dataflow processing** to be deleted.

Note: You cannot delete a dataflow processing if there are any dependencies on it. You are prompted if there are dependencies belonging to the dataflow processing being deleted.

3. Click **Delete**.
4. Click **OK** at the prompt.

The dataflow processing is deleted. You must now synchronize the subsystem. (See [About Applying Changes to an IXP Subsystem](#))

About Q.752 Dataflows

Q.752 dataflows are a type of dataflow processing (see “[Configuring xDR Dataflow Processings](#)”). A Q.752 dataflow is created to route Q.752 statistical data from XMF to IXP.

About configuring Q.752 Dataflows

Configuring Q.752 dataflows is performed in a specific sequence. CCM is set up to enable you to go through this sequence in *Wizard* fashion through a set of tabs. The procedure for each tab is discussed in proper sequence.

About managing counter Activation

You route specific Q.752 traffic from the XMFs to IXP by choosing *Q.752 counters*. These counters are defined by the SS7 standards from Q.752 statistics. Activating and deactivating the counters internally creates the corresponding dataflow build and stores dataflow processings and then routes the data to sessions (created automatically). It is important that you choose what input streams to apply the Q.752 dataflows to. On choosing the input streams you have the option of configuring two parameters:

- No PDU Timeout
- Automatically Clear Alarms

These two parameters are internally applied to the build dataflow processes. You then have the option to apply SSN and linkset filters to the configuration. The filter values are applied to the build dataflow process created internally. When you navigate to the *Linkset filters* tab, you are presented with a list

of linksets. These linksets are derived automatically based on the input stream that you chose. You can choose a set of linksets and apply a pre-created OPC-DPC-SIO filter to the linksets.

When you choose to de-select a counter the associated session is not deleted automatically. You can navigate to the sessions list and delete the session manually. This results in the session also are deleted in the DWH.

About the Q.752 Dataflow Assistant

The Q.752 Dataflow Assistant option provides a wizard to help you quickly create a Q.752 processing. The process follows five stages:

- Selecting the Q.752 counters
- Selecting the PDU Inputs (Streams and/or Dataflows)
- Configuring the General Parameters
- Selecting (or not) an SSN Filter to be used with the processing
- Selecting the Linkset Filters to be used with the processing

Using the Q.752 Processing Assistant

Note: Because Q.752 processings utilize input streams, you must first create your input streams or PDF dataflows before you create your Q.752 processings.

1. Select **Mediation > Site > IXP > Subsystem** that needs the Q.752 processings.

The Q.752 list screen opens

<input type="checkbox"/>	#	Table	Description	Period	Name
<input type="checkbox"/>	1	1	MTP - Signalling link fault and performance	30'	Q752_1
<input type="checkbox"/>	2	2	MTP - Signalling link availability	30'	Q752_2
<input type="checkbox"/>	3	3	MTP - Signalling link utilization	5'	Q752_3
<input type="checkbox"/>	4	4	MTP - Signalling link set and route set availability	30'	Q752_4
<input type="checkbox"/>	5	6	MTP - Signalling link traffic distribution	30'	Q752_6
<input type="checkbox"/>	6	7	SCCP - Error performance	30'	Q752_7
<input type="checkbox"/>	7	9	SCCP - Utilization	5'	Q752_9
<input type="checkbox"/>	8	9 bis	SCCP - Quality of service	5'	Q752_9bis
<input type="checkbox"/>	9	11	ISUP - Utilization	5'	Q752_11
<input type="checkbox"/>	10	-	ISUP - Call failure measurement	30'	Q752_ISUPFailCau
<input type="checkbox"/>	11	-	MTP - Signalling link occupancy rate	5'	Q752_SLOR

Figure 129: Q.752 Processing List Screen

2. Select one or more **Q.752 Counters** from the list.
3. Click **Next**.

The Inputs screen opens.

Note: The Inputs tab has two screens: PDU Streams and PDU Dataflows. Depending on your needs, you can select from one or both. If you are want to add streams, complete steps 4 and 5. If you want to add dataflows, complete steps 6 thru 8.

Counter Activation **Inputs** General Parameters SSN Filters Linkset Filters

Do you want to include MSW Linksets

PDU Streams PDU Dataflows

<input type="checkbox"/>	#	PDU Stream Name	User Information	Crit	Use RID
<input type="checkbox"/>	1	CCM_BICC_DF_CCM_MG_MERCURY_ikp0888	Auto generated PDU Stream as part of routing PDU dataflow and monitoring group	✓	✓
<input type="checkbox"/>	2	CCM_ETSI_ISUP_DF_Prithvi-0a_ikp0888	Auto generated PDU Stream as part of routing PDU dataflow and monitoring group	✓	✓
<input type="checkbox"/>	3	CCM_SIP_DF_DL360-0A_ikp0888	Auto generated PDU Stream as part of routing PDU dataflow and monitoring group	✓	✓
<input type="checkbox"/>	4	ISUP_PERF		✗	✗
<input type="checkbox"/>	5	ISUP_PERF2		✗	✗
<input type="checkbox"/>	6	STCtoFC_FCT-320_ikp0888	Auto generated PDU Stream as part of routing PDU dataflow and monitoring group	✓	✓

Figure 130: Inputs Screen (PDU Streams Tab)

- Select one or more **PDU Streams** from the list.
If you want to add dataflows, complete steps 7 thru 9
- (Optional) If you want Message Switch linksets included, click **MSW** field where it asks you if you want MSW linksets .
- Select the **PDU Dataflows** tab.

Counter Activation **Inputs** General Parameters SSN Filters Linkset Filters

Do you want to include MSW Linksets

PDU Streams **PDU Dataflows**

SS7 Q752

<input type="checkbox"/>	#	PDU Dataflow Name	Type
<input type="checkbox"/>	1	CCM_BICC_DF	MSU
<input type="checkbox"/>	2	CCM_ETSI_ISUP_DF	MSU
<input type="checkbox"/>	3	DF1test	MSU
<input type="checkbox"/>	4	STCtoFC	MSU
<input type="checkbox"/>	5	mercury_sthsi_1	MSU

Figure 131: Inputs Screen (PDU Dataflows Tab)

- Select what type of **dataflow** (SS7 / Q.752) .
Note: You can select both types of input streams.
- Select one or more **PDU Dataflows** from the list.
- Click **Next**.

The General Parameters screen appears.

Counter Activation Inputs **General Parameters** SSN Filters Linkset Filters

No PDU Timeout(sec)
600

Automatically Clear Alarms

Figure 132: General Parameters Screen

- Enter the **number of sec** in the the No PDU Timeout field (default is 600).
- (Optional) Select to **automatically clear alarms** after the process has run.

12. Click **Next**.

The SSN Filter screen appears.

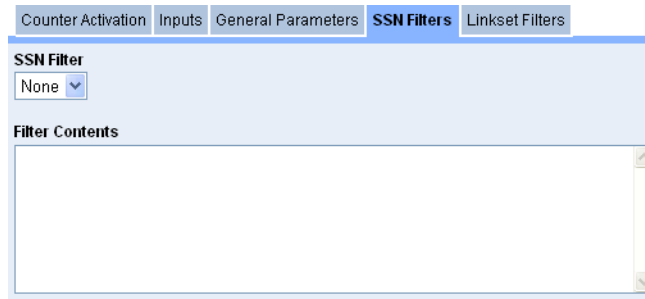


Figure 133: SSN Filter Screen

13. Select the **SSN Filter** type from the pull-down menu.

The contents of the filter appears in the Filter Contents field.

14. Click **Next**

The Linkset Filters screen appears.

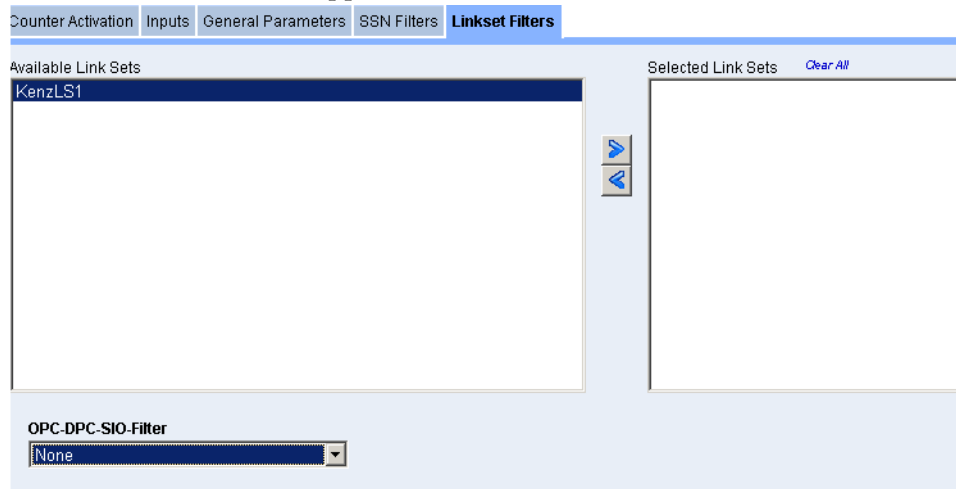


Figure 134: Linkset Filters Tab

15. Select one or more **Available Linksets**.

16. Click **right arrow** to place them into the Selected Linksets field.

17. (Optional-according to the linksets used) Select an **OPC-DPC-SIO Filter**.

18. Click **Finish**.

The configured Q.752 processing is saved.

Note: Make sure you apply changes for the changes to be reflected in the IXP subsystem.

About Distributions

The distribution option enables you to move IXP Dataflow Processing from one server to another for the purpose of load sharing. Complete these steps to use the Distribution option.

1. Select **Site >IXP Subsystem > Distribution**.

The Dataflow distribution list screen opens shown below.

Dataflow Processing	Type	Input Stream(s)	Output Stream(s)/Session(s)	Server
1 dfp_ip_010808	Building	pmf_ip_stream_010808	B_VoipMgcpCap_010808_2	ixp0960-1c
2 S_VoipMgcpCap_010808	Storage	B_VoipMgcpCap_010808_2	VoipMgcpCap_010808	ixp0960-1c
3 Sample DPF	Building	imf_isup_stream_010808	B_Sample3_6 B_Sample_3 B_Sample1_4 B_Sample2_5	ixp0960-1a
4 S_Sample	Storage	B_Sample_3	Sample	ixp0960-1c
5 S_Sample1	Storage	B_Sample1_4	Sample1	ixp0960-1c
6 S_Sample2	Storage	B_Sample2_5	Sample2	ixp0960-1c

Figure 135: Distribution List

2. Select a different **server** from the *dataflow processing* *Server* column pull-down list.
3. Click **Done**.

You are prompted to synchronize to save the changes to the subsystem.

About Software

The software option enables you to view the applications on each IXP server. Selecting the software option opens the *Software List* screen shown below.

```

IXP package
Name      : TKLCixp                Relocations: (not relocatable)
Version   : 4.0.0                  Vendor: Tekelec
Release   : 8.2.0                Build Date: Wed 16 Jul 2008 10:13:31 AM EDT
Install Date: Wed 16 Jul 2008 03:47:18 PM EDT   Build Host: deneb
Group     : IAS/IXP              Source RPM: TKLCixp-4.0.0-8.2.0.src.rpm
Size      : 75697501             License: Tekelec
Signature : (none)
URL       : http://www.tekelec.com
Summary   : Integrated xDR Platform

MySQL_IDB package
Name      : comcol-mysql          Relocations: (not relocatable)
Version   : 5.1.1                Vendor: (none)
Release   : p2677_tpd3.1.0_61.10.0 Build Date: Thu 05 Jun 2008 01:51:01 PM EDT
Install Date: Wed 16 Jul 2008 03:43:13 PM EDT   Build Host: localhost
Group     : System Environment/Base Source RPM: comcol-5.1.1-p2677_tpd3.1.0_61.10.0.src.rpm
Size      : 9063280              License: Tekelec (C) 2006
    
```

Figure 136: Software List Screen

The *Software List* screen has a tab for each server in the subsystem as well as the xDR Builders.

The IXP *Server* tab lists:

- IXP Package contents (shown above)
- MySQL-IDB Package contents (shown above)
- COMCOL Package contents (not shown)
- IXP Builders Package contents (not shown)

About Subsystem Preferences

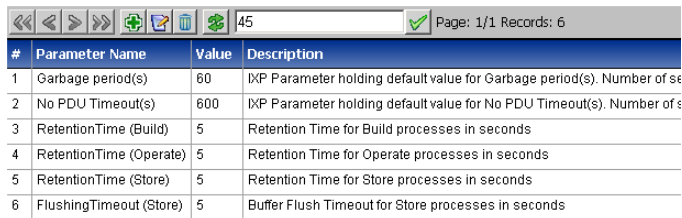
Subsystem references enables you to create preferences with values for the subsystem.

Adding a subsystem Preference

Complete these steps to add a subsystem preference.

1. Select **Mediation > Site > Subsystem > Subsystem Preferences**.

The *Subsystem Preferences* screen opens shown below.



#	Parameter Name	Value	Description
1	Garbage period(s)	60	IXP Parameter holding default value for Garbage period(s). Number of se
2	No PDU Timeout(s)	600	IXP Parameter holding default value for No PDU Timeout(s). Number of ε
3	RetentionTime (Build)	5	Retention Time for Build processes in seconds
4	RetentionTime (Operate)	5	Retention Time for Operate processes in seconds
5	RetentionTime (Store)	5	Retention Time for Store processes in seconds
6	FlushingTimeout (Store)	5	Buffer Flush Timeout for Store processes in seconds

Figure 137: Subsystem Preferences List Screen

2. Click **Add**.

The *Subsystem Preferences Add* screen opens shown below.

Mediation > **Sites** > **IXP-M12** > **IXP** > **ixp1108** > **Subsystem Preference**

Name

Value

Reset to Default

Description

Reset **Cancel** **Add**

Figure 138: Subsystem Preferences List Screen

3. Enter the **Name** of the preference.
4. Enter a **Value** (or to reset value click **Reset to Default**).

Note: The values can be for:

- Garbage Periods - integer between 0 and 32767
- No PDU Timeouts - integer between 1 and 32767
- RetentionTime (Build) - default is 5
- RetentionTime (Operate) - default is 5
- RetentionTime (Store) - default is 5
- FlushingTime (Store) - default is 5

5. (Optional) Enter a **Description** of the preference.
6. Click **Add**.

The preference is added to the list.

Modifying a subsystem Preference

Complete these steps to add a subsystem preference.

1. Select **Mediation > Site > Subsystem > Subsystem Preferences**.
The *Subsystem Preferences* screen opens.
2. Select the **Preference** that needs to be modified.
3. Make the necessary modifications.
4. Click **Modify**.
The preference is modified.

Deleting a Subsystem Preference

Complete these steps to add a subsystem preference.

1. Select **Mediation > Site > Subsystem > Subsystem Preferences**.
The *Subsystem Preferences* screen opens.
2. Select the **Preference** to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.
The record is deleted.

Managing Multiple IXP Subsystems

The *Mediation* perspective enables you to manage certain elements globally, (multiple IXP subsystem within a site or IXP subsystems within multiple sites). The following elements can be managed globally.

- xDR filters - see [About xDR Filters](#)
- Dictionaries - see [About Dictionaries](#)
- Sessions - see [About Sessions](#)

About Dictionaries

Dictionaries describe a session, by providing its column names, titles, syntax, data type, and other information. A dictionary is a text file with an *a7d* extension that is physically stored on a server. Dictionaries must be present in the NSP database in order for NSP applications to use them.

In general, a DIH application is not based on the specific content of a dictionary, rather, it can adapt based on the content of a dictionary. Therefore, for an application to be able to do anything with a session, the dictionary for it must reside in the NSP *database*. This section describes how to create dictionaries. Dictionaries are specified in ASCII format and a dictionary file extension is *a7d*.

Select **Mediation > Dictionaries**. The *Dictionary List* screen opens shown below. From this screen you can add, modify and delete dictionaries.

Dictionary Name	Type	Version	Protocol	Stack	Action
13124 Stat26FPv	STATISTICS	1.0.0	N/A	N/A	[Add] [Edit] [Delete]
16867 dfvgtb	STATISTICS	1.0.0	N/A	N/A	[Add] [Edit] [Delete]
16913 CCCC_1	STATISTICS	1.0.0	N/A	N/A	[Add] [Edit] [Delete]
25591 BPL_BOSCH	STATISTICS	1.0.0	N/A	N/A	[Add] [Edit] [Delete]
25596 BPL_BOSCH	STATISTICS	1.0.0	N/A	N/A	[Add] [Edit] [Delete]
9292 JFM_Stats	STATISTICS	1.0.0	N/A	N/A	[Add] [Edit] [Delete]
GPRS Ob Stats_5,0,2	STATISTICS	5,0,2	N/A	N/A	[Add] [Edit] [Delete]
GPRS Ob TDR_5,3,0	RECONSTITUTION	5,3,0	GPRS Ob	GENERIC	[Add] [Edit] [Delete]
GPRS Ob TDR_CAPTURE_5,3,0	CAPTURE	5,3,0	GPRS Ob	GENERIC	[Add] [Edit] [Delete]
GPRS Gn Op CDR_5,1,0	RECONSTITUTION	5,1,0	GPRS Gn Op	GENERIC	[Add] [Edit] [Delete]
GPRS Gn Op State_5,0,0	STATISTICS	5,0,0	N/A	N/A	[Add] [Edit] [Delete]
GPRS Gn Op TDR_5,3,0	RECONSTITUTION	5,3,0	GPRS Gn Op	GENERIC	[Add] [Edit] [Delete]
GPRS Gn Op TDR_CAPTURE_5,3,0	CAPTURE	5,3,0	GPRS Gn Op	GENERIC	[Add] [Edit] [Delete]

Figure 139: Dictionary List Screen

Creating a Dictionary

Dictionaries describe a session, by providing its column names, titles, syntax, data type, and other information. Dictionaries must be present in the NSP database in order for NSP applications, such as ProTrace to use them. Complete these steps to add a dictionary to the system.

1. Select **Mediation > Dictionaries**.
2. Click **Add** on the tool bar.

The *Add* screen opens shown below.

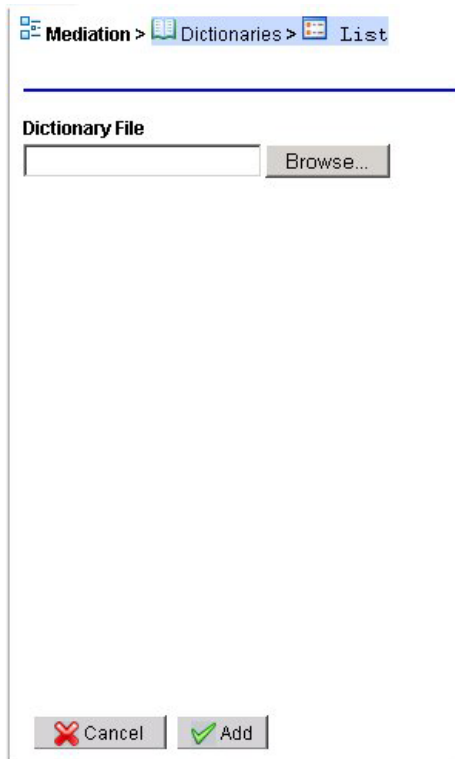


Figure 140: Add Dictionary Screen

3. Browse for the **Dictionary File**.
(A dictionary is a text file with an *a7d* extension that is physically present on the IXP subsystem.)
4. Click **Add**.
The dictionary is added to the system.
5. From the host right-click menu, select **Apply Changes** for the changes to take effect.

Modifying a Dictionary

Complete these steps to modify an existing dictionary file-type reconstitution.

1. Select **Mediation > Dictionaries**.
The *List* screen opens.
2. Select the **Dictionary** to be modified.
3. Click **Modify**.
The *ModifyDictionary* screen opens shown below.

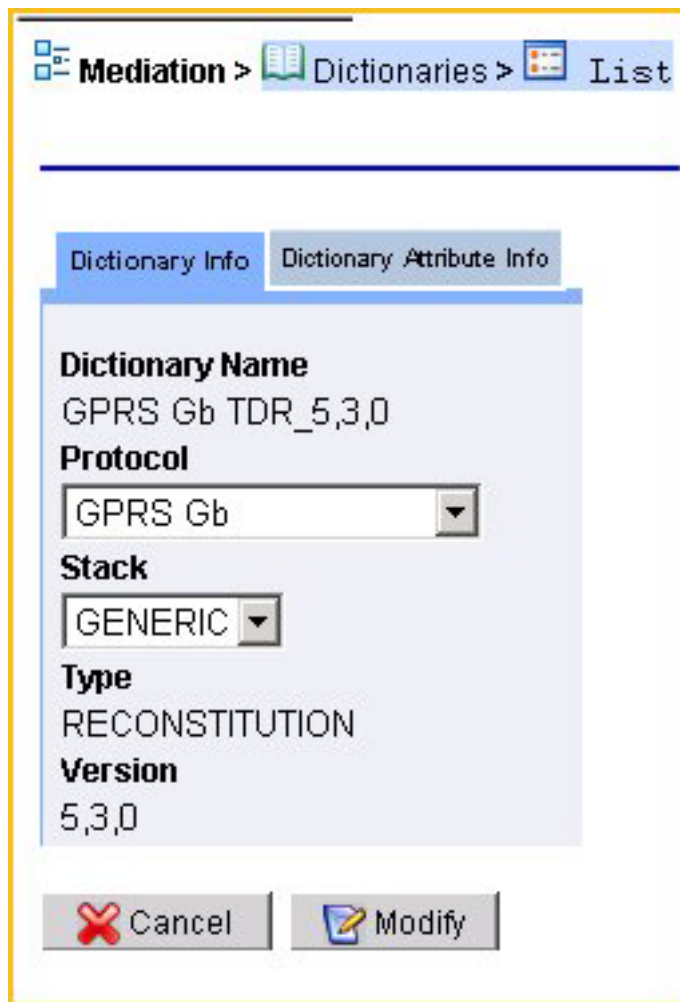


Figure 141: Modify Dictionary - Dictionary Info Tab

4. Select **Dictionary Info** tab.
5. Modify either the **Protocol** or **Stack** information.
6. Select **Dictionary Attribute Info** tab shown below.

The screenshot shows a web application interface for 'Mediation > Dictionaries > List'. Below the navigation, there are tabs for 'Dictionary Info' and 'Dictionary Attribute Info'. The main area displays a table with 9 rows of attribute information. The table has columns for 'Attribute Name', 'Short Name', 'Long Name', 'Description', 'Enumeration', and 'Conditionable'. Each row has a checkbox in the first column.

	Attribute Name	Short Name	Long Name	Description	Enumeration	Conditionable
<input type="checkbox"/>	CellUpdateDuringTransfer	Cell Update During Transf	Cell Update During Transf	Indicates if the Cell Updat	Yes	<input checked="" type="checkbox"/>
<input type="checkbox"/>	CauseNSorBSSGP	Cause NS or BSSGP	Cause NS or BSSGP	This field holds the differ	Yes	<input checked="" type="checkbox"/>
<input type="checkbox"/>	IMSI	IMSI	International Mobile Subst	International Identifier of a	No	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SMCause	SMCause	SM Cause	SM Cause	Yes	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SenCentAdd	SCA	SCA, Service Center Addr	Taken from RP Originator	No	<input checked="" type="checkbox"/>
<input type="checkbox"/>	UDHI	UDHI	UDHI, Transfer protocol u	Parameter indicating that	Yes	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ANumberNature	A-nature	A-nature of address	Taken from the nature of a	Yes	<input checked="" type="checkbox"/>
<input type="checkbox"/>	CellReselecDuration	Cell Reselec Dur	Cell Reselection Duration	Duration between incomin	No	<input checked="" type="checkbox"/>
<input type="checkbox"/>	UnitsTotalSizeIn	Size UL	Size, for total sum of UI U	Size (in bytes) of all UpLir	No	<input checked="" type="checkbox"/>

Figure 142: Modify Dictionary - Dictionary Attribute Info Tab

7. Select the **Attribute(s)** to be modified.
You can modify the following fields.
 - a) Short Name
 - b) Long Name
 - c) Description
8. Select the following within the attribute:
 - a) If attribute is to have **Conditions**.
 - b) If attribute is to be **Displayed**
 - c) If attribute is to be **Masked**.
(For privacy reasons.) If it is to be masked then complete the following steps.
 - Select what part should be masked (**Beginning, End, Hide All**).
 - How many **digits** should be hidden.
9. Repeat steps 7-8 for each attribute.
10. Click **Modify**.
The Capture type dictionary is modified.

Enabling or Disabling PDU Decode Hiding for a Dictionary

Complete these steps to enable or disable PDU decode hiding for a specific dictionary.

Note: The PDU hide option must be enabled to use the PDU decode hide feature. See Enabling or Disabling PDU Hiding from the Home Page.

Note: The dictionary must be added to the system before the PDU decode hiding feature can be enabled or disabled.

1. Select **Mediation > Dictionaries**.
The *List* screen opens.
2. Select the **Dictionary** to be modified.
3. Click **Modify** from the tool bar.

4. Select the **Protocol Hiding** tab.
5. Select **Hide** for a specific category.
Note: To disable the hide feature, click on the the selection field to de-select the hide feature.
6. Click **Modify**.

Editing Category Titles in a Dictionary

Complete these steps to edit Category Titles for a for a specific dictionary.

1. Select **Mediation > Dictionaries**.
The *List* screen opens.
2. Select the **Dictionary** to be modified.
3. Click **Modify** from the tool bar.
4. Select the **Protocol Hiding** tab.
5. Select **Hide** for a specific category.
Note: To disable the hide feature, click on the the selection field to de-select the hide feature.
6. Click **Modify**.

Enabling and Disabling PDU Summary Hiding

Complete these steps to enable or disable PDU summary hiding for a specific protocol.

Note: The PDU hide option must be enabled to use the PDU decode hide feature. See Enabling or Disabling PDU Hiding from the Home Page.

Note: The dictionary must be added to the system before the PDU decode hiding feature can be enabled or disabled.

1. Select **Mediation > Dictionaries**.
The List screen opens.
2. Select the **Dictionary** to be modified.
3. Click **Modify** from the tool bar.
4. Select the **Protocol Summary Hiding** tab.
5. Select **Mask** for the heading.
Note: To disable the hide feature, click on the the selection field to de-select the hide feature.
6. Select **Hide All** option from the Hidden From column drop-down list.
7. Click **Modify**.

Deleting a Dictionary

Note: You cannot delete a dictionary if it is associated with a session. You must first disassociate the session from the dictionary or delete any children of that dictionary .

Complete these steps to delete a dictionary from the system.

1. Select **Mediation > Dictionaries**.
The *List* screen opens.
2. Select the **Dictionary** to be deleted.
3. Click **Delete**.

Note: To delete only one dictionary file, click *Delete* in the actions column. To delete several dictionary files, select each file and click *Delete* on the toolbar.

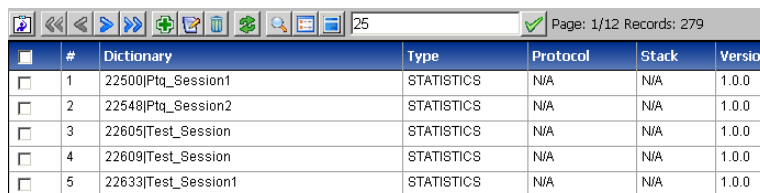
4. Click **OK** at the prompt.
The dictionary is deleted from the list.

Viewing a Dictionary Source

The *View Source* option enables you to view the dictionary source file (.a7d file) as a text file. To view a dictionary source file, complete these steps.

1. Select **Mediation > Dictionaries**.

The *List* screen opens shown below.

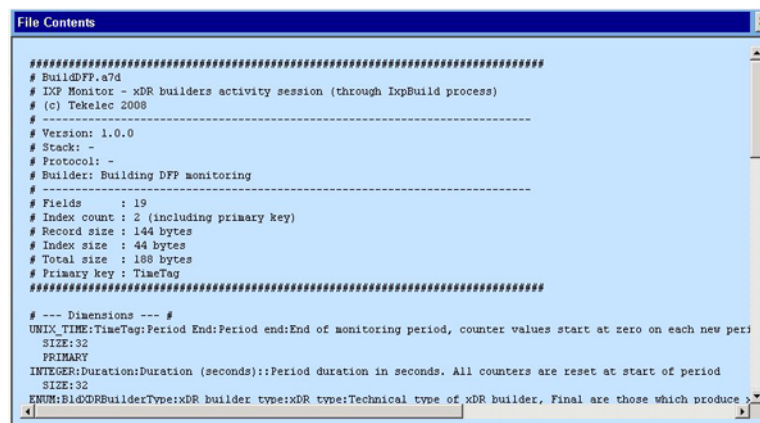


#	Dictionary	Type	Protocol	Stack	Version
1	22500 Pttq_Session1	STATISTICS	N/A	N/A	1.0.0
2	22548 Pttq_Session2	STATISTICS	N/A	N/A	1.0.0
3	22605 Test_Session	STATISTICS	N/A	N/A	1.0.0
4	22609 Test_Session	STATISTICS	N/A	N/A	1.0.0
5	22633 Test_Session1	STATISTICS	N/A	N/A	1.0.0

Figure 143: Dictionary List Screen

2. Select the **dictionary** source you want to view shown above.
3. Click **View Source** from the tool bar.

The source file opens shown below.



```
#####
# BuildDFP.a7d
# IXP Monitor - xDR builders activity session (through IxpBuild process)
# (c) Tekelec 2008
# -----
# Version: 1.0.0
# Stack: -
# Protocol: -
# Builder: Building DFP monitoring
# -----
#
# Fields      : 19
# Index count : 2 (including primary key)
# Record size : 144 bytes
# Index size  : 44 bytes
# Total size  : 188 bytes
# Primary key : TimeTag
#####

# --- Dimensions --- #
UNIX_TIME:TimeTag:Period End:Period end:End of monitoring period, counter values start at zero on each new per
SIZE:32
PRIMARY
INTEGER:Duration:Duration (seconds)::Period duration in seconds. All counters are reset at start of period
SIZE:32
ENUM:BuildXDRBuilderType:xDR builder type:xDR type:Technical type of xDR builder. Final are those which produce
```

Figure 144: Dictionary List Screen

Click the **Close** icon at the top right-hand corner of the screen to close the file.

Listing Unused Dictionaries

The Discrepancy Report option enables you to list the dictionaries that are unused after an update. To view the Discrepancy report, complete these steps.

1. Select **Mediation > Dictionaries**.

The *List* screen opens.

2. Select a **Dictionary** that has been updated.

Note: All updated dictionaries will be in bold type.

#	Dictionary	Type	Protocol	Stack	Version	Used
12	GPRS Gb Stats by APN_5,1,0	STATISTICS	N/A	N/A	5,1,0	Y
13	GPRS Gb Stats by Cell_5,1,0	STATISTICS	N/A	N/A	5,1,0	Y
14	GPRS Gb Stats by IMEI_5,1,0	STATISTICS	N/A	N/A	5,1,0	Y
15	GPRS Gb TDR_5,3,3	RECONSTITUTION	GPRS Gb	GENERIC	5,3,3	Y
16	GPRS Gb TDR_CAPTURE_5,3,3	CAPTURE	GPRS Gb	GENERIC	5,3,3	Y
17	GPRS Gn/Gp CDR_5,2,0	RECONSTITUTION	GPRS Gn Gp	GENERIC	5,2,0	Y
18	GPRS Gn/Gp Stats_5,0,0	STATISTICS	N/A	N/A	5,0,0	Y
19	GPRS Gn/Gp TDR_5,3,3	RECONSTITUTION	GPRS Gn Gp	GENERIC	5,3,3	Y
20	GPRS Gn/Gp TDR_CAPTURE_5,3,3	CAPTURE	GPRS Gn Gp	GENERIC	5,3,3	Y
21	Generic ProTrace SUDR_1,0,2	SUDR	All	GENERIC	1,0,2	Y
22	Generic SUDR_2.3.1	SUDR	All	ETSI	2.3.1	Y
23	IMS COPS TDR_1,3,2	RECONSTITUTION	IMS COPS	GENERIC	1,3,2	Y
24	IMS COPS TDR_CAPTURE_1,3,2	CAPTURE	IMS COPS	GENERIC	1,3,2	Y
25	IMS DIAMETER CC CDR_1,8,6	RECONSTITUTION	IMS DIAMETER	GENERIC	1,8,6	Y

Figure 145: Dictionary List with Unused Dictionary Selected

3. Select the **View Discrepancy Report** button on the tool bar to generate the report (last button on right). The report screen opens.

The report shows:

- Basic Information
- Non-ENUM Field(s) Descrepancies
- ENUM Field(s) Descrepancies

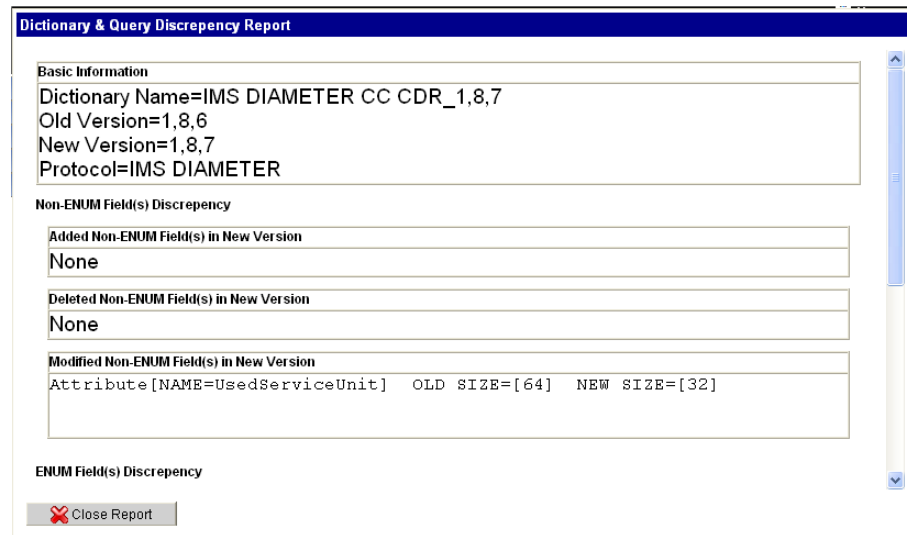


Figure 146: Unused Dictionary Discrepancy Report

4. Click the **Close Report** to close the report.

About xDR Filters

xDR Filters are treated as global entities. xDR Filters are needed when:

- A subset of the generated xDRs are *operated on* or *stored* where xDRs matching a condition can be filtered out.

The figure below shows the xDR filters list screen.



Figure 147: Xdr Filter List Screen

Adding xDR Filters

Complete these steps to add an xDR filter.

1. Select **xDR filters**.
The *xDR Filter List* screen opens.
2. Click **Add** (or right click on the xDR Filters object tree).
The *xDR filter add* screen show below.

Figure 148: Xdr Filter Add Screen

3. Type in a **filter name**.
4. (Optional) Type in a **description**.
5. Select the **dictionary** that is associate with the filter.
6. Create the **filter**.
 - a) Click **Add**.

(not shown in the figure above). The field definition fields open shown below.

Note: The filter screen provides an automatic operator selection with a default to *and*. You can choose one of the other two operators if you need them when creating filters with several expressions.

Figure 149: Filter Definition Screen

- b) Select a **field** from the pull-down list.
- c) Select an **operator** from the pull-down list.
- d) Select a **value** from the pull-down list.
- e) Repeat steps **b-d** to create more expressions.

Note: Each expression is labeled A, B, C... with the operator between them. For example, A AND B, B OR C are examples of simple expressions.

7. Click **Create**.

The filter is created and saved to the system shown below.

The screenshot shows a web interface for 'Mediation > xDR Filters > List'. It features a table with columns: Filter Number, Filter Name, Description, Dictionary Name, Dictionary Version, and Actions. There are two rows of filter data.

Filter Number	Filter Name	Description	Dictionary Name	Dictionary Version	Actions
1	Sample_xDR_Filter_2	This is an example of an OR expression filter	BuildMonitor	VERSION	[Edit] [Delete]
2	sample_xDR_filter	This is an example of an xDR filter used for NSP applications	BuildMonitor	VERSION	[Edit] [Delete]

Figure 150: Added Xdr Filter To List

Modifying xDR Filters

Complete these steps to modify an xDR filter.

1. Select **xDR filters**.
The *xDR Filter List* screen opens.
2. Select the **xDR filter** to be modified.
3. Click **Modify** (or right click on the specific xDR Filter object tree).
The *xDR filter modify* screen opens.
4. Make the necessary modifications.
5. Click **Modify**.
The xDR filter is modified.

Deleting xDR Filters

Note: You cannot delete an xDR filter if it is used in a dataflow processing. You must first delete the dataflow processing or any other dependent object before you can delete the filter.

Complete these steps to delete an xDR filter.

1. Select **xDR filters**.
The *xDR Filter List* screen opens.
2. Select the **xDR filter** to be deleted.
3. Click **Delete** (or right click on the specific xDR Filter object tree).
4. Click **OK** at the prompt.
The xDR filter is deleted from the list.

About Sessions

The sessions menu option provides a convenient means of viewing discovered sessions as well as viewing statistical information on a session that is used by the NSP applications such as: ProTraQ, ProPerf and ProTrace. CCM enables you to create, modify and delete xDR sessions globally.

Note: A session name must be unique for each IXP subsystem or dataserer, but sessions can have identical names if they reside on separate IXP subsystems.

Selecting the **Sessions** object from the *Object tree* opens the *xDR Sessions List* screen.

#	Session	Type	Format	Dictionary	Subsystem Name	Lifetime	Sequence ID
1	BVT_SESSION	RECONSTITUTION	SINGLE	SS7 ISUP ANSI CDR_2,6,0	ixp0888_Pool	72	Disabled
2	test_phl_historical	STATISTICS	SINGLE	47702test_phl_historical	ixp0888_Pool	840	Disabled
3	BSS_RANCC_11Aug1_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled
4	BSS_RANCC_11Aug2_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled
5	BSS_RANCC_PT3_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled
6	BSS_RANCC_PT_S	RECONSTITUTION	SINGLE	RAN CC CDR_6,2,2	ixp0888_Pool	72	Disabled

Figure 151: xDR Sessions List Screen

About xDR Session Table Layout

The *Sessions List* screen is in table format and has the follow information:

Table 49: Xdr Table Layout

Column	Description
Select	Enables you to select one or more sessions
Session	Provides the name of the session
Type	Shows the type of session: <ul style="list-style-type: none"> • Reconstitution • Capture • Statistics • SUDR
Format	Shows the type of format the session is in.
Dictionary	Shows the name of the dictionary associated with the session
Host	Shows the name of the host that houses the dictionary and the session
Lifetime	Shows how long, in hours, the session is scheduled to run
Sequence ID	Shows if the session is enabled or disabled
User Information	Provides additional information about the session
Owner	Shows the name of the user who created the session

Column	Description
State	Shows the state of the session
Replace by	Shows the name of the user who has altered the session
Created	Shows the data and time the session was created

Listing xDR Sessions

Complete these steps to list xDR sessions.

1. Select **Mediation > Sessions**
2. Right-click and select **List**.

The *List* screen opens.

The xDR Session screen tool bar has the following function buttons

Table 50: xDR Tool Bar

Button	Description
Select Columns	Enables you to select the columns you want to view
First Page	Enables you to go to the first page of a multi-page list of sessions
Previous page	Enables you to go to the previous page of a multi-page list of sessions
Next page	Enables you to go to the next page of a multi-page list of sessions
Last page	Enables you to go to the last page of a multi-page list of sessions
Add	Enables you to add a session
Modify	Enables you to modify a session
Delete	Enables you to delete a session
Refresh	Enables you to refresh a screen to view any changes you have made
Filter sessions	Opens the filter query screen and enables you to search for specific sessions
Permissions	Enables you to set permissions for different users (write, read, execute)
Modify session backup	Enables you to select one or more sessions in order to modify session backup options

Adding a Protocol-Specific xDR Session

A protocol-specific xDR session must be created to house the xDRs for that protocol.

Once xDR generation is configured for a builder, xDR records are stored in a session. A session is associated with a dictionary. The dictionary mechanism is a way of describing the content of the xDR fields. NSP applications, such as ProTrace use the dictionary to access and display the data making the applications independent of the xDR record format.

Complete these steps to add an protocol-specific xDR session.

1. Select **Mediation > Sessions**.

The *xDR Sessions List* screen opens.

2. Click **Add** from the toolbar.

The *Add* screen opens shown below.

The screenshot shows a web-based form for adding an xDR session. The breadcrumb navigation at the top reads: Mediation > Sites > Morrisville > IXP > ixp0500 > Sessions > List. The form has several input fields: 'Session Name' with the value 'Sample_Session', 'Lifetime (hours)' with the value '72', 'Storage' with a dropdown menu showing 'ixp5001-1a', 'Dictionary' with a dropdown menu showing '8951|monica_sess', and a 'Description' text area containing the text 'This is an example of a session'. At the bottom of the form are three buttons: 'Reset' (with a red arrow icon), 'Cancel' (with a red X icon), and 'Add' (with a green checkmark icon).

Figure 152: xDR Session Add Screen

3. Type a **Session name**.

Note: The session name must be unique for each IXP subsystem, but sessions can have identical names if they reside on separate IXP subsystems.

4. Type in the **Lifetime** (number of hours the session exists).

Note: It is recommended that the Lifetime not be less than 48 hours. Anything less than 48 hours can lead to potential data loss or truncation of last 24 hours due to nightly purges of the system.

Note: Adding more than five (5) sessions in one 24 hour period may cause xDR storage degradation. Please consider spacing your session additions over several days to ensure xDR storage performance.

5. Select the **Storage** subsystem.
6. Select the **Dictionary** associated with the session.
7. (Optional) Type in a **Description**. Shown below is a completed session.
8. Click **Add**.

The session is added to the session list shown below.

Mediation > Sessions > List

Session	Type	Format	Dictionary	Host	Lifetime
<input type="checkbox"/> 1 AG_ISUP_ANSI_28	RECONSTITUTION	SINGLE	SS7 ISUP ANSI CDR_2,4,0	ixp0960-1a	120
<input checked="" type="checkbox"/> 2 Sample_Session	STATISTICS	SINGLE	BuildMonitor	ixp0960-1a	150
<input type="checkbox"/> 3 xip0960StreamMonitor	STATISTICS	SINGLE	StreamMonitor	ixp0960-1a	336
<input type="checkbox"/> 4 xip0960BuildMonitor	STATISTICS	SINGLE	BuildMonitor	ixp0960-1a	336
<input type="checkbox"/> 5 xip0960OperateMonitor	STATISTICS	SINGLE	OperateMonitor	ixp0960-1a	336
<input type="checkbox"/> 6 xip0960StoreMonitor	STATISTICS	SINGLE	StoreMonitor	ixp0960-1a	336
<input type="checkbox"/> 7 INAP_Rec_28	RECONSTITUTION	SINGLE	SS7 INAP TDR_2,9,5	ixp0960-1a	100

Figure 153: Completed Session In Session List

Modifying an xDR Sessions

1. Select **Mediation > Sessions**.
The sessions list screen opens.
2. Select the **session** to be modified shown here.

Session	Type	Format	Dictionary	Host	Lifetime
<input checked="" type="checkbox"/> 1 Sample_Session	CAPTURE	SINGLE	SS7 AIN TDR_CAPTURE_2,6,1	ixp5001-1a	72
<input type="checkbox"/> 2 Sample_Session_1	RECONSTITUTION	SINGLE	SS7 AIN TDR_2,6,1	ixp5001-1a	72
<input type="checkbox"/> 3 xip5001StreamMonitor	STATISTICS	SINGLE	StreamMonitor	ixp5001-1a	336

Figure 154: Selected Session For Modification

3. Click **Modify** on the toolbar.
The session record opens shown below.

Session Name: Sample_Session Lifetime (hours): 72 Storage: xip5001-1a

Dictionary: SS7 AIN TDR_CAPTURE_2,6,1

Sequence Id: Enabled

Description:

Buttons:

Figure 155: Modify Session Screen

4. You can only modify the **Lifetime (hours)**, **Sequence ID** or the **Description** fields.
5. Click **Modify**.
The record is modified.

Deleting xDR Sessions

Complete these steps to delete an xDR session.

Note: You can not delete a session that is using a dataflow processing. You must first delete the dataflow processing or modify the dataflow processing to use another session.

Note: Important--When you delete a session on CCM, the session also gets deleted in the IXP database causing all the xDRs stored in the session also to be deleted.

1. Select **Mediation > Sessions**.
The sessions list screen opens.
2. Select the **session** to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt. The session is deleted.

Purging Static Sessions

There are times when it is necessary to purge static sessions from the IXP subsystem by using the `ManageStaticPurge.sh` command. Complete these steps to purge static xDR sessions from the IXP subsystem.

1. Log into the **Oracle database**. (`./ManageStaticPurge.sh <connection> <option>`)
Must use Oracle userid and password (`password@db_string`).

2. Enter one of the following command options:

```
./ManageStaticPurge.sh
-c# create the job
-r# remove the job
-d# disable the job
-e# enable the job
-m# modify the job: = new job frequency in hours
```

3. Log out of the Oracle database.

Creating an xDR filter for an existing Session

You can create a filter for an existing xDR session using the **Filter sessions** button on the toolbar shown below.

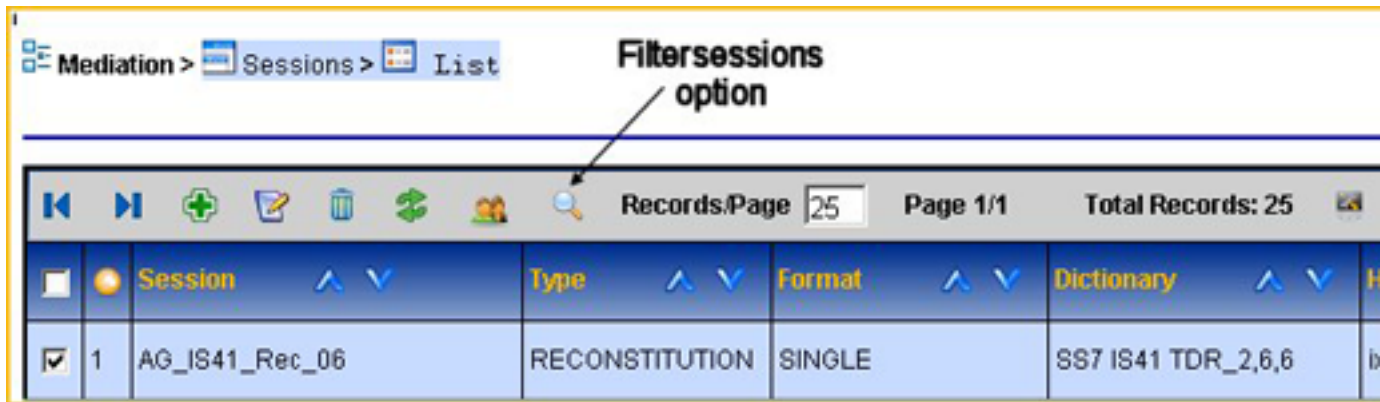


Figure 156: Xdr Session Filter Icon

Clicking on the button opens the filter screen. For more information, see [“Adding xDR Filters.”](#)

Modifying xDR Session Backups

CCM enables you to modify session backup options. Complete these steps to modify an existing session backup.

1. Select **Mediation > Sessions**.
The sessions list screen opens.
2. Select the **session** to be modified.
3. Click **Modify Backup** from the toolbar shown below.

The *Modify Backup* screen opens.



Figure 157: Modify Session Backup Toolbar

4. Select the **backup option** (none, xDR only, xDR and PDU) from the pull-down list.
5. Click **Modify**.
The backup option is modified for that session.

Creating and associating a dictionary with a Session

Complete these steps to create and associate a dictionary with an xDR session.

1. Select and right-click on the **IXP subsystem** that needs the sessions.
2. Select **discover sessions**.

The discovery process begins and the *Sessions List* screen opens shown below.

Session Name	Remote Status	NSP Status	Action Remark	Type	Dictionary	Actions
1 AG_ISUP_ANSI_28	✓	✓	No change found in session	RECONSTITUTION	SS7 ISUP ANSI CDR_2,4,0	Discover Session
2 INAP_Rec_28	✓	✓	No change found in session	RECONSTITUTION	SS7 INAP TDR_2,9,5	Discover Session

Figure 158: Sessions List

3. Select a **session**.
4. Click **create/associate dictionary** that belongs to that session (*Actions* column - *Discover Session*).

Note: If there is already more than one session associated with a dictionary, you can select another session from the pull-down list from the *Associate with existing dictionary and discover session* field and click Apply dictionary & Discover session.

Figure 159: Associate Dictionary Screen

5. Enter the **Dictionary Name**.
6. Select the **Stack** for the dictionary.
7. Select the **Protocol** for the dictionary.
8. Enter a **version number** for the dictionary.
9. Click **Create dictionary**.

The dictionary is created shown below.

Note: You must now synchronize the subsystem to apply changes. For more information see, [About Applying Changes to an IXP Subsystem](#) .

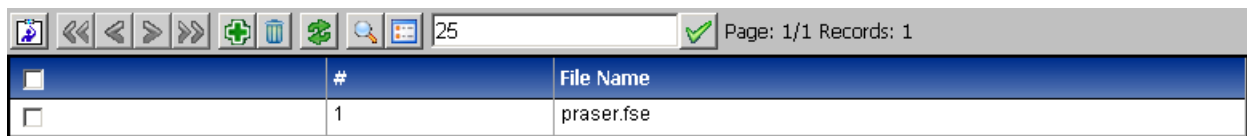
xDR Builder Parameters

Each Build xDR session of a dataflow processing has a set of parameters that are set by default but can be customized for your system. Refer to Appendix C “xDR Builder Parameters” for descriptions of builder fields.

About Enrichment Files

Enrichment files are files with fse extension that enable you to populate xDRs with additional fields. These fields are used by *ProTraq*.

Selecting the **Enrichment Files** object from the Object tree opens the Enrichment Files List screen.



	#	File Name
<input type="checkbox"/>	1	praser.fse

Figure 160: Enrichment Files List Screen

Adding Enrichment Files

Complete these steps to add enrichment files.

1. Select **Mediation > Enrichment Files**.

The *xDR Sessions List* screen opens.

2. Click **Add** from the toolbar.

The *Add* screen opens.



Enrichment File

Browse...

Cancel Upload

Figure 161: Xdr Session Add Screen

3. Click **Browse...**
4. Locate the file **fse file** in its directory.
5. Click **Upload**.

The file is uploaded into the system.

Deleting Enrichment Files

Complete these steps to delete enrichment files.

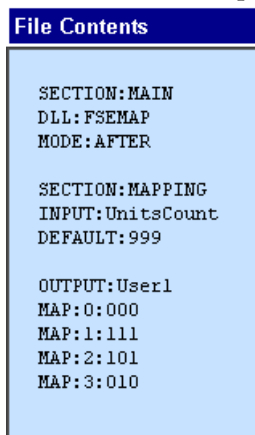
Note: Before deleting enrichment files, you must first delete any dependent objects belonging to the enrichment file. You must also *apply changes* to the subsystem before the changes take place.

1. Select **Mediation > Enrichment Files**.
The Enrichment Files list screen opens.
2. Select the **File** to be deleted.
3. Click **Delete** from the tool bar.
4. Click **OK** at the prompt.
The file is deleted from CCM.
5. Click **Upload**.
The file is uploaded into the system.

Viewing Enrichment File Source Code

Complete these steps to view enrichment files source code.

1. Select **Mediation > Enrichment Files**.
The Enrichment Files list screen opens.
2. Select the **File** to be viewed.
3. Click **Source** from the tool bar.
The source screen opens.



The screenshot shows a window titled "File Contents" with a light blue background. The text inside is as follows:

```
SECTION:MAIN
DLL:FSEMAP
MODE:AFTER

SECTION:MAPPING
INPUT:UnitsCount
DEFAULT:999

OUTPUT:User1
MAP:0:000
MAP:1:111
MAP:2:101
MAP:3:010
```

Figure 162: Source Code Screen

4. Click **Close** to close the screen.

Chapter 11

Monitoring Policies

Topics:

- [About 3G Monitoring Policies.....219](#)
- [About Filtering Monitoring Policies.....222](#)

About 3G Monitoring Policies

CCM is equipped with Intelligent Data Monitoring (IDM) for 3G. IDM enables customization of the PIC system to fit the amount of system traffic while providing two important parameters for on demand customer care:

- Less data to transfer to mediation (IXP) layer for less data to process and store
- Accurate and efficient traffic monitoring

xMF enhancement provides the capacity to reduce the traffic sent to IXP by sending all PDUs for on demand or sampled users. This capacity also enables load balancing between multiple IXP servers that results in more efficient traffic monitoring.

The Monitoring Policies Screen

The monitoring policies List screen is comprised a tool bar and two tables..

Besides the basic functions of adding, modifying and deleting selected users it has the additional functions:

- Filtering - the Filtering button provides the capacity to filter for specific policies
- Traffic Classifications - the Show Traffic Classification button shows the classifications for specific policies The traffic classifications for a specific policy appear on the bottom table
- Activating and deactivating - the Activate and Deactivate buttons provide the capacity to activate or deactivate specific policies

The policy (top) table provides the following information:

- Policy Name - name of policy
- Description - brief description of policy
- Policy Status - active or not
- On Demand - on demand is on or off
- Sampling - sampling is on or off
- Sampling Ratio - sampling ratio of mobile users
- Track Statistics - statistics for tracking sampled mobile users
- Owner - user who created policy
- State - activated or not
- Created - date created

The Traffic Classification (TC) table shows the following information for a selected policy:

- TC Name - shows the name of the TC for associated with the policy
- Description - shows any pertinent information about the TC
- Server - shows the server where the TC is located
- Internet Protocol - shows the protocol constraints for the TC
- Transport Protocol - shows the type(s) of transport protocol(s) for the TC
- Application Layer - shows the GTP layer IP address
- Forwarding - shows what is forwarding (for example, packets and counters)
- Annotations - Any special annotation for the traffic classification
- Status - shows if the traffic classification is active or not

Adding a Monitoring Policy

Prerequisites:

- PDU Filter (VLAN Filter) is created
- Traffic Classifications are created
- IP Dataflows are created with load balancing and GTP algorithms
- Dataflow Processings are created with appropriate builders (Gn/Gp mobile activity, IP HTTP TDR, IP MMS TDR and/or Gn/Gp TDR)

Complete the following steps to add a Monitoring Policy.

1. Select **Monitoring Policies > 3G Policies**.
2. Click **Add** from the tool bar on the polices table.

The Add Policies screen opens.

Note: Black arrows to the left of the fields signify if the field is expanded or not. (Down is expanded).

Table 51: Add Policies Screen Field Descriptions

Field	Description
Name	Alphanumeric field for adding name (limit 25 characters)
Description (Optional)	Text field for adding pertinent information (limit 255 characters)
On Demand	Default = No Check box select if you want to forward the user plane traffic for the mobile devices that are in demand by Customer Care (See Customer Care User Guide)
Sampling	Default = No Check box select yes to allow IPDR creation for a random sample of mobile users. PMF sends FULL control plane and FULL user plane packets for the selected traffic.
What is the percentage of mobile users	Numeric field that enables you to put in a percentage (0-100) that will be sampled (see sampling description)
Forward Statistics	Default = No Check box select "yes" enables IPDR creation for mobile users identified as to track activity statistics for all mobile users that are "on-demand" or sampled

Field	Description
	PMF sends FULL control plane and FULL user plane packets for the selected on-demand users.
GTP-C-TCs	<ul style="list-style-type: none"> Shows available GTP-C-TCs to be used with the policy. Multiple GTP-C-TCs can be selected Shows selected GTP-C-TCs for the policy.
GTP-U-TCs	<ul style="list-style-type: none"> Shows available GTP-U-TCs to be used with the policy. Multiple GTP-U-TCs can be selected Shows selected GTP-U-TCs for the policy

- Enter the **Name** of the policy.
- (Optional) Enter a **Description**.
- If the policy is to be On Demand, select **Yes**.
- If the policy is to have Sampling capabilities, select **Yes**
- If the policy is to have Forward Statistics capabilities, select **Yes**.
- (Optional) Select **GTP-C-TCs** that will be associated with the policy.
- (Optional) Select **GTP-U-TCs** that will be associated with the policy.
- Click **Add** to add the policy to the system.

Modifying a Monitoring Policy

Complete the following steps to modify a monitoring policy.

- Select **Monitoring Policies > 3G Policies**.
- Select the policy to be modified from the policy (top) table.
- Click **Modify** from the tool bar.
- Modify the appropriate values.
- Click **Modify**.

The database is updated with the change.

Deleting a Monitoring Policy

Complete these steps to delete a monitoring policy.

- Select **Monitoring Policies > 3G Policies**.
- Select the **policy** to be deleted
- Click **Delete**.
- Click **OK** at the prompt.

The policy is deleted.

Activating and Deactivating Monitoring Policies

To activate or deactivate a monitoring policy complete these steps.

1. Select **Monitoring Policies > 3G Policies**.
2. Select the **Policy(s)** to be activated or deactivated.
3. Click the **appropriate button (activate/deactivate)** on the tool bar.
4. Click **OK** at the prompt.
5. Click **Apply** to initiate the filtering operation.

About Filtering Monitoring Policies

In large systems there can be a large number of monitoring policies. CCM is equipped with a filtering function, located on the Monitoring Policy tool bar, to filter policies by specific criteria using expressions.

Note: The filtering function is applied for immediate use and cannot be saved.

Filtering Monitoring Policies

Complete the following steps to use the filtering operation.

1. Select **Monitoring Policies > 3G Policies**.
2. Click **Filter Policies** from the tool bar on the polices table.
The IdmPolicies Filter screen opens.
3. Click **Add** .
The screen changes to show the **Expression** line.
Note: The expressions are in alphabetical order beginning with "A." Each expression has select a field, operator and value fields. Multiple expressions can be used to make the search as specific as possible.
Note: When using multiple expressions, choose the appropriate Operator (And, Or, Use Brackets). The Expression field at the bottom of the screen will show all expressions used with their operators.
4. Select the **Field(s)** to be used in the expression.
5. Select the appropriate **Operator** for the expression.
6. Select the appropriate **Value** for the expression.
7. Repeat steps 4-6 in multiple expressions are needed in the filtering operation.
8. Click **Apply** to initiate the filtering operation.

Note: Mobiles and Access Points are created "on the fly" and are not saved.

The results of the filtering operation are listed in the policies table screen.

Appendix

A

Configuration Workflows

Topics:

- *Provisioning Guide for Configuring a DIH System.....224*
- *Setting up DIH Sites.....224*
- *IP Network Data Acquisition for PMF.....225*
- *Configuring for 3G Intelligent Data Monitoring (IDM).....225*
- *Routing PDUs to xDR Builders.....225*

Provisioning Guide for Configuring a DIH System

This outline represents the main steps in configuring an DIH system using CCM.

Note: See the Quick Start Guide for basic procedures on configuring a DIH system.

Creating sites.

- Discover Legacy subsystems and create destinations if traffic needs to be routed to them
- Discover xMF subsystem
- Discover IXP subsystem

Discovering or manually configuring (for PMF) Network Elements

Configure Network Views (see Network View Configuration)

Configure xMF subsystem (see xMF Acquisition)

If configuring an IXP subsystem:

- Create (route) input streams on that IXP subsystem
- Use Dataflow processings (DFP) wizard to create DFPs

OR

- If creating DFPs manually on that IXP subsystem, then create them in the following order:
 - Build
 - Operate
 - Store
- Create the distribution on that IXP subsystem for load balancing or during server maintenance
- Create the sessions on that IXP subsystem
- Manage the subsystem preferences for that IXP subsystem.

Setting up DIH Sites

This procedure must be followed by users who are setting up the DIH system for the first time, adding new DIH servers or adding new applications on an existing server.

Complete these steps (and refer to sections for detailed information), for setting up a DIH system.

1. Create a site.
(See [Creating a Node](#)). Now you can add a host.
2. Add an IXP subsystem (see [Adding an IXP Subsystem](#)).
3. Add a PMF subsystem (see [Adding a PMF Subsystem to a Site](#)).

IP Network Data Acquisition for PMF

Complete these steps to set up PMF monitoring of an IP network.

1. Create, or discover, the **PMF card(s)** that will do the monitoring under the PMF application, if it doesn't already exist (see [Modifying a PMF Subsystem Host](#)).
2. Create one or more **Input streams** (see [Adding a PDU Stream](#)).
Use filtering to discard IP traffic not needed.

Configuring for 3G Intelligent Data Monitoring (IDM)

Complete these steps to configure an DIH system to utilize 3G IDM.

1. Create a **VLAN PDU Filter** from the acquisition perspective.
2. Create a **Traffic Classification**, (both GTP-C and GTP-U) that will be associated with the filter.
3. Create an **IP Dataflow** (acquisition perspective - IP Dataflows) to route the classified GTP PDUs to the PMF subsystem.
 - a) Select **2** for the number of destinations.
Note: If two or more destinations are used, then the same number of DataFlow Processings must be configured at the mediation level for this IP DF.
 - b) Select both GTP options (Algorithms and Destinations).
 - c) Set packet truncation to **0**.
4. Associate the GTP-C traffic classification with the IP Dataflow.
5. **Apply Changes** to the PMF subsystem.
6. From the mediation perspective, create **Dataflow Processings** using the xDR Dataflow Assistant. Builders to consider are: Gn/GP Mobile Activity, IP HTTP TDR, IP MMS TDR.
Note: Gn/GP TDR can be selected if Control Plane xDRs are expected and/or if On-Demand User Plane TDR are expected.
7. **Apply Changes** to the IXP subsystem.
8. Create a **Monitoring Policy**.
9. Create either a **mobile** or **access point** "on demand" record in Customer Care application.

Routing PDUs to xDR Builders

These steps are used to route PDUs from PMF to IXP. When you assign links , linksets , or create IP Streams, the PDUs are collected by the PMF and stored in its local cache. After collection then you need to configure the route for the collected data to the xDR Builders for generating xDRs and KPIs.

Complete these steps to route PDUs to xDR Builders.

1. Ensure the **linksets/links** are assigned.
2. Create **link-based network view(s)** containing the links and/or IP streams from which PDUs are collected.

Note: If you have a large network, it is recommended that you organize the views in a hierarchical manner. Organizing hierarchically enables you to keep track of the routing process.
3. Define any **PDU filters** that you need to classify PDUs as described in (see [About PDU Filters](#)).
4. Create a **PDU data flow** by specifying:
 - a) the type of traffic
 - b) optional filters
5. Select the **data flow** you created and select the **list route** option (see [About PDU Dataflows](#)).
The system displays all the datasources where the PDUs are being collected and cached for that data flow.
6. Assign the **routes** by specifying one or more datasources for every data flow.

Appendix B

xDR Builder Parameters

Topics:

- *List of Parameters for Each xDR Builder.....228*
- *Initial Parameters.....228*
- *IP Transport Screen.....229*

List of Parameters for Each xDR Builder

Each Build xDR session of a dataflow processing has a set of parameters that are set by default but can be customized for your system.

Initial Parameters

Table 52: Initial Step Screen

Field	Description
Generic Parameters	
No PDU timeout (s)	Defines the duration (in seconds) beyond which an alarm is generated if no PDU has been detected.
Max transaction duration (s)	<p>Defines (in seconds) the maximal accepted duration of a transaction (or communication). When a transaction duration exceeds this value, an xDR is generated (with "timer expiry" or "long call" status), even if the transaction is not really terminated.</p> <p>This parameter is displayed only if "reconstitution" is part of the xDR builder name. It is used only if the garbage period is different from 0.</p> <p>The value of the parameter Max transaction duration may be overloaded by an xDR builder specific parameter for a given transaction type (see the xDR builder user's manual).</p>
Garbage period (s)	<p>Defines the period (in seconds) of activation of the long transaction cleaning (i.e. the generation of xDRs with "timer expiry" status for all the transactions which duration exceeds the max transaction duration). This parameter is displayed only if "reconstitution" is part of the xDR builder name.</p>
Monitored	This check box indicates if the builder is being monitored or not. This check box cannot be selected in this screen.
Specific Parameters	
Send xDRs and frames to the xDR consumer	Select this if you want to send the xDRs and frames to the xDR consumer. The default is selected.
Period of flow trace displaying	Defines the period where the flow trace is displayed. The default is 0.
Maximum authorized frame length acceptable (in KB)	Enables you to enter the max. length of frame length in KBs. Default is 4KB.
ATM layer activation	Select this field if you want the ATM layer to be activated. Default is selected.

Field	Description
Defaults button	Click this button to reset the screen to default values.

IP Transport Screen

Table 53: Initial Step Screen

Field	Description
Generic Parameters	
No PDU timeout (s)	Defines the duration (in seconds) beyond which an alarm is generated if no PDU has been detected.
Max transaction duration (s)	<p>Defines (in seconds) the maximal accepted duration of a transaction (or communication). When a transaction duration exceeds this value, an xDR is generated (with "timer expiry" or "long call" status), even if the transaction is not really terminated.</p> <p>This parameter is displayed only if "reconstitution" is part of the xDR builder name. It is used only if the garbage period is different from 0.</p> <p>The value of the parameter Max transaction duration may be overloaded by an xDR builder specific parameter for a given transaction type (see the xDR builder user's manual).</p>
Garbage period (s)	<p>Defines the period (in seconds) of activation of the long transaction cleaning (i.e. the generation of xDRs with "timer expiry" status for all the transactions which duration exceeds the max transaction duration). This parameter is displayed only if "reconstitution" is part of the xDR builder name.</p>
Monitored	This check box indicates if the builder is being monitored or not. This check box cannot be selected in this screen.
Specific Parameters	
Run SCTP path naming function	Select this if you want to run the naming function. Default is selected.
Period of subscribed summary displaying(s)	Numerical field where you can enter an integer to show the period length. Default is 0.
List of servers ports known	<p>Select this parameter is you want to determine the Way and set inactivity garbage. In this format:</p> <p>Protocol Name [Ports] (Max inactivity in seconds)</p>
Run IP reassemble function	Select this if you want to run reassemble function. Default is selected.

Field	Description
Max duration of an IP fragmented inactivity	Numerical field where you can enter an integer to show the duration length. Default is 10.
Set SCTP path naming (8 bytes max)	Enter a path name in the field. For example: Path1=[FF01::10.25.23.15-4569][10.25.6.66-4469]
Max PLDs in SCTP retention	Numerical field where you can enter the number of PLDs in retention. For example: (0->retention function deactivated)
IP fragmented max frame limit	Numerical field where you can enter the number of PLDs in retention. For example: (0->No limit)
Max duration of a TCP connection inactivity(s)	A set of numerical fields to entering the following: Connecting - default 60 Connected - default 60 Closing - default 60 Closed - default 10 Established - default 300 You can also add a new item and its value by clicking the plus icon.
Send xDRs and frames to the xDR consumer	Select this if you want to send the xDRs and frames to the xDR consumer. The default is selected.
Always set the way management function	Select this if you want to set the management function for the builder. The default is not selected.
Period of flow trace displaying	Numerical field where you can enter an integer for the display period.
Max PLDs in SCTP retention	Numerical field where you can enter the number of PLDs in retention. For example: (0->retention function deactivated) Default is 50.
Max duration of an IP fragmented inactivity(s)	Numerical field where you can enter an integer for the maximum period of inactivity. Default is 10.
Defaults button	Click this button to reset the screen to default values.