Oracle® Communications
Performance Intelligence Center

Centralized Configuration Manager Administration Guide

Release 9.0

February 2014

ORACLE®

Oracle Communications Performance Intelligence Center Centralized Configuration Manager Administration Guide, Release 9.0

Table of Contents

List of Figures

List of Tables

Chapter 1: About This Help Text

Overview

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

A typical PIC system consists of many 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. A large PIC system consists of many such sites with each site containing multiple servers performing the functions of data collection and storage, xDR generation and storage as well as KPI generation and storage. A site may also contain a data storage unit storing terabytes of data.

PIC web-based applications, such as CCM, are hosted by a cluster of application servers located at the customer's Network Operations Center (NOC). It is quite common for a PIC system to consist of over 100 computer servers located across a wide geographical area. 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 Performance Intelligence Center

The Performance Intelligence Center (PIC) is a monitoring and data gathering system that provides network performance, service quality and customer experience - across various networks, technologies, protocols, etc. Beyond monitoring performance and gathering data, the solution also provides analytics, actionable intelligence and potentially an intelligent feedback mechanism. It allows Service Providers to simultaneously look across the Data Link, Network, Transport and Application layer traffic to better correlate and identify the impact of network problems on revenue generating applications and services.

PIC functionality is based on the following general flow. The Integrated Message Feeder (IMF) is used to capture SS7 and SigTran traffic. The Probed Message Feeder (PMF) is used to capture both SS7 and IP traffic. Both products forward Probe Data Units (PDUs) to the Integrated xDR Platform (IXP). The IXP stores this traffic data and correlates the data into detailed records (CDRs, IPDRs, TDRs, etc.).

The IXP then stores the data on the system for future analysis. The Network Software Platform (NSP) provides applications that mine the detailed records to provide value-added services such as network performance analysis, call tracing and reporting.

PIC centralized configuration tasks fall into one of two categories:

- Data Acquisition and Processing – the configuration of the probes, routing of PDUs to the xDR builder setup, KPI generation, data feeds, etc.
- PIC System Administration - the configuration of monitoring sites, configuring PIC servers, setting up permissions, etc.

Note: For more information see Centralized Configuration Manager Administration Guide.

This is a graphic overview of the PIC system.

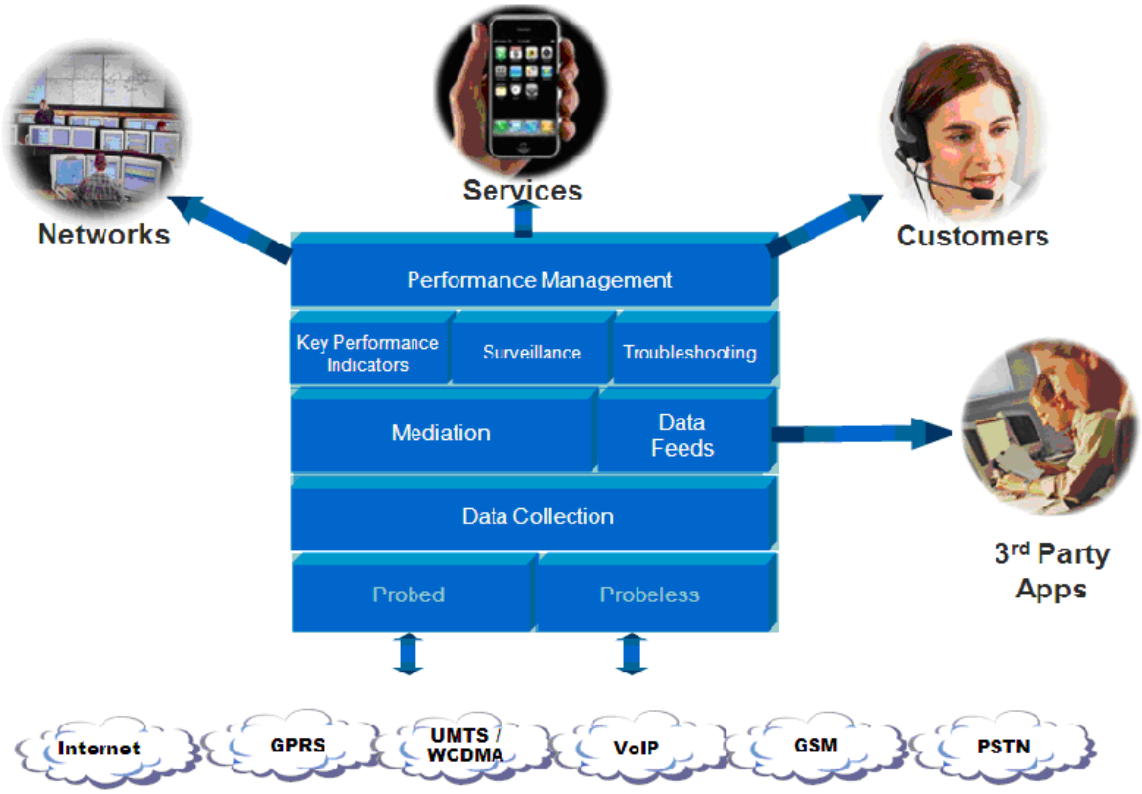


FIGURE 1: PIC OVERVIEW

User Preferences

All applications that query 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.

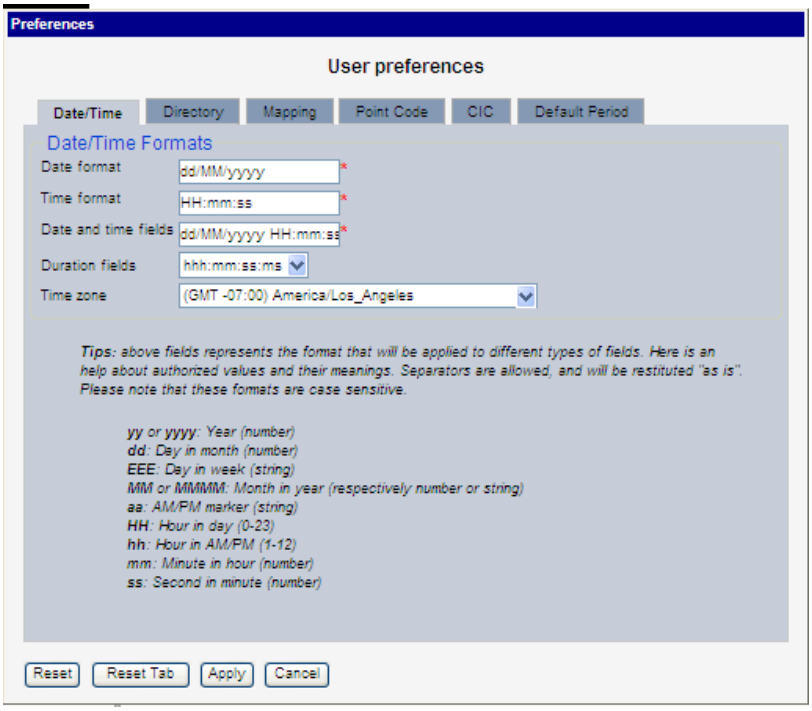


Figure 2: Date/Time Tab Screen

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.

TABLE 1: TIME TAB SCREEN

Directory tab

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

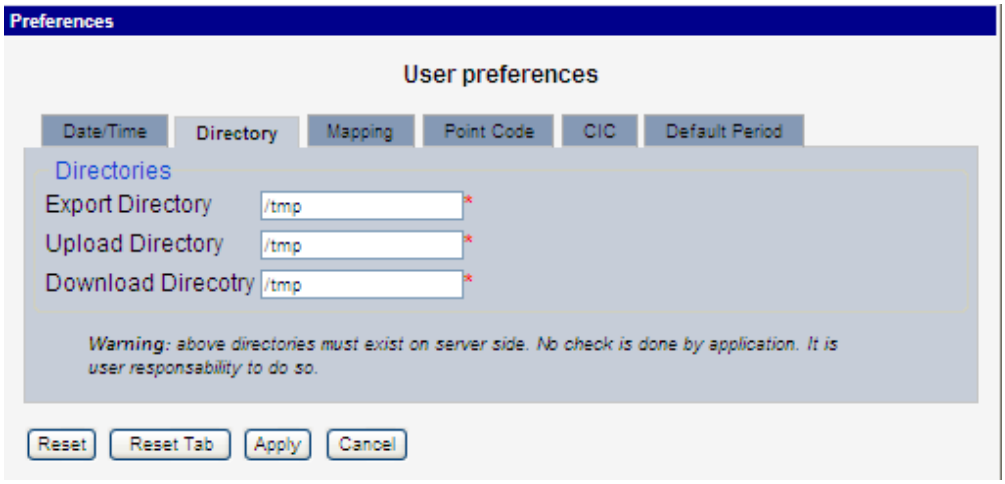


Figure 3: Directory Tab Screen

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.

TABLE 2: DIRECTORY TAB FIELD DESCRIPTION

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.

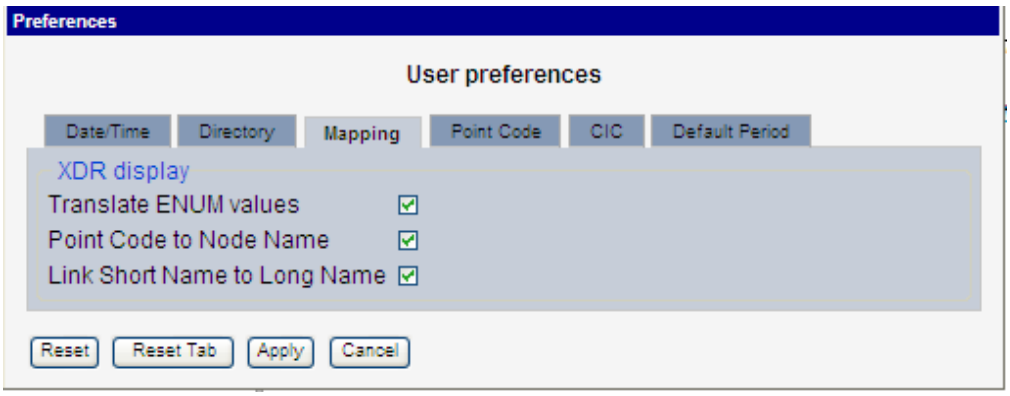


Figure 4: Mapping Tab Screen

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.

TABLE 3: MAPPING TAB

Point Code tab

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

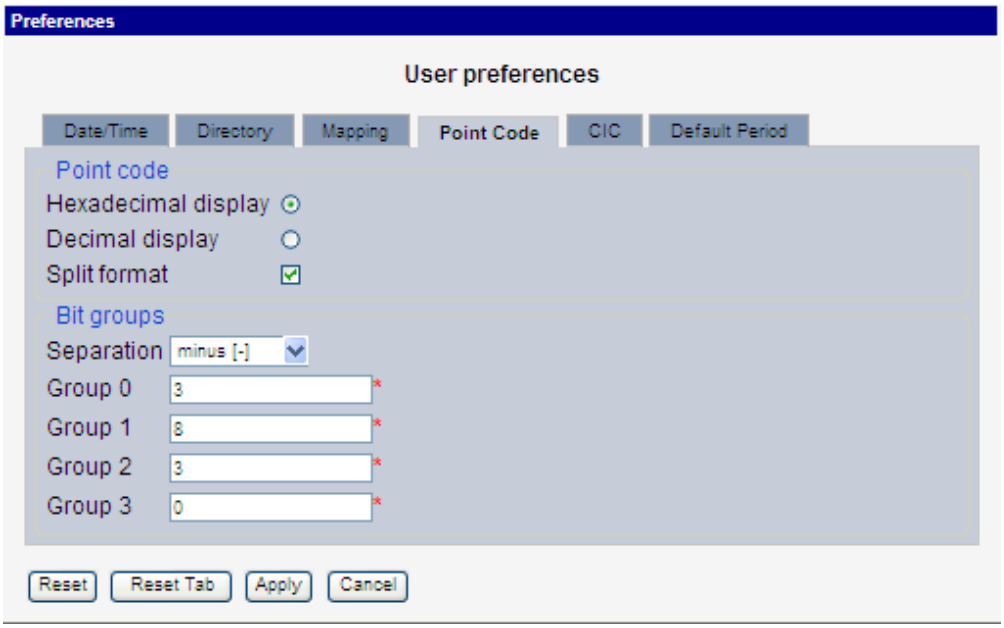


Figure 5: Point Code Tab Screen

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.

TABLE 4: POINT CODE TAB

CIC tab

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

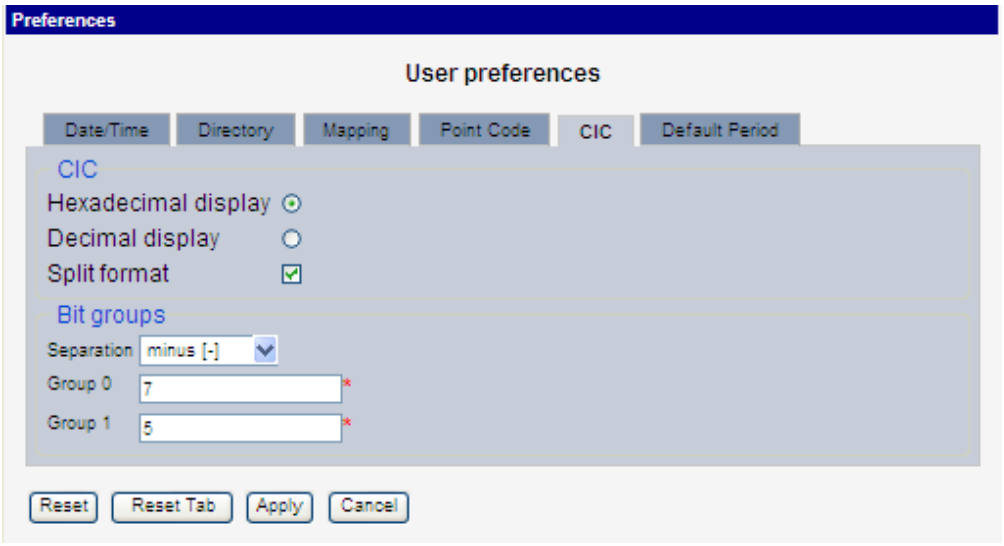


Figure 6: Formatting Rules (CIC) Screen

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.
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.

TABLE 5: CIC TAB FIELD DESCRIPTIONS

Default Period tab

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

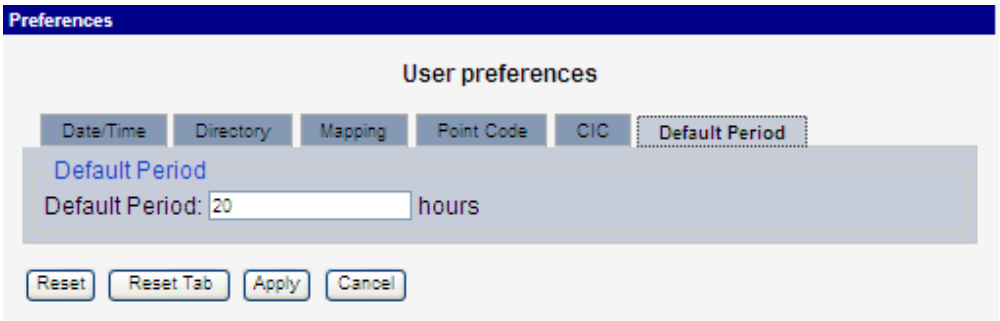


Figure 7: Default Period Tab Screen (ProTrace only)

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.

TABLE 6: DEFAULT PERIOD TAB FIELD DESCRIPTIONS

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:

8:30 a.m. through 6:30 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.

PIC Documentation Library

PIC 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 PIC documentation library of user guides:

- Security User Guide
- Alarms User Guide
- ProAlarm Viewer User Guide
- ProAlarm Configuration User Guide
- Centralized Configuration Manager Administration Guide
- Customer Care User Guide
- Alarm Forwarding Administration Guide
- Diagnostic Utility Administration Guide
- ProTraq User Guide
- ProPerf User Guide
- ProPerf Configuration User Guide
- System Alarms User Guide
- ProTrace User Guide
- Data Feed Export User Guide
- Audit Viewer Administration Guide
- ProDiag User Guide
- SigTran ProDiag User Guide
- Report Server Platform User Guide
- Reference Data User Guide
- Exported Files User Guide
- Scheduler User Guide
- Quick Start User Guide

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.

Chapter 2: Key Concepts

About PIC

The Performance Intelligence Center, (PIC), functionality is based on the following general flow. The Integrated Message Feeder (IMF) is used to capture SS7 and SigTran traffic. The Probed Message Feeder (PMF) is used to capture both SS7 and IP traffic. Both products forward the PDUs to the Integrated xDR Platform (IXP). The IXP stores this traffic data and correlates the data into detailed records (CDRs, IPDRs, TDRs, etc.). The IXP then stores the data on the system for future analysis. The Network Software Platform (NSP) provides applications that mine the detailed records to provide value-added services such as network performance analysis, call tracing and reporting.

PIC centralized configuration tasks fall into one of two categories:

- Data Acquisition and Processing – the configuration of the probes, routing of PDUs to the xDR builder setup, KPI generation, data feeds, etc.
- PIC System Administration - the configuration of monitoring sites, configuring PIC servers, setting up permissions, etc.

CCM Overview

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

About Data Acquisition and Processing

Data acquisition and processing refers to collecting PDUs from monitored networks, generating xDRs and KPIs from the collected PDUs and storing/forwarding the data for use by applications.

IMF Data Acquisition

IMF data acquisition comprises three general steps. They are:

1. Eagle timestamps and delivers MSUs to an IMF
2. IMF processes the MSUs and filters it for delivery to an IXP
3. The IXP processes the MSUs for storage, xDR correlation and KPIs

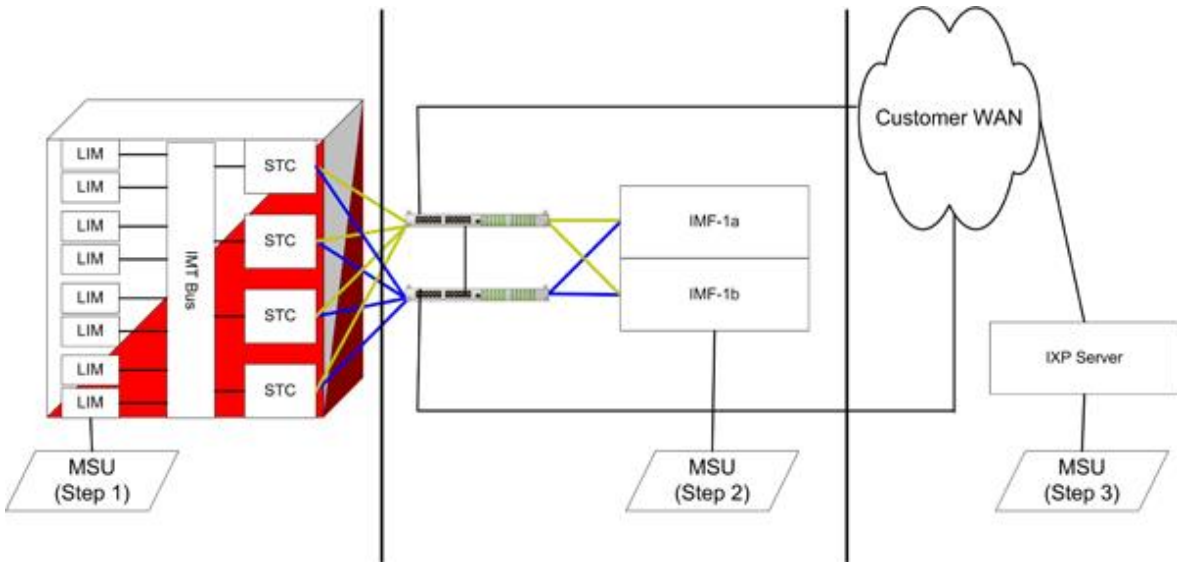


Figure 8: Imf Acquisition Sequence

PMF E1/T1 Data Acquisition

PMF E1/T1 data acquisition comprises three general steps. They are:

1. PMF acquires MSUs from SS7 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

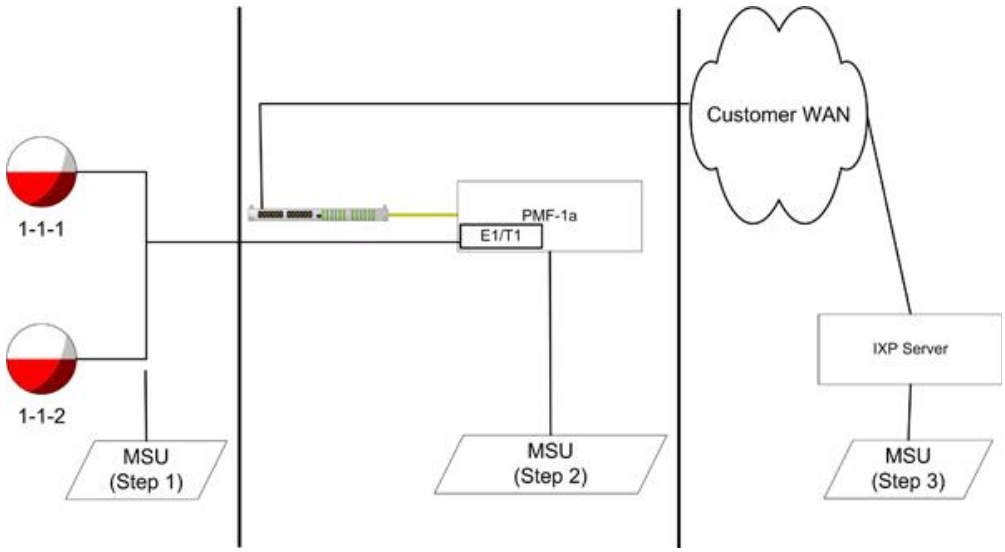


Figure 9: Pmf E1/T1 Data Acquisition Sequence

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

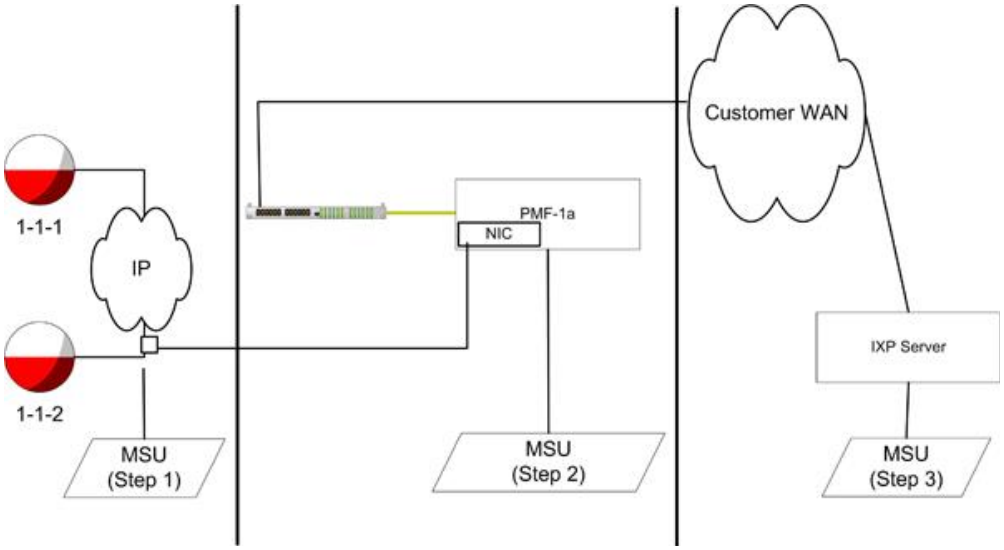


Figure 10: Pmf IP Data Acquisition Sequence

PIC NTP Sources for Accurate Time Stamping

The figure shows the PIC NTP timestamping process and an example of a valid NTP configuration. In this example, an NTP server provided by the customer is referenced as the NTP source for the NSP server. The IXP servers use the NSP server as their NTP source. The IMF servers also use the NSP server as their NTP source, and then also the IMF-1a and IMF-1b servers broadcast NTP to the Eagle for it to use to timestamp MSUs. The PMF servers, not shown, also use the NSP server as their NTP source, and then timestamps MSU's internally.

Note: Some MSUs that need to be correlated into an xDR happen with 5 milliseconds between them, therefore the NTP server that is provided by the customer must meet the specification of a stratum 3 (+/- 4.6 microseconds) to insure accurate correlation of xDRs.

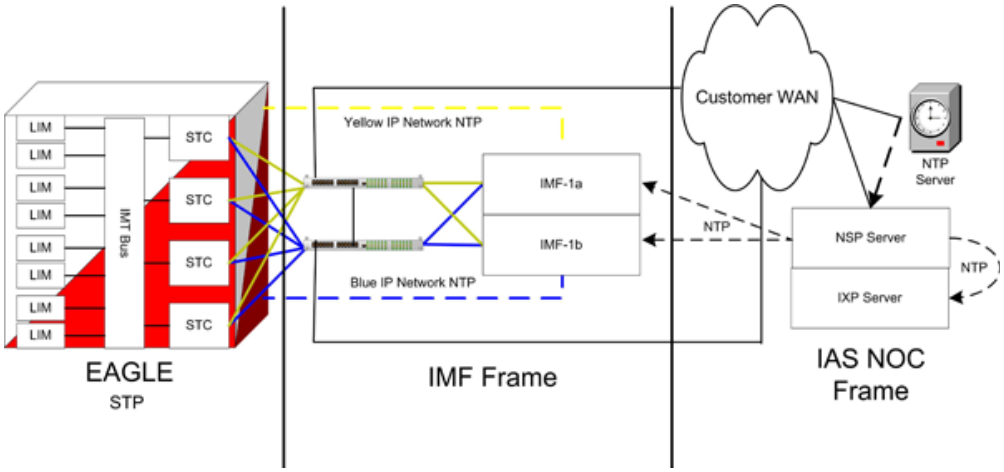


Figure 11: PIC NTP Example

Overall PIC Configuration

This figure illustrates the three major data acquisition processes described above and shows the PIC components at each level of functionality that have access to the acquired and correlated data.

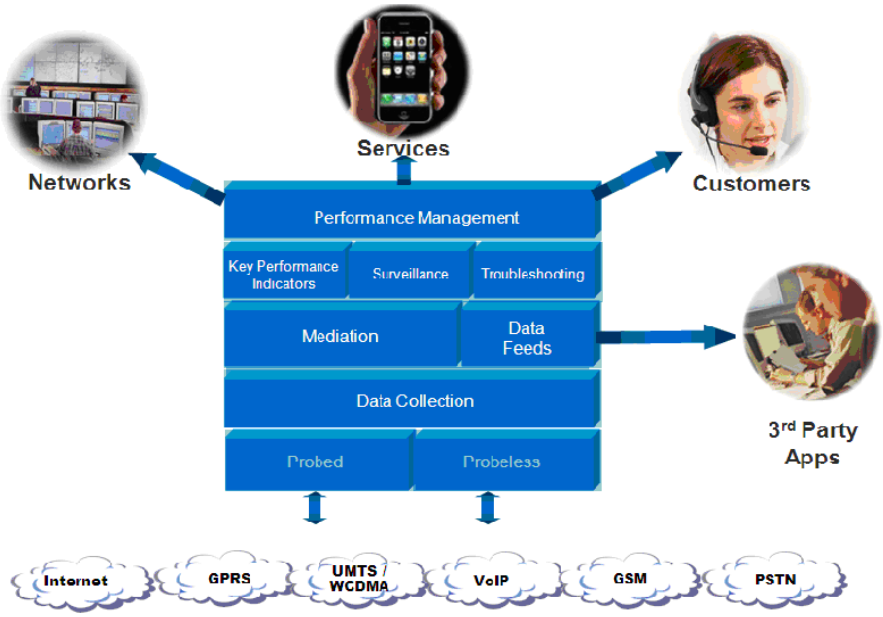


Figure 12: PIC System

Configuration is required at each level of the system, up to and including the storage of the data. The configuration concepts related to the various components shown in the figure.

These concepts are:

- Monitored Network Elements
- PDU Collection
- PDU Filtering and Routing
  - Input Stream
  - Dataflow
  - Destination (Datasource)
  - Routing
  - RID Groups
- Q.752 Processing
- xDR Generation
  - Sessions and Dictionaries
- KPI Generation
- Network Views
- Report configuration

Monitored Network Elements

The term, Network Elements, refers to customer network SS7, GPRS and IP elements. These elements are divided into:

- Node Elements - elements, linksets and links that are contained in SS7, GPRS and IP nodes.
- Non-node Elements - SS7, GPRS and IP elements. Non-node elements are divided into three main categories
  - SS7 elements:
    - Linksets

    - Associations
    - Links
    - Signaling Points (SPs)
- GPRS elements:
    - Gb links
    - Signaling Points (SPs)
- IP elements:
    - Signaling Points (SPs)
    - IP Cards
    - Application Servers (AS)
    - Associations
    - Application Server Process (ASP)

Examples of network elements include: SS7 service switching points (SSP), SS7 linksets, GPRS service switching gateway node (SGSN), Voice over IP (VoIP), etc. The PIC system monitors some of these elements and collects the messages transported between the elements. The messages are referred to as PDUs.

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

In CCM, network elements are added to the centralized database in one of the following two ways:

- Through discovery from associated IMF data collectors - you can select a specific data collector and issue the command to discover or synchronize network elements. The data collector reports to CCM all of the network elements it discovers and CCM adds them to the centralized database.
- Through manual creation - for configuring PMF you can define each individual network element using the user interface.

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

Data collectors monitor and collect PDUs exchanged between nodes. The data collectors include the IMF and PMF.

PDU Collection on SS7 Networks (IMF)

In order for the PDUs to be collected by IMF for SS7 networks, you must complete these actions in the following order:

1. Create monitoring group(s) which are assigned automatically to an IMF server.
2. Assign linksets, (network elements), to the monitoring group(s)

   Note: In the case of utilizing SigTran Fast Copy you assign an association to a monitoring group.
3. Create PDU dataflows
4. Route the assigned PDU dataflows to input streams on IXP.

PDU Collection on SS7 Networks (PMF) and GPRS

In order for the PDUs to be collected by PMF for SS7 networks, following steps must be completed:

1. Select an E1/T1 card

   Note: For PDUs from SS7-GPRS networks, you can select a SPAN (E1/T1) card on a specific PMF server.
2. Configure the required ports on the E1/T1 card
3. Create an SS7 or Gb link for each E1/T1 card port

4. Assign links to ports on the E1/T1 card
5. Create PDU dataflows
6. Route the assigned PDU dataflows to input streams on IXP

PDU Collection on IP Networks (IMF or PMF)

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. For PMF, assign the link network view to the IP dataflow
   For IMF, assign an association 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. (See CCM step 2 in IMF Acquisition Sequence, PMF E1/T1 Data Acquisition Sequence, PMF IP Data Acquisition Sequence.)
- A PDU can be routed to multiple xDR builders for building different types of xDR records. (See CCM step 2 in in IMF Acquisition Sequence, PMF E1/T1 Data Acquisition Sequence, 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 CCM in IMF Acquisition Sequence, PMF E1/T1 Data Acquisition Sequence, 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.
- An SS7 xDR builder needs to "know" when to handle multi-legged PDUs it receives from a data collector. Duplicate PDUs can result when multiple points in the customer network are being monitored by the same data collector and the same PDU passes through these points. Reference ID groups (see CCM topic About RID Groups) provide a mechanism for handling duplicate PDUs. If this area is not properly planned and configured, then xDR correlation problems can occur.
- 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 IMF/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. One limitation of input filters, like input streams, is that Q.752 or similar processing cannot be done on discarded traffic since the Q.752 processing is done on cached PDUs.

About Data Transport Service (DTS)

Routing data from xMF (IMF/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 the IMF or 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 RID Groups

An RID group enables differentiation of multi-legged PDUs. For example, an SS7 xDR builder needs to know how to differentiate multi-legged PDUs it receives so that it does not discard the original and multi-legged PDUs as erroneous during error checking, resulting in loss of xDR records. A multi-legged PDU occurs when two points (linksets) in the customer's network are being monitored and the same PDU passes through both points (it is collected twice) and the PDU traffic from both linksets is routed to the same builder. To handle this situation, the SS7 linksets must be grouped carefully into RID groups, (see About Resource ID Groups (RID)), and the xDR builder informed of the associated RID group for each PDU so that a multi-legged PDU that has already been reported from a different RID group can be processed separately by the builder. This prevents the first PDU from being discarded as well, and the xDR record for it can be generated and stored.

About Auto RID

Auto RID is used for IMFs where links are monitored at the Eagle side. This feature is also used where "edge" devices, devices that do origin-based routing, are involved. In addition, Auto RID can be used for network elements (ssp/scp) with one point code. Auto RID Reverse is used when probes are linked near the network elements (scp/ssp).

About Q752 Processing

PIC supports a subset of the ITU Q.752 standards. Q.752 defines a standard set of measurements and alarms for monitoring the health of SS7 networks. Both IMF and PMF perform the low-level processing required for Q.752. That is, IMF and PMF apply processing on received PDUs to record key performance indicators (see KPI Generation) and generate alarms if thresholds are exceeded. The KPI counters are sent over special Dataflows to xDR builders for consolidation and further processing. One of the tasks of a CCM user is to configure the Q.752 Dataflows as well as the Q.752 alarms thresholds (see About Q.752 Counters).

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.

KPI Generation

The PIC system enables you to configure KPIs using the NSP application ProTraq Configuration. ProTraq defines the rules for generating KPIs from the xDR records that have been configured.

KPI data is stored in KPI sessions in a dictionary format like xDR records. Similarly, KPI sessions are discovered by CCM. Once discovered, the sessions can be accessed by NSP applications like Data Feed Export or ProPerf.

About xDR Data Feeds

PIC 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 a PIC 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 PIC system to select a dataset. Applications like ProTrace and ProDiag use network views.

The types of elements that can be grouped together into a network view include PDU sources such as SS7 linksets, Gb links, 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 (SS7, Gb, 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 PIC 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
- Hosts

About Sites

Sites represent logical locations where an PIC application is located. A PIC application either runs on a single server or it may be distributed over a group of servers (referred to as a subsystem). Using CCM, you define sites.

When you create a site, follow this guideline:

- There can be, at most, one XMF subsystem (IMF or PMF) for a given site. For example, you can have one IMF or PMF subsystem along with multiple IXP subsystems. For this reason, a physical location where there are multiple xMF subsystems needs to be represented in CCM by multiple sites.

  Note: An IMF subsystem can monitor only one Eagle STP.

About Hosts

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

About Subsystems

Some PIC 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 PIC 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:

- XMF (IMF or 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.

About Report Configuration

CCM provides a means of configuring a configuration report using MS Excel spreadsheet. When you have run the report, each page is dedicated to a specific aspect of the system (Network Views, Network Elements, Role Profils, Acquisition, etc). The configuration report is created from the Home Page.

Chapter 3: Using CCM

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.

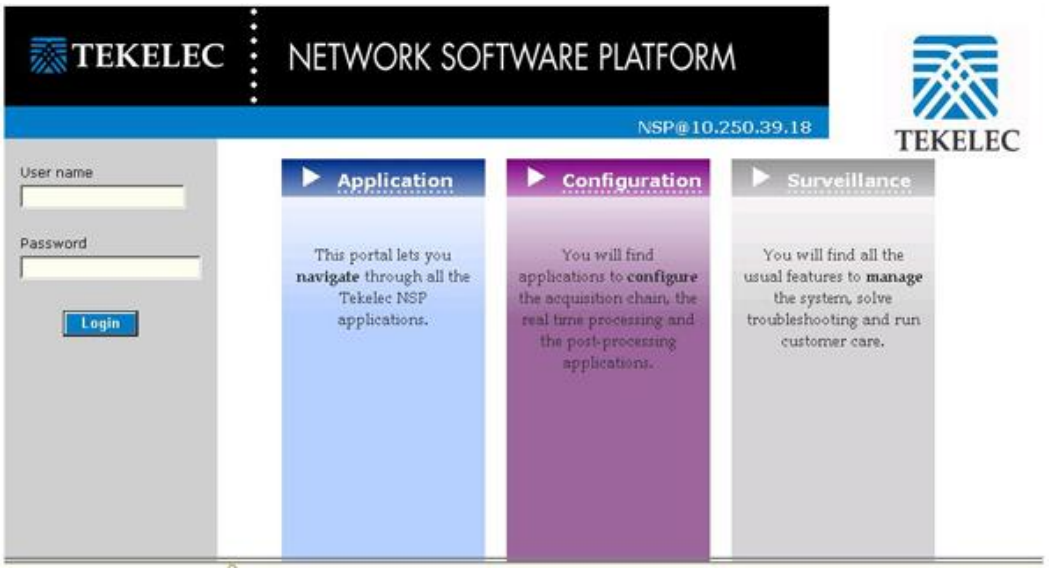


Figure 13: NSP Portal Screen

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

The CCM Home screen opens.

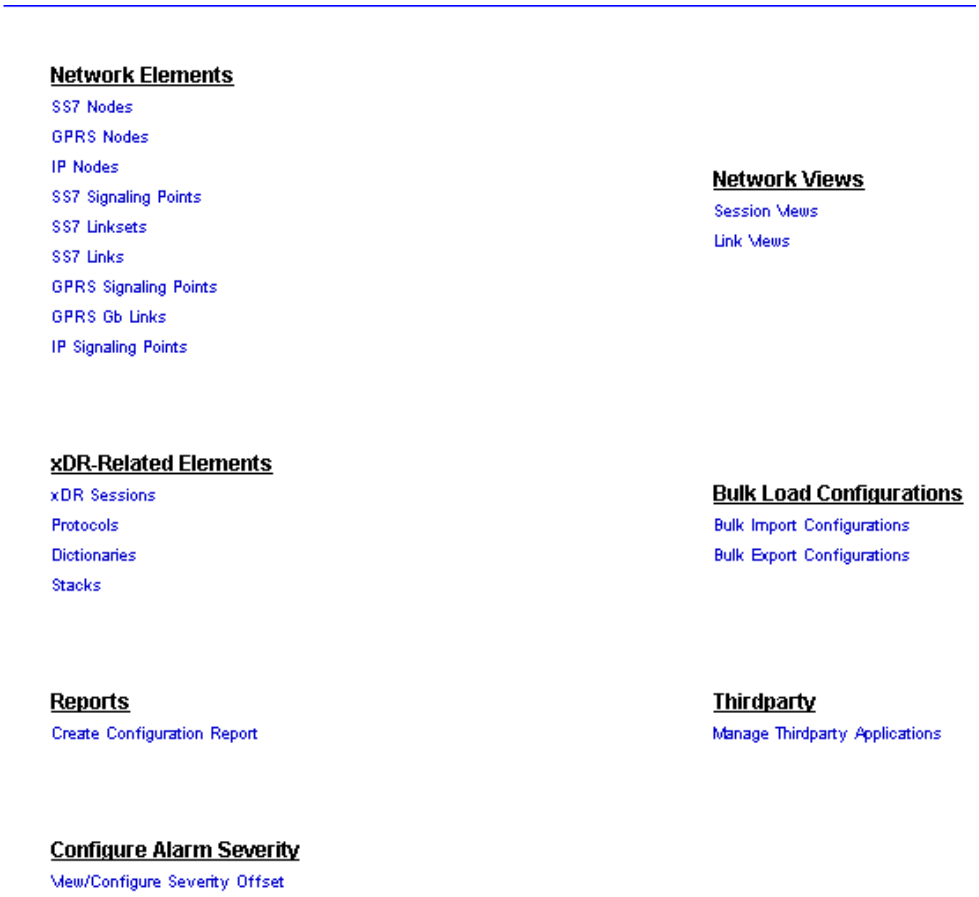


Figure 14: CCM Home Screen

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 navigate through the data (not shown).

   The six perspectives are:

   - Equipment Registry
   - Network Elements
   - Network Views
   - Acquisition
   - Mediation
   - Reference Data

b. Screen body - on the Home screen provides links for *Network Elements, Network Views* and *xDR-Related Elements, Bulk Load Configurations, Reports, Thirdparty applications* and *Alarm Severity Configuration*.

On other screens it allows you to create, modify, delete, or list configured data. Each of these objects is discussed as specific subjects.

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 4: Home Screen Operations

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 are also Bulk Load and Reports functionalities. 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 CCM Home screen 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 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.

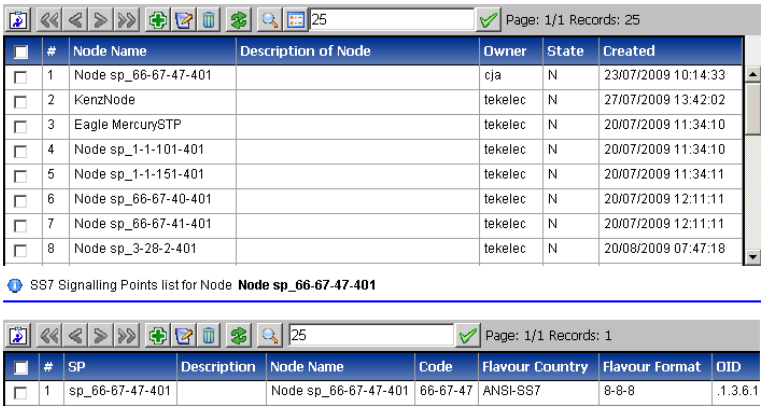


Figure 15: SS7 Node(s) List Screen

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.

Signaling Points List Screen

Each type of signaling point is located under the network element category (SS7, GPRS or IP). The signaling points link provides a list of ALL the signaling points configured in your system. Clicking the link opens the Signaling Point(s) List screen (SS7 Signaling Points screen shown).

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

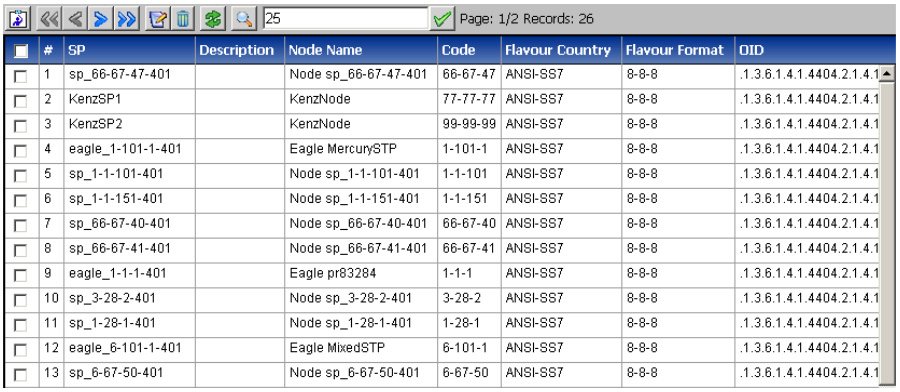


Figure 16: SS7 Signaling Points List Screen

SS7 Linksets List Screen

The linksets link provides a list of all the SS7 linksets configured in your system. Clicking on SS7 Linksets in the Home page opens the SS7LinksetList screen shown below that has two tables. Selecting a linkset in the top (linkset) table shows the links that belong to that set. From this screen you can modify, delete, search, override custom name, assign RID groups and see details of a linkset. You can also: add, modify, delete, search, override custom name and see details of a linkset's associated links.

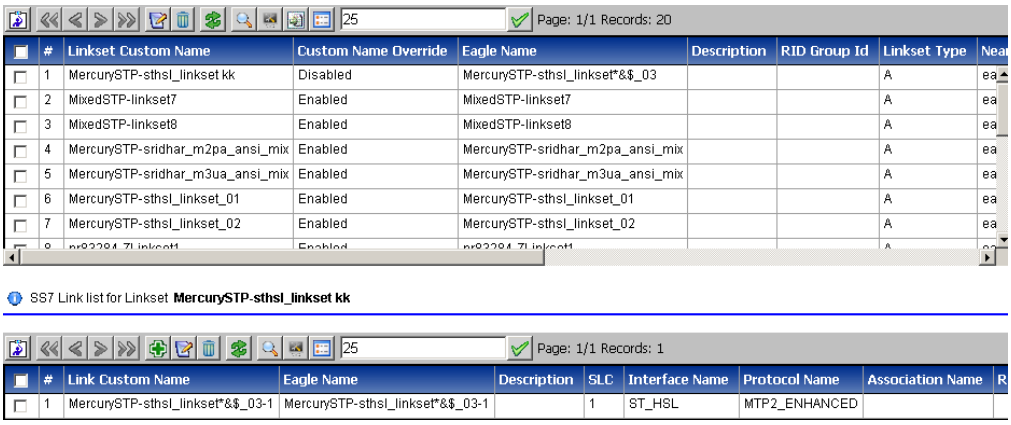


Figure 17: Selected SS7 Linkset List Showing Associated Links

SS7 Links List Screen

The links link provides a list of all the SS7 links configured in your system. Clicking the link opens the Link List screen. From this screen you can: modify, delete, search, set the custom name override or see the details of a particular link.

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

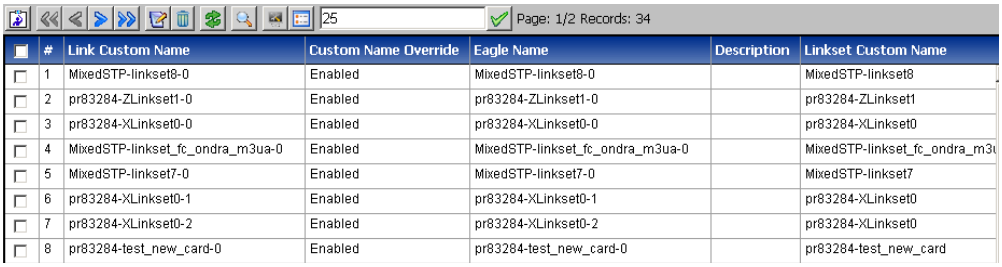


Figure 18: SS7 Links List Screen

GPRS Signaling Point List Screen

The GPRS signaling point list screen provides a list of GPRS linksets configured in your system. The GPRS linkset screen is shown below.

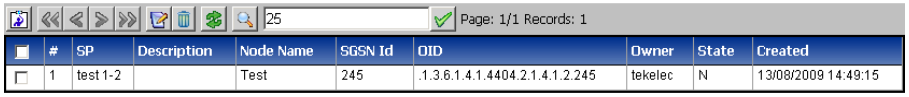


Figure 19: Gprs Signaling Point List Screen

GPRS Gb Link List Screen

The GPRS Gb links list screen provides a list of the GPRS Gb links configured in your system. The GPRS Gb link list screen is shown below.

Figure 20: Gprs Gb Link List Screen

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.

Figure 21: 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.

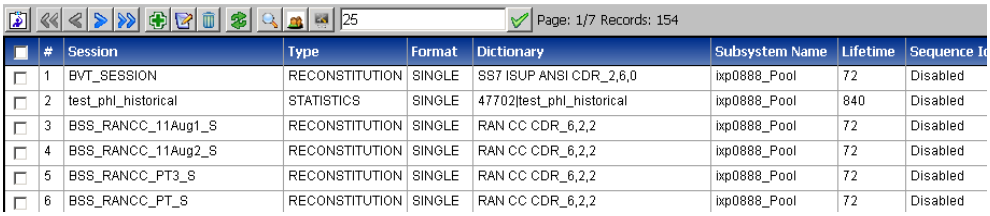


Figure 22: Network Sessions List Screen

Link Views

The Link Views link provides a list of all the link network views configured in your system. Clicking the link opens the Link Network View(s) List screen.

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

Figure 23: Link Network View(s) List

xDR-Related Elements

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

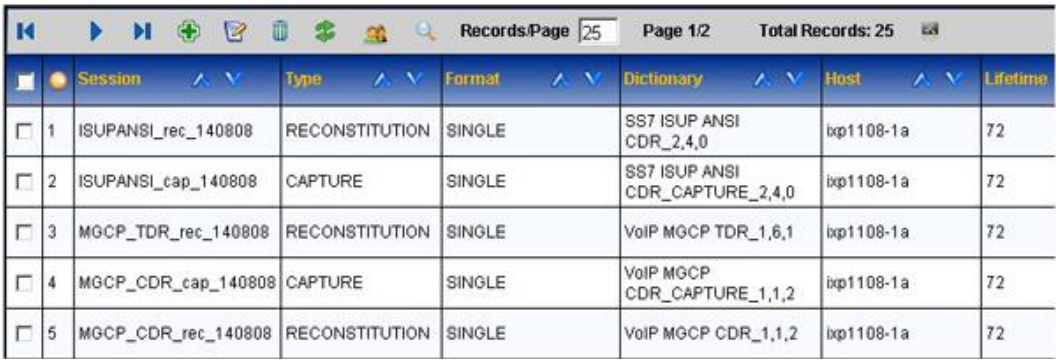
- xDR Sessions
- Protocols
- Dictionaries
- Stacks
- PDU Hiding

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.



Records/Page 25 Page 1/2 Total Records: 25

	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 24: 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 protocols list 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 25: 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.

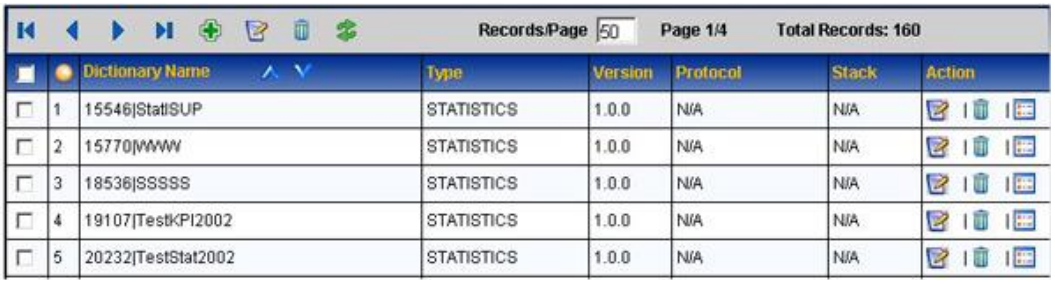


Figure 26: Dictionaries Present Screen

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.

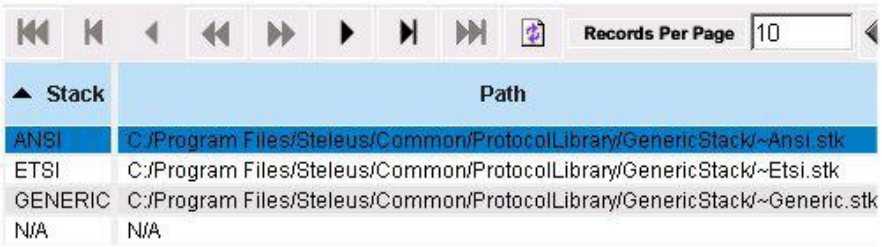


Figure 27: Stacks List Screen

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 both IMF and PMF configurations offline without requiring xMF to be up and running. For IMF configurations this process includes the capability to

import sites, hosts, applications, signaling points (both SS7 and Gb), linksets, links (both SS7 and Gb), SS7 filters, IP filters, probe assignment configurations and monitoring groups.

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
- SS7 combination filters
- GT filters
- DLCI filters
- IP Combination Filters
- IP filters
- Port filters
- VLAN filters
- PC filters
- Raw filters
- Sites
- Hosts
- Nodes
- SS7 Signaling Points
- Linksets
- SS7 Links
- Gb Signaling Points
- Monitoring Groups
- PMF cards
- PMF ports
- PMF Port Assignments

These file types can be uploaded in any order.

Bulk Loading Process

The separate files should be prepared for the file formats specified in the next sections. If some configuration already exists in the system, (for example, Sites added from the CCM Add Site screen), then the Bulk load of the corresponding *.csv* file can be skipped. While preparing the *.csv* files for initial import, the Object ID fields should be set to NA value (for example, the SiteID field in Sites.csv or the HostID fields in Hosts.csv are set to NA). Finally, during the Bulk Load Process, files can be uploaded in any order but all dependent files should be imported together (for example, Hosts.csv and Sites.csv should be uploaded together).

IMF Element Configurations

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

Note: All these csv files must exist and must be imported so that the import process is error free.

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

2	Site ID	Number			No	
3	Name	String			Yes	30
4	Description	String		Yes	Yes	255

TABLE 7: SITE CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		2		No	
2	Host ID	String			No	
3	Host Name	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	IMF-NG PMF-NG		No	
11	Site Name-ID	String			No	30

TABLE 8: HOST CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		4		No	
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			No	30
8	Node Name - ID	String			No	30
9	Site Name - ID	String			No	30

TABLE 9: SS7 SIGNALING POINT 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
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 10: LINKSET CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load		8			
2	Association ID	Number			No	
3	Association - Name	String			Yes	80
4	EagleID	Number			Yes	
5	SiteName-ID	String			No	30

TABLE 11: ASSOCIATIONS CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		6			
2	SS7LinkID	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			No	
9	Eagle Port Number	Number			No	
10	Linkset Name - ID	String			No	30
11	SiteName - ID	String			No	30
12	EagleID	Number		Yes	Yes	

TABLE 12: SS7 LINK CONFIGURATIONS

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load		7		No	
2	Monitoring GroupID					
3	Name	String			No	30
4	Description	String		Yes	Yes	255
5	Site Name-ID				No	30
6	Linkset Names-IDs		"comma separated Linkset Names/IDs under quotes"	Yes	Yes	
7	EagleID		"comma separated EagleIDs for associations under quotes"	Yes	Yes	

TABLE 13: MONITORING GROUP CONFIGURATION

Sample of an IMF Configuration CSV File

Here is an example of the *.csv* files that comprise an IMF configuration.

Note: ID is an NSP identifier for mobile entries. It is used in the update/delete process for existing entries through import feature. It can be left blank for new entries.

Site csv file

```
#Sites.csv,,,
#BulkLoadType,SiteID,SiteName,Description
1,NA,IMF_Delhi,Delhi Site
1,NA,IMF_Chennai,Chennai site
1,NA,IMF_Mumbai,Mumbai site
1,NA,IMF_Kolkata,Kolkatta site
```

Host csv file

```
#Hosts.csv,,,,,,,,,
#BulkLoadType,HostID,HostName,Description,Frame,Position,IP,AppName,Descrip
tion,AppType,Site
2,NA,IMF-DE-1A,,1,1,172.31.254.5,IMF-DE-1A,IMF NG,IMF NG,IMF_Delhi
2,NA,IMF-DE-1B,test1,1,2,172.31.254.6,IMF-DE-1B,IMF NG,IMF NG,IMF_Delhi
2,NA,IMF-DE-1C,,1,3,172.31.254.7,IMF-DE-1C,IMF NG,IMF NG,IMF_Delhi
2,NA,IMF-DE-1F,,1,6,172.31.254.10,IMF-DE-1F,IMF NG,IMF NG,IMF_Delhi
```

SS7SP csv file

```
#SS7SPs.csv,,,,,,,
#BulkLoadType,SPID,SPName,Description,Flavor,PointCode,CLLI,NodeID,SiteID
4,NA,eagle_4-14-4-402,,402,8308,mumstp,,IMF_Mumbai
4,NA,eagle_4-14-5-402,,402,8309,kolstp,,IMF_Kolkata
4,NA,eagle_4-7-4-402,,402,8252,chnstp01,,IMF_Chennai
4,NA,eagle_8502-aa-405,,405,8502,kolstp,,IMF_Kolkata
4,NA,eagle_s-111-aa-405,,405,1073741935,delstp01,,IMF_Delhi
4,NA,eagle_s-222-aa-405,,405,1073742046,mumstp,,IMF_Mumbai
4,NA,eagle_s-444-aa-405,,405,1073742268,chnstp01,,IMF_Chennai
4,NA,sp_1-1-1-402,,402,2057,,,IMF_Chennai
4,NA,sp_1-1-1-402,,402,2057,,,IMF_Delhi
```

Linksets csv file

```
#Linksets.csv,,,,,,,
#BulkLoadType,LinkSetID,Name,Description,Type,NEPC,FEPC,ResourceID,Site
5,NA,delstp01-212,Delhi,A,sp_6921-aa-405,sp_9589-aa-405,54,IMF_Delhi
5,NA,delstp01-213,,A,sp_4-7-3-402,sp_2-174-7-402,1,IMF_Delhi
5,NA,delstp01-214,,A,sp_4-7-3-402,sp_4-40-0-402,1,IMF_Delhi
5,NA,delstp01-215,,A,sp_6921-aa-405,sp_9493-aa-405,22,IMF_Delhi
5,NA,delstp01-216,,A,sp_4-7-3-402,sp_2-72-3-402,1,IMF_Delhi
5,NA,delstp01-217,,A,sp_6921-aa-405,sp_5547-aa-405,72,IMF_Delhi
5,NA,delstp01-218,,A,sp_6921-aa-405,sp_9961-aa-405,63,IMF_Delhi
```

Associations csv file

```
8,NA,Association1,1,IMF_Mumbai
8,NA,Associaton2,2,IMF_Mumbai
```

SS7 Links csv file

```
#SS7Links.csv,,,,,,,,,,
#BulkLoadType,LinkID,Name,Description,SLC,Interface,TransportProtocol,Eagle
Card,EaglePort,LinkSet,Site,
6,NA,mumstp-1211-30,,14,8,0,233413,239768,mumstp-9,IMF_Mumbai,1
6,NA,mumstp-1211-31,,15,8,0,233413,239772,mumstp-9,IMF_Mumbai,1
6,NA,mumstp-1211-24,,1,8,0,233413,233436,mumstp-9,IMF_Mumbai,1
6,NA,mumstp-1211-25,,0,8,0,233413,233438,mumstp-9,IMF_Mumbai,2
6,NA,mumstp-1211-26,,3,8,0,233413,233440,mumstp-9,IMF_Mumbai,2
```

Monitoring Group csv file

```
#MonitoringGroups.csv,,,,,,
#BulkLoadType,MGID,Name,Description,Site,Linksets,EagleIdsForAssociations
7,NA,MG1,,DUO,,6
```

Importing IMF Configurations

Pre-conditions for importing IMF 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 IMF configuration.

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

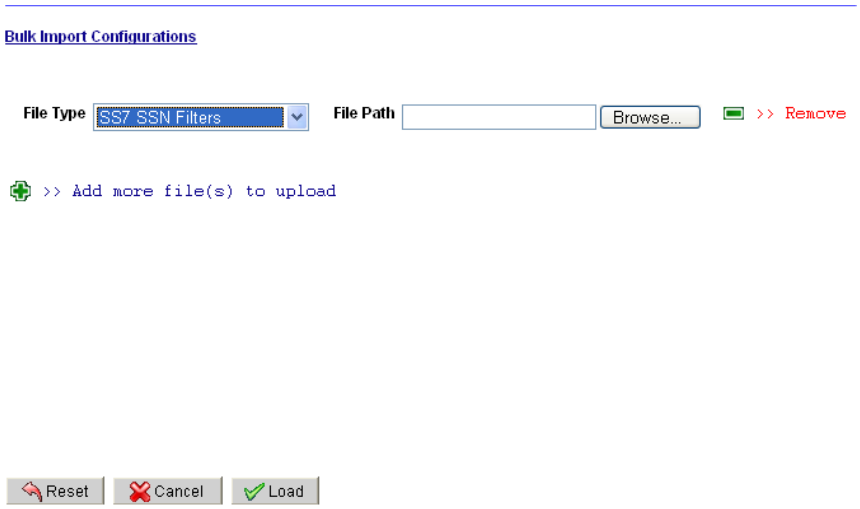


Figure 28: Bulk Load Import Screen

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. SS7SP.csv
   c. Linksets.csv
   d. Associations.csv
   e. SS7 Links.csv
   f. MonitoringGroups.csv

7. Click **Load**.
   The files are uploaded to the system.

Once you have imported the files, you must **Synchronize** the Subsystem.

PMF Element Configurations

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

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

TABLE 14: SITE CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load		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	String	IMF-NG PMF-NG		No	
11	Site Name-ID	String			No	30

TABLE 15: HOST CONFIGURATION

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

TABLE 16: NODE CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load Type		4		No	
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 17: SS7 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 18: GB SIGNALING POINT 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
5	Type	Char	A,B,C,D,E		Yes	
6	SP1 (Name/ID)	String			No	30

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
7	SP2 (Name/ID)	String			No	30
8	Resource ID Group				Yes	
9	Site Name/ID				No	30

TABLE 19: LINKSET CONFIGUATION

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 20: SS7 LINK CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load		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 21: GB LINK CONFIGURATIONS

ID	Field	Data Type	Value	Optional	Can Be Updated	Max Length
1	Bulk Load		11		No	
2	CardID	Number			No	
3	Slot Number	Number			No	
4	Hardware Type	Number	0-SPAN (E1/T1)		No	
5	Software Type	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 22: PMF CARD CONFIGURATION

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

ID	Field	Data Type	Possible Values	Optional	Can Be Updated	Max Length
1	Bulk Load		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	

ID	Field	Data Type	Possible Values	Optional	Can Be Updated	Max Length
7	Name/ID	String		No	Yes	30

TABLE 24: PMF PORT ASSIGNMENT CONFIGURATION

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,IMF-Quatro
1,NA,Demo1
1,NA,ixp2627
1,NA,IMF-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,Descrip
tion,AppType,Site
2,NA,IMF-DE-1A,,1,1,172.31.254.5,IMF-DE-1A,IMF NG,IMF NG,IMF_Delhi
2,NA,IMF-DE-1B,test1,1,2,172.31.254.6,IMF-DE-1B,IMF NG,IMF NG,IMF_Delhi
2,NA,IMF-DE-1C,,1,3,172.31.254.7,IMF-DE-1C,IMF NG,IMF NG,IMF_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.

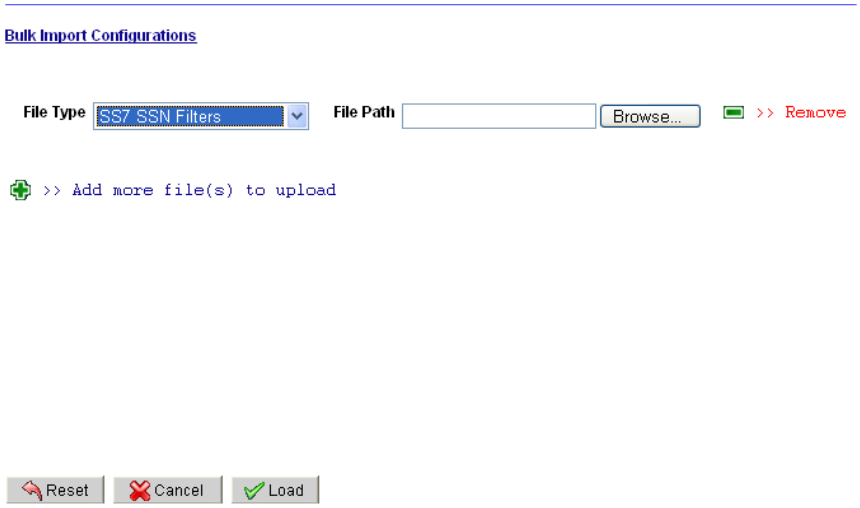


Figure 29: Bulk Load Import Screen

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 **Synchronize** the Subsystem.

PDU Filter Configurations

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

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		30		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Type	String	Calling, Called, Both		Yes
6	SSN List	String			Yes

TABLE 25: SSN FILTER CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		31		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Type	String	OPC, DPC, Both		Yes
6	Flavor	String	ANSI-SS7, etc.		
7	PC List	String			Yes

TABLE 26: PC FILTER CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		32		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Type	String	Calling, Called, Both		Yes

ID	Field	Data Type	Value	Optional	Can Be Updated
6	GT List	String			Yes

TABLE 27: GT FILTER CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		34		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Expression	String			Yes

TABLE 28: RAW FILTER CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load Type		33		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
5	Expression	String			Yes

TABLE 29: SS7 COMBO FILTER CONFIGURATION

Importing PDU Filters

Pre-conditions for importing PDU 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.
4. A log entry exists in the Audit Viewer application.

Complete these steps when importing an PDU 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.

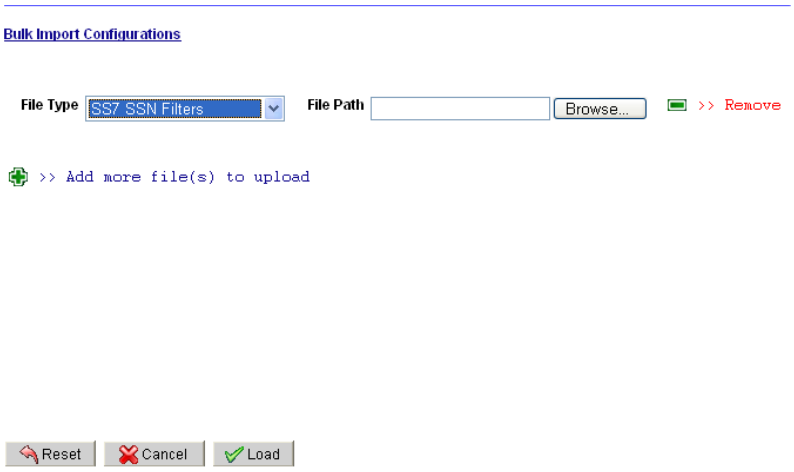


Figure 30: Browse Screen

3. Select the **SSN.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. PCFilters.cvs
   b. GTFilters.cvs
   c. RawFilters.csv
   d. SS7ComboFilters.csv

6. Click **Load**.
   The files are uploaded to the system.

Once you have imported the files, you must **Synchronize** 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.

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

TABLE 30: IP ADDRESS FILTER CONFIGURATION

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load		36		No

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

TABLE 31: IP PORT 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
5	VLAN List	String			Yes

TABLE 32: VLAN FILTER CONFIGURATION

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

TABLE 33: IP COMBO FILTER CONFIGURATION

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.

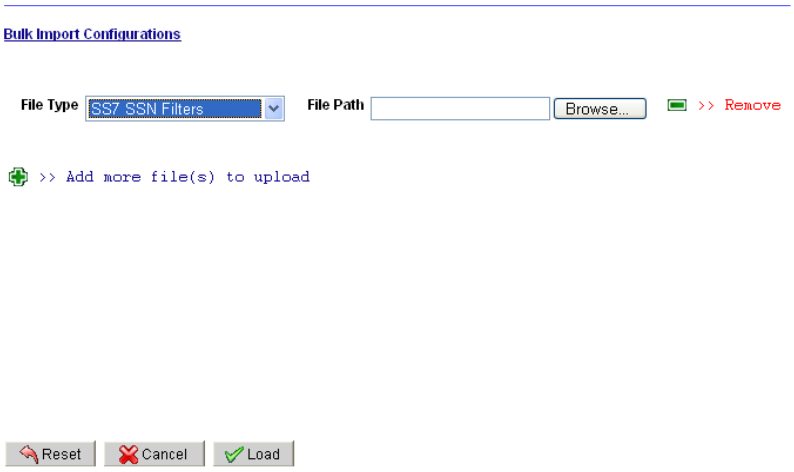


Figure 31: Browse Screen

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 Synchronize the Subsystem.

PMF GB Filter Configuration

This table shows the basic PMF GB filter configuration, (DLCI Filter), needed when importing GB filters using the bulk import process along with an example of a DLCI Filter.

ID	Field	Data Type	Value	Optional	Can Be Updated
1	Bulk Load		39		No
2	Object ID	Number			No
3	Name	String			Yes
4	Description	String		Yes	Yes
	Selected DLCI Numbers	String	INCLUDE EXCLUDE		Yes
6	DLCI List	String			Yes

TABLE 34: DLCI FILTER CONFIGURATION

Bulk Load	FieldID	Name	Description		DLCI List
39	NA	DLCI_Test_2	test	INCLUDE	8
39	NA	DLCI_Test_1	test	EXCLUDE	2,4

TABLE 35: DCLI.CSV FILE

Importing PMF GB Filters

Pre-conditions for importing PMF GB 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 an PMF GB 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.

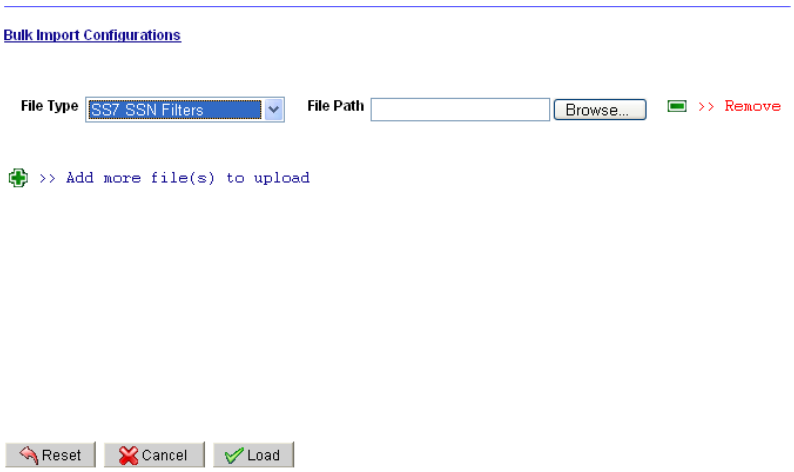


Figure 32: Browse Screen

3. Select the **DLCIFilters.csv**.
4. Click **Open**.
   The directory path with the file appears in the field.
5. 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 IMF and PMF)
- SS7 Network Elements
- Gb Network Elements
- IMF Linkset Assignments
- PMF Link Assignments
- SS7 PDU filters
- 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.

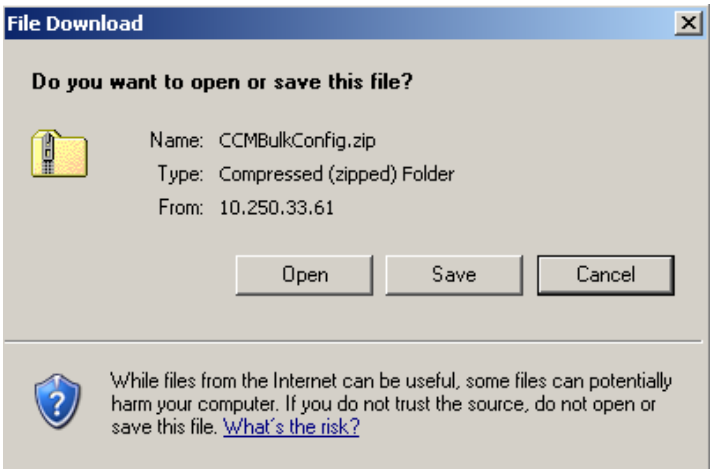


Figure 33: Bulk Export Configurations Prompt

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.

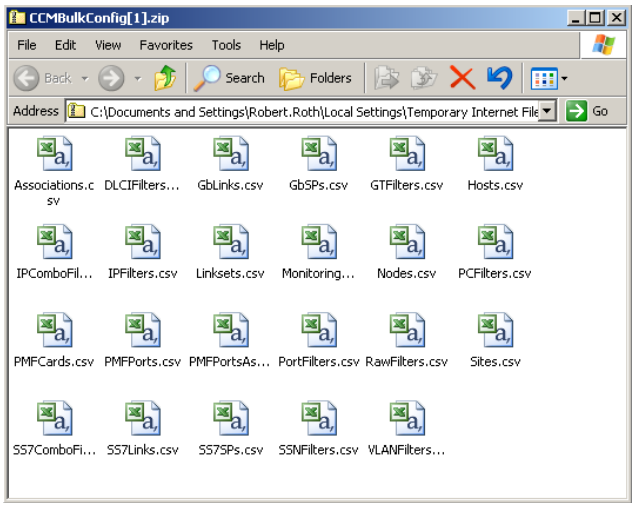


Figure 34: Bulk Export Configurations Prompt

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 your PIC system as well as ProTraq and ProAlarm applications.

Selecting the **Create Configuration Report** option initiates a prompt shown below.

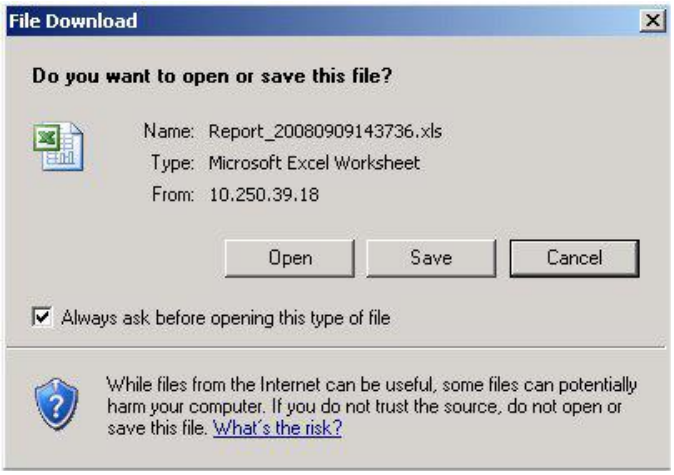


Figure 35: Open/Save Prompt For Configuration Report

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.

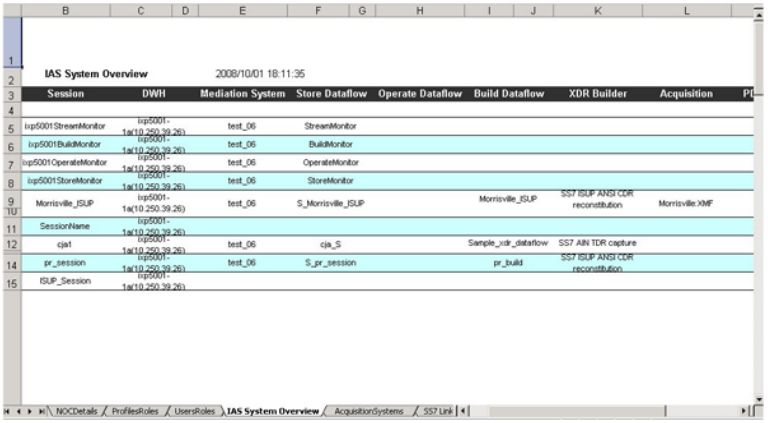


Figure 36: Sample Report

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

Configure alarm severity offset

The View/Configure Severity offset link provides a list of all the alarm specific problems present in your system. It allows to override incoming alarm severity according its specific problem. This mechanism is applied at listening time when each alarm event is received.

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

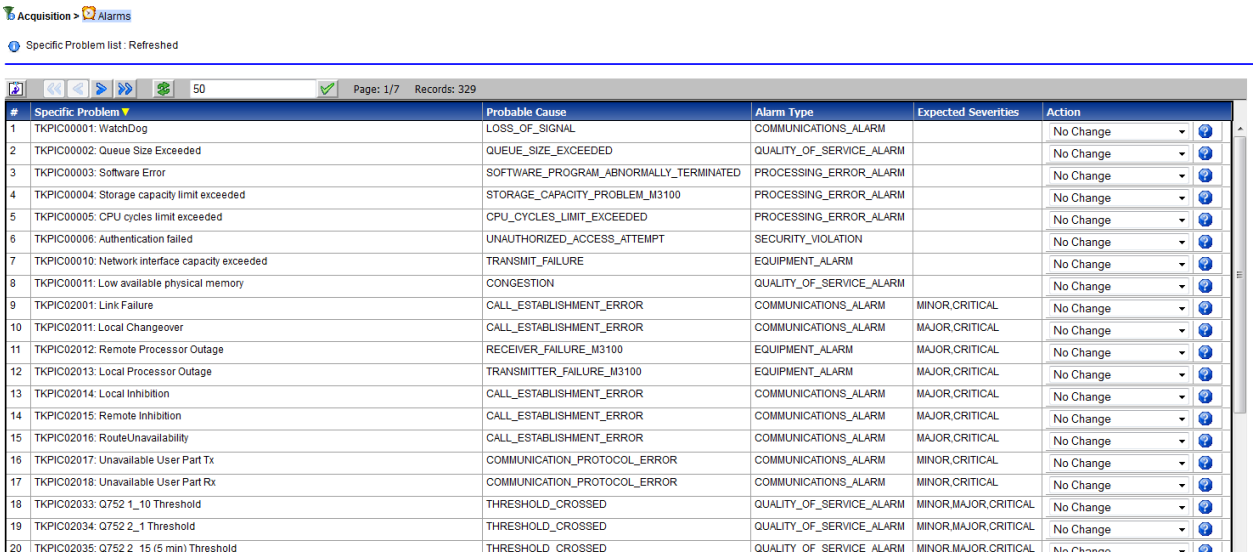


Figure 37: Alarms Severity offset Screen

1. Display the **Alarm** Specific Problem to be modified.
2. Modify offset setting in Action column. It will modify incoming alarm event severity (or reject event) according its specific problem according below table

Incoming severity	**Increase severity**			**No change**	**Decrease severity**			**Ignore**
	By 3	By 2	By 1		By 1	By 2	By 3	
CRITICAL	CRITICAL	CRITICAL	CRITICAL	CRITICAL	MAJOR	MINOR	WARNING	NONE
MAJOR	CRITICAL	CRITICAL	CRITICAL	MAJOR	MINOR	WARNING	WARNING	NONE
MINOR	CRITICAL	CRITICAL	MAJOR	MINOR	WARNING	WARNING	WARNING	NONE
WARNING	CRITICAL	MAJOR	MINOR	WARNING	WARNING	WARNING	WARNING	NONE

TABLE 36: ALARM SEVERITY OFFSETS

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

Managing Third Party (External) Applications

The CCM Home page also provides a means of managing third party (external) applications. Clicking on the link enables you to add, modify or delete an external application.

The list screen shows the following application information.

Figure 38: Thirdparty List Screen

Column	**Description**
Host Name	Provides the name of the server housing the application
IP Address	Gives the IP Address of the server
Application	Shows the application name
Version	Shows the version of the application
Description (Optional)	Shows any specific information (if any) about the application
Actions	Provides icons to perform specific actions on the applicaiton such as deleting an application.

TABLE 37: THIRD PARTY (EXTERNAL) APPLICATION COLUMNS

Creating a Third Party Session

Complete these steps to create a third party session:

1. From the Home Page, click **Manage Thirdparty Applications**.
   The *List* screen opens.

Figure 39: Thirdparty List Screen

2. Click **Add** from the tool bar.
   The *Add* screen opens

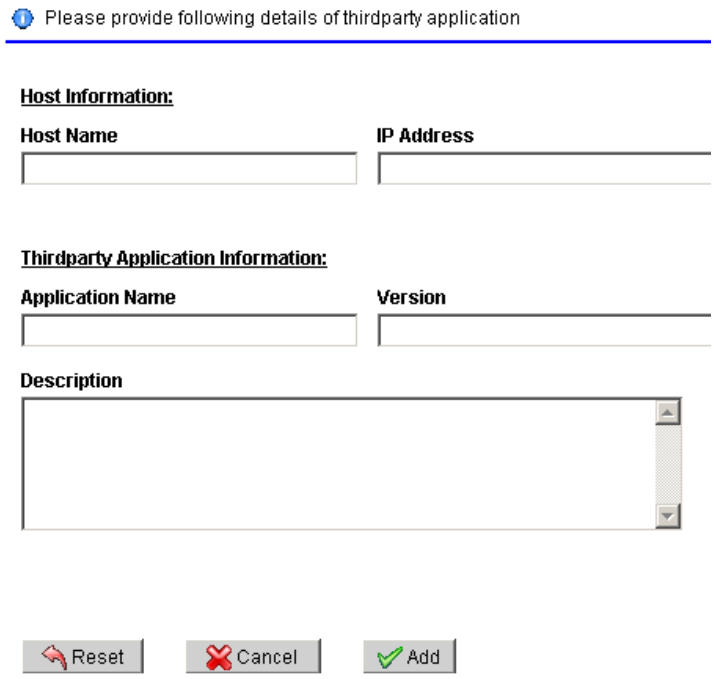


Figure 40: Thirdparty Application Add Screen

3. Enter the **Host Name**.
4. Enter the **IP Address** of the host machine.
5. Enter the **Application Name**.
6. Enter the **Version**.
7. (Optional) Enter a **Description** of the application.
8. Click **Add**.
   The session information is added to the system

Modifying a Third Party Session

Complete these steps to modify a third party application session:

1. Select **Home Page > Manage Thirdparty Applications**.
   The *List* screen opens.
2. Select the **session** to be modified.
3. Click **Modify** the session screen opens.
4. Make the necessary modifications.

5. Click **Modify**.
   The modifications are saved and you are returned to the list screen.

Deleting a Third Party Session

Complete these steps to delete a third party application session:

1. Select **Home Page > Manage Thirdparty Applications** .
   The *List* screen opens.
2. Select the **session** to be deleted.
3. Click **Delete** the session screen opens.
4. Click **OK** at the prompt.
   The session is deleted from the system.

Auto Synch Parameters

The CCM Home page provides a Auto Synch Parameters feature that automates the synchronization and apply process at timed intervals for IMF subsystems.

Note: The Auto Synchronization process is only for IMF subsystems. Both IXP and PMF subsystems need to be manually synchronized and applied.

Clicking on the **Auto Synch Parameters** feature on the Home Page opens the Auto Synch Parameters pop-up window. This pop-up window has two options.

- Configure Auto Synch - this option enables the user to turn on or turn off the auto synch feature.

  Note: The default is **Off**.

- Synch Interval (in minutes) - once the auto synch feature is turned on, then the user can enter a time interval in minutes and the auto synch process will continue to occur at that interval.

Once the parameters have been set, click **OK**. The pop-up window vanishes and the system is now set.

xMF Synchronization Reports

The CCM Home page provides an xMF Synchronization Reports feature that provides a text file providing the information traditionally given in the manual synchronization process. This feature works in combination with the Auto Synch Parameters feature. If the Auto Synch Parameters feature is turned on, then the IMF synchronization reports are generated at the intervals set in Auto Synch Parameters.
Note: Default interval is 5 minutes

The xMF synchronization report, like the manual process, provides the following information in text format.

- Elements Added - shows the number of elements added to the IMF subsystem.
- Elements Removed - shows the number of elements added from the IMF subsystem.
- Elements Modifies - shows that number of elements modified in the IMF subsystem.
- No Change - shows the number of elements that were not affected in the synchronization process.
- Errors - shows errors that occurred during the synchronization process.

Chapter 5: Equipment Registry

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 PIC.

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 (xMF) 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, except Report Server that needs to be loaded manually, you do not need to change/add anything under the NOC site. For more information about the report server, see Managing the Report Server. 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 four categories of subsystems are automatically created under the site:

- DWH - Data Warehouse
- IXP - Integrated xDR Processor (Mediation Perspective)
- XMF - Integrated Message Feeder (IMF) and Probe Message Feeder (PMF) (Acquisition Perspective)
- EFS - Exported Filer Server
- NEPTUNE – Astellia Neptune probe

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 XMF 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.

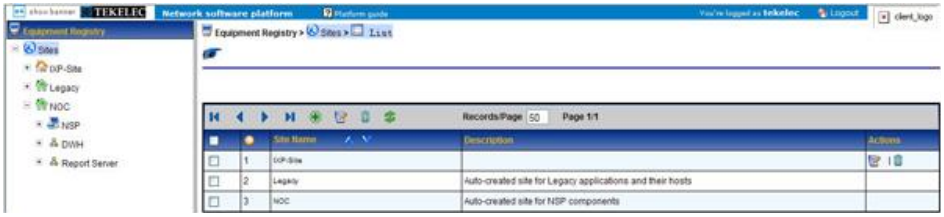


Figure 41: Site List Screen

Creating a Site

Complete these steps to add a site.

1. On the object tree, select **Sites**.
2. Select **Add** from the pop-up menu.
   The *Add* screen opens shown in the figure.

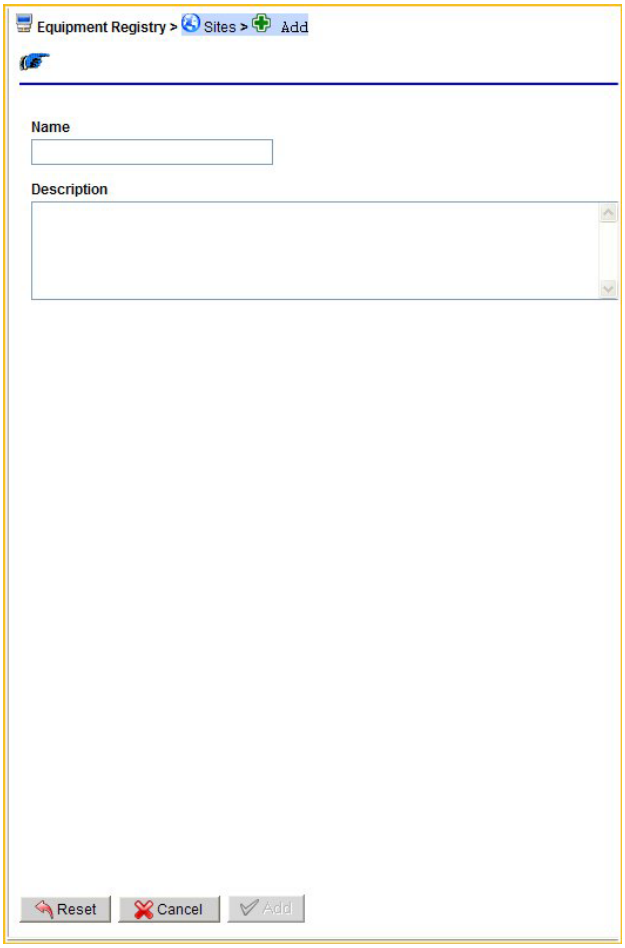


Figure 42: Site Add Screen

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.

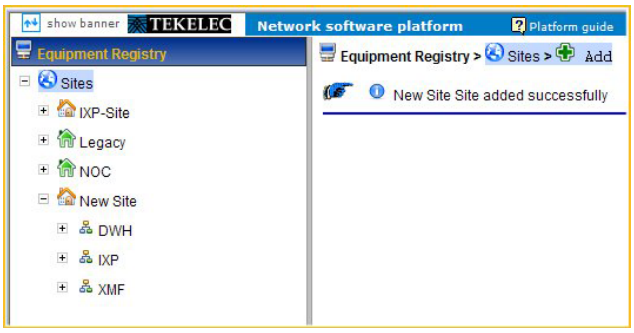


Figure 43: New Site With Subsystems

Modifying a Site

Complete these steps to modify a site.

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

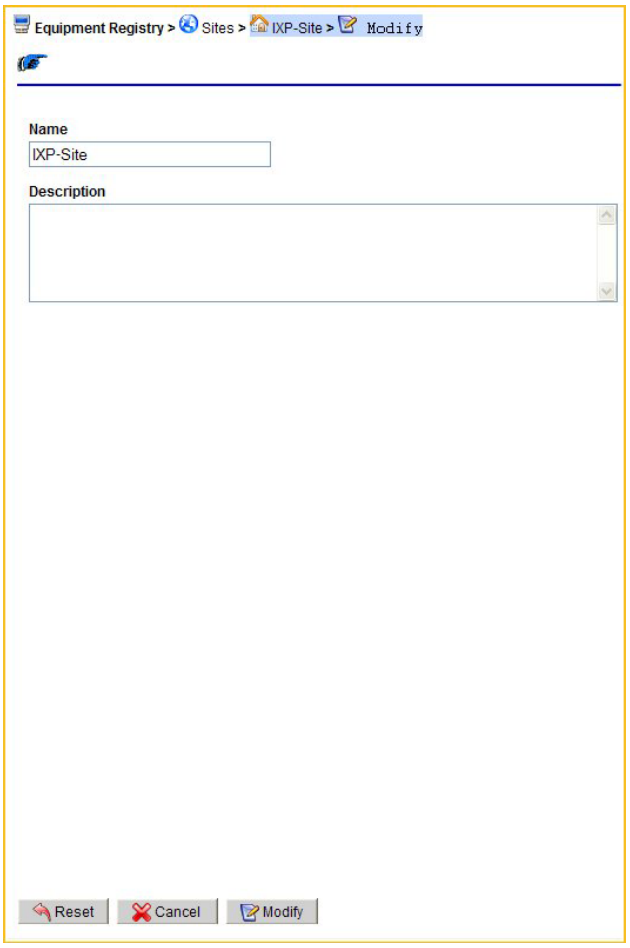


Figure 44: Site Modify Screen

1. Make necessary modifications to the site information.
2. 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 Sever (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 Sever (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 Sever (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.

Managing the Export File Server

The export file server (EFS), if it is present, can be added to any site, and is part of the Data Feed Export function of PIC. It is an IXP server that is assigned the EFS designation to handle the data export process. The EFS provides the infrastructure for static enrichment and KPI generation.

Note: You can only have one export file server per site.

To add an export server, follow the steps used in adding an IXP subsystem.

About Subsystems

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

- DWH for storage
- IXP for storage and correlation
- xMF for data acquisition
- EFS for exported files

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.

Adding a Data Warehouse (DWH)

Complete these steps to add a Data Warehouse to the DWH subsystem.

1. Select **Equipment Registry > Site > DWH**.
2. Right-click on **DWH**.
3. Select **Add** from the pop-up menu.
   The *Addscreen* appears.
   Add DATA WAREHOUSE subsystem screen - field descriptions

Field	Description
Storage Name	The name of the DWH server
Version	Vesion of the Oracle database (default 10.2) housed in the DWH
Description (optional)	Text field to add useful descriptions about the DWH (Default phrase is, "Created for external storage."
Login User ID	User ID to log into the DWH
Password	Password for logging into the DWH
Service Name	Alphanumeric field to provide the name of the service running the database
Port	Numeric field to enter the port number of the DWH
IP Address	TheIP address of DWH

TABLE 38: DATA WAREHOUSE ADD SCREEN

4. Enter the **Storage Name** of the DWH .
5. Enter the **Version** of the Oracle database running on the DWH.
6. (Optional) Enter a **Description** of the DWH
7. Enter the **Login User ID** for the DWH
8. Enter the **Password**.
9. Enter the **Service Name** of the DWH.
10. Enter the **Port number**.
11. Type in the **IP Address** of the DWH
12. Click **Add** to add the subsystem to the list.
    The DWH is added to the system.

Modifying a Data Warehouse (DWH)

Complete these steps to modify a subsystem.

1. Select **Equipment Regristry > Site > DWH** to be modified.
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 a Data Warehouse (DWH)

Complete these steps to delete a DWH subsystem.

1. Select the **Equipment Registry >Site > DWH** to be deleted.
2. Select **Delete** from the popup menu.
3. Click **OK** at the prompt.

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 xMF) 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 examplethe Bcast 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**.
   The *Add* screen appears.
   Add IXP subsystem 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 assignment of the VIP address can be the default of the broadcast address (broardcast-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.

TABLE 39: IXP SUBSYSTEM ADD SCREEN FIELD DESCRIPTIONS

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.

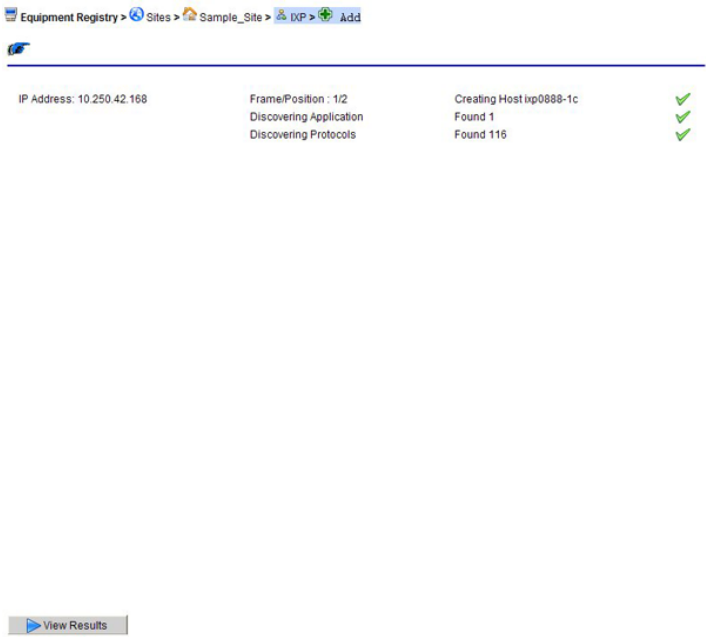


Figure 45: Subsystem Results Summary Screen

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

Figure 46: Results Summary Screen With Error Symbol

9. Click **View Results**.
   The Results screen opens.
   The screen has four tabs with five subtabs:
   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 47: 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.

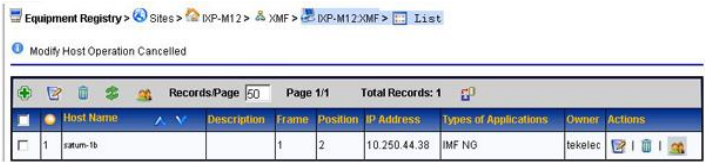


Figure 48: IXP Subsystem List Screen

2. Select **Host** from the list.
3. Click **Discover Applications** on the toolbar.
   The screen changes, shown below, to show the re-discovered applications.

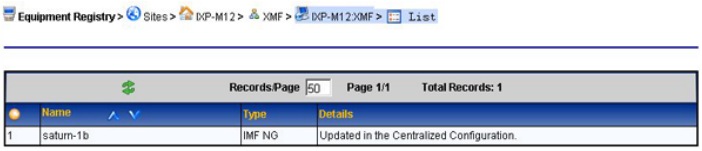


Figure 49: IXP Subsystem List Screen

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

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.

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.

TABLE 40: IXP STORAGE SERVER STATES

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 an 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.

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

TABLE 41: IXP SERVER DESIGNATIONS

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. 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.

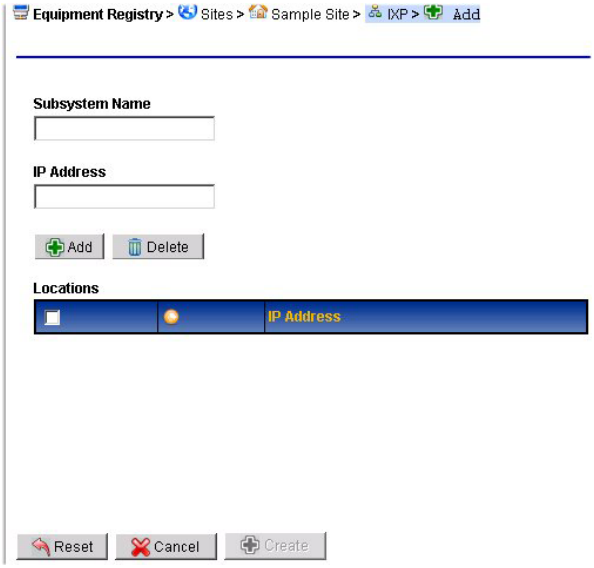


Figure 50: Add IXP Subsystem Screen

Add IXP subsystem screen - field descriptions

Field	Description
Subsystem Name	The name of the subsystem (required)
IP Address	TheIP address of subsystem
Add button	Adds theIP address, to the list (you can have more than oneIP 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.

TABLE 42: IXP SUBSYSTEM ADD SCREEN

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.

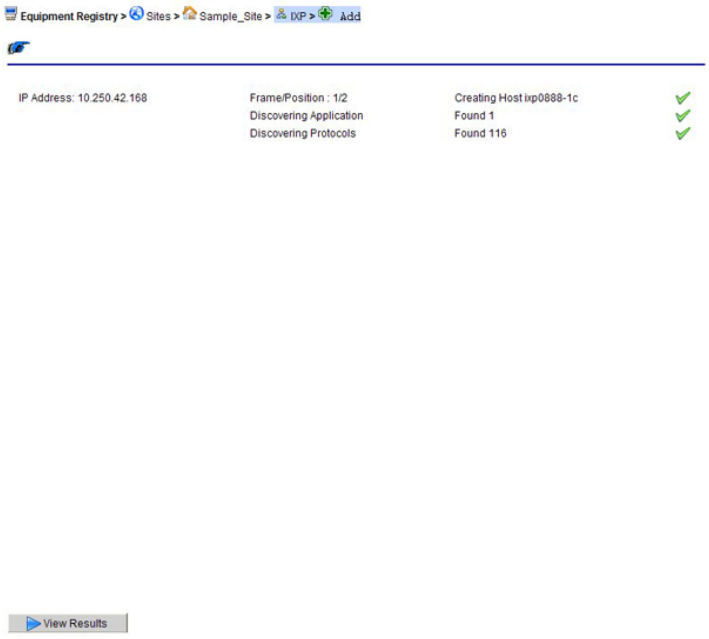


Figure 51: Subsystem Results Screen

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

Figure 52: 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 53: 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 server **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 (IMF and PMF) Subsystems

You have the ability to discover xMF Subsystem information. xMF subsystems include both IMF and PMF. Once the subsystem has been created and hosts discovered you must go to either the Acquisition perspective to configure the Subsystem.

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

Adding an IMF Subsystem to a Site

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

Note: A site can only have one IMF subsystem.

Note: When an IMF subsystem is added all network elements are automatically discovered.

1. Select **Equipment Registry > Site > xMF**.
2. Click **Add** on the xMF subsystem tool bar.

   Note: The right-click menu on the xMF folder can be also used. Select Add from the menu options.

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 xMF subsystem resides. **Note:** The VIP is established by the xMF subsystem when it is installed and integrated into the customer network. The assignment of the VIP address can be the default of the broadcast address 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 IMF subsystem.
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.

TABLE 43: XMF SUBSYSTEM ADD SCREEN FIELD DESCRIPTIONS

3. Enter the **VIP Address**. (See *Virtual IP Address Assignment* for more information on using VIPs.)
4. Enter the **IP Address** for the IMF host.

   Note: This address is established when the IMF subsystem is installed and integrated into the customer network.

5. Click **Add**.
6. Click **Create**.
   The *Verification* screen opens to show the discovery process.

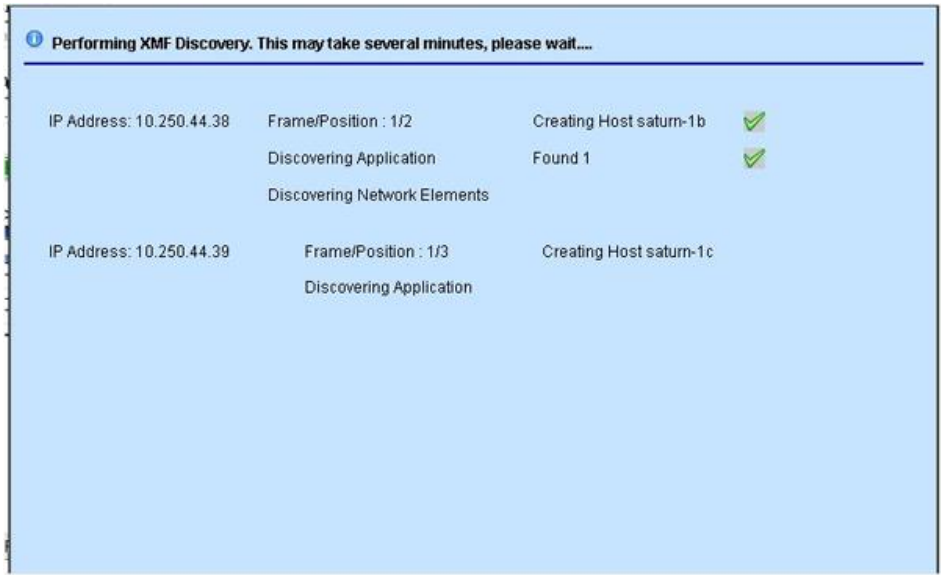


Figure 54: Verification Screen - Done Button Not Shown

7. Click **Done**.
   The Results screen opens showing the following information:

   Note: The Results Summary screen only opens when the discovery process has finished.

   a. Host tab - showing the IP addresses of the discovered hosts and the result
   b. Application - showing the applications that were discovered
   c. Network Element Discovery - showing the links belonging to the hosts that has the following five tabs:

      - Added - shows any elements that have been added to the host since the last discovery process
      - Removed - shows any elements that have been removed since the last discovery process
      - Modified - shows any elements that have been modified since the last discovery process
      - No change - shows the elements that have not changed since the last discovery process
      - Error - shows any errors that occurred in the discovery process

        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 changes have been made to an existing IMF subsystem and the Synchronize function is used and the discovery process is repeated (see how to modify hosts).

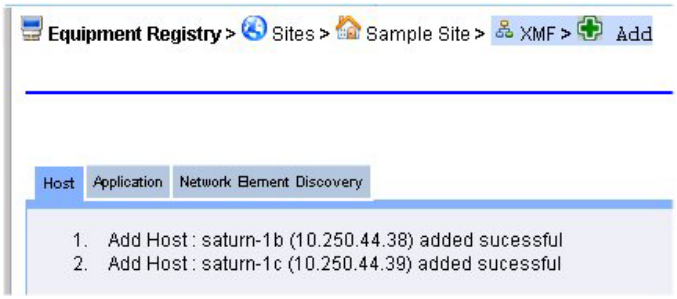


Figure 55: Results Summary Screen - Host Tab

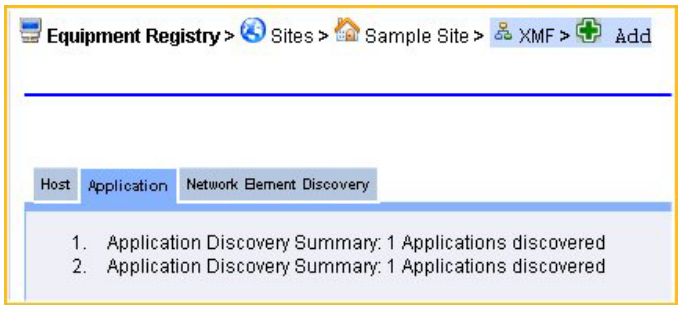
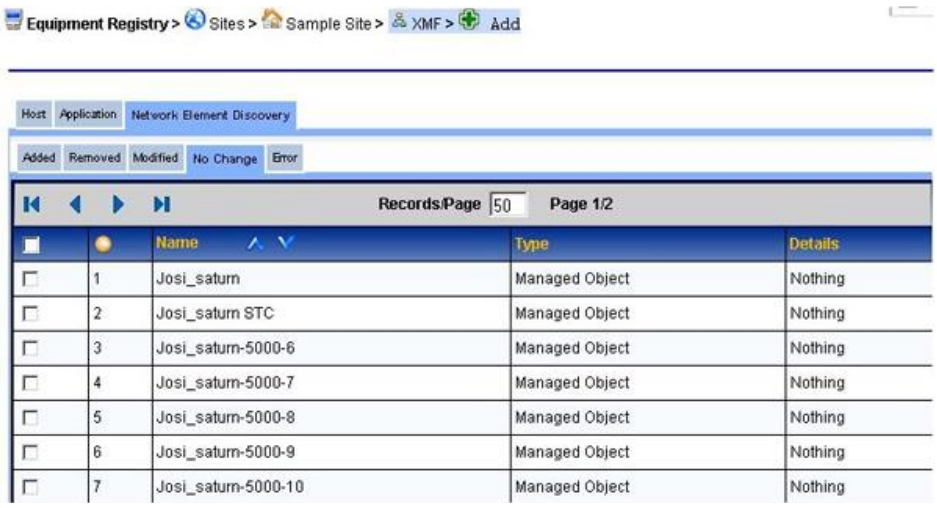


Figure 56: Results Summary Screen - Application Tab



		Name	Type	Details
☐	1	Josi_saturn	Managed Object	Nothing
☐	2	Josi_saturn STC	Managed Object	Nothing
☐	3	Josi_saturn-5000-6	Managed Object	Nothing
☐	4	Josi_saturn-5000-7	Managed Object	Nothing
☐	5	Josi_saturn-5000-8	Managed Object	Nothing
☐	6	Josi_saturn-5000-9	Managed Object	Nothing
☐	7	Josi_saturn-5000-10	Managed Object	Nothing

Figure 57: Results Summary Screen - Network Element Discovery

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

Modifying an xMF Subsystem

Complete these steps to modify an xMF subsystem host.

1. Select the **Site > xMF subsystem** to be modified from the object tree.
   The *List* screen opens.
2. Select the **Host**.
3. Click **Modify** from the tool bar.
4. Make necessary **modifications** on either screen (click Next) to open the next screen.
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.

Modifying an IMF Subsystem Host

Complete these steps to modify an xMF subsystem host.

1. Select the **Site > xMF** subsystem to be modified from the object tree.
   The *List* screen opens.
2. Select the **Host**.
3. Click **Modify** from the tool bar.
4. Make necessary **modifications** on either screen (click Next) to open the next screen.
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 an xMF Subsystem

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

Complete these steps to delete an xMF subsystem.

1. Select **Site > xMF** to be deleted.
The *List* screen opens. (Or select the subsystem from the Site List screen.)
2. Click **Delete**.
3. Click **OK** at the prompt.
The subsystem is deleted.

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**.

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. See *Virtual IP Address Assignment*.
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.

TABLE 44: XMF SUBSYSTEM ADD SCREEN FIELD DESCRIPTIONS

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. See Adding an E1/T1 (SPAN) Card (PMF) for more information.

Figure 58: 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

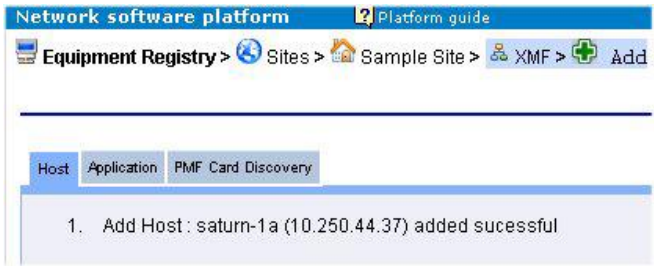


Figure 59: Discovery Summary Screen - Hosts Tab

Figure 60: 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.).

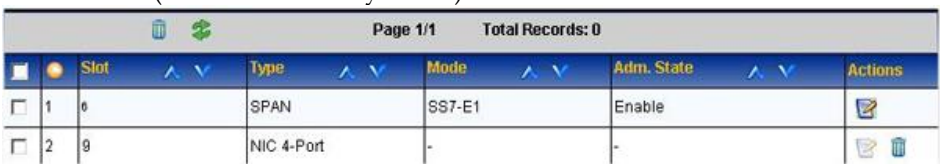


Figure 61: Discovery Summary Screen - PMF Card Discovery

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.

Adding a Neptune probe to a Site

Complete these steps to add Neptune probe.

1. Select the **Equipment Registry > Sites > Site > NEPTUNE**
   The *List* screen opens.
2. Enter **Probe name**.

   Same validation restriction as session name with maximum length 8.
3. Enter any **User information**.
4. Enter probe **Administration IP**.
5. Enter probe **Process Flow IP**.

6. Enter probe **Login** and **Password**.

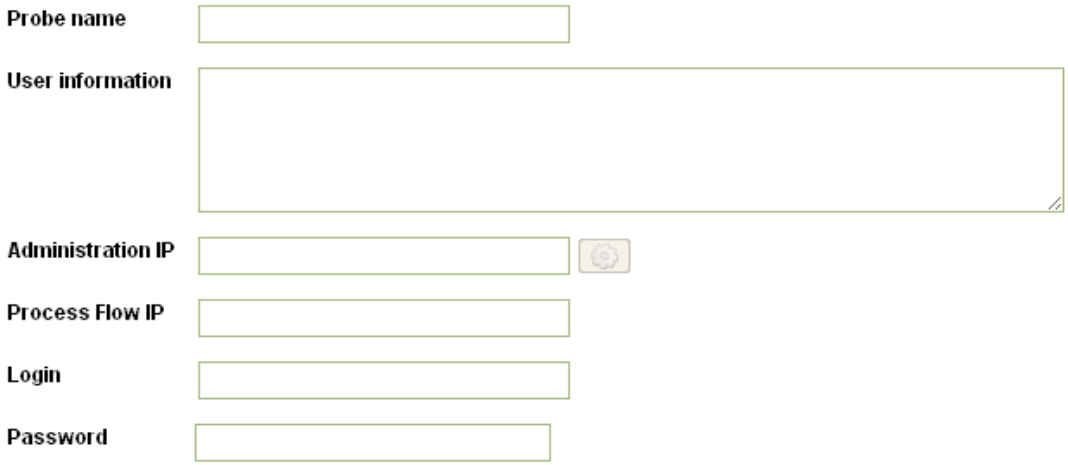


Figure 62: Neptune probe registration

Modifying a Neptune probe

Complete these steps to modify Neptune probe.

1. Select the **Equipment Registry > Sites > Site > NEPTUNE**
   The *List* screen opens.
2. Select the Neptune probe to be modified.
3. Select **Modify** from the toolbar.
4. Make necessary **modifications**.
5. Click **Modify** after the necessary modifications are updated.

Deleting a Neptune probe

Complete these steps to delete Neptune probe.

1. Select the **Equipment Registry > Sites > Site > NEPTUNE**
   The *List* screen opens.
2. Select the Neptune probe to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.
   The Neptune probe is deleted.

Chapter 6: Network Element Configuration

About Network Elements

The term, Network Elements, refers to customer network SS7, GPRS and IP elements. The perspective is divided into four categories:

- Nodes that include SS7, GPRS and IP
- SS7 Elements that includes Linksets, Links and Signaling Points
- GPRS Elements that includes GB links and Signaling Points
- IP Elements that include Signaling Points, Cards, Application Servers and Associations and Application Server Processes. Associations are divided into two subcategories: IMF and PMF.

In addition, each network element has a child table showing all dependent elements down to the link level. For example, selecting a linkset (shown in the figure) and clicking on the selecting Show Details button on the tool bar shows all the links belonging to that particular linkset.

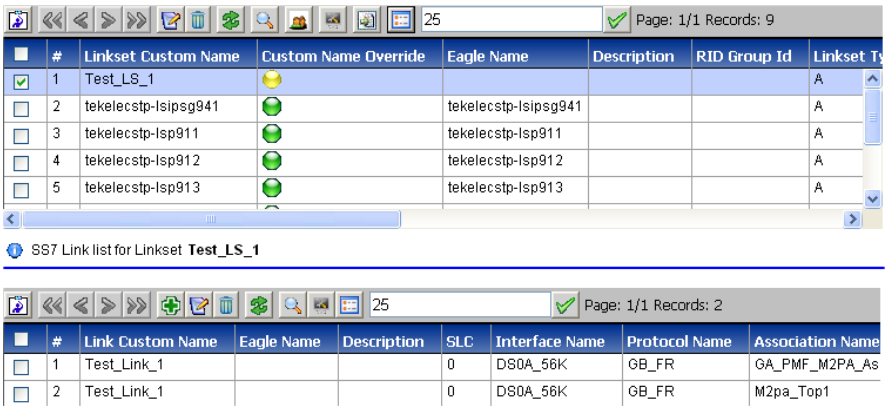


Figure 63: Selected Linkset with Corresponding Links

For quick reference, you can query for specific network elements such as nodes, linksets, links or signaling points. This function is very helpful in large networks.
In addition, for linksets and links, you can use the Eagle name or by using the custom override operation create a custom name for a linkset or link.

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.

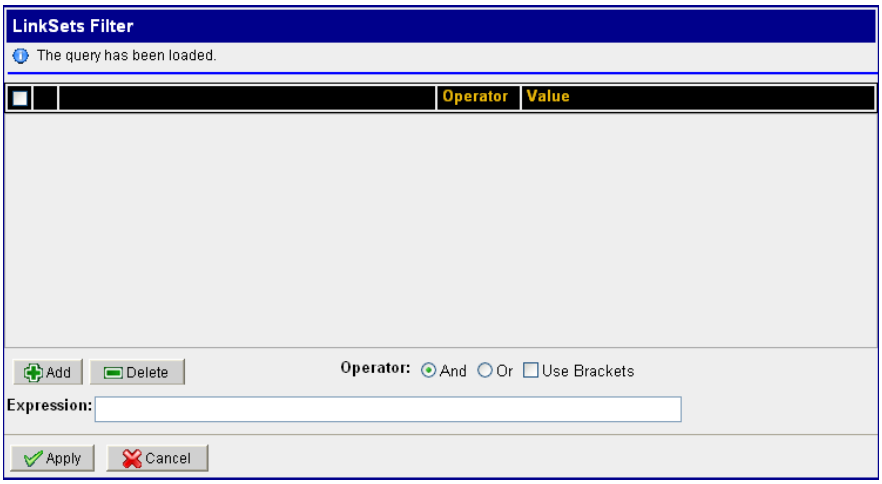


Figure 64: Network Element Filter Screen (Linkset shown)

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).

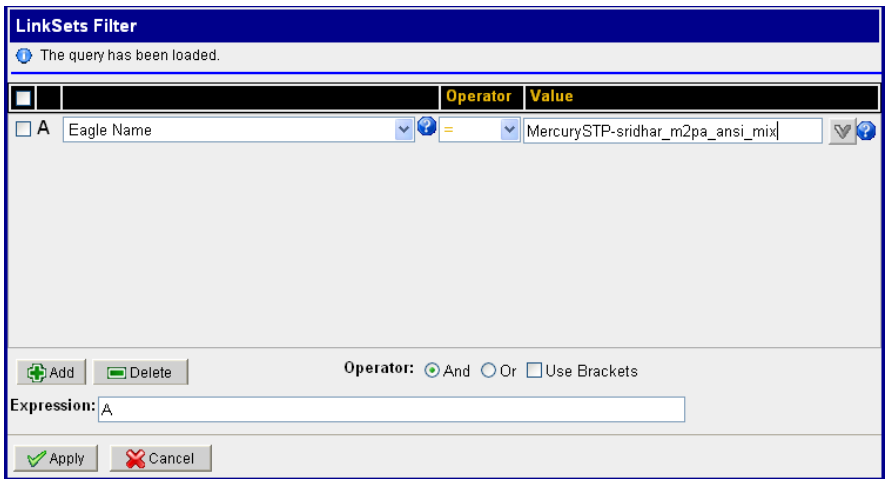


Figure 65: Filter Screen Filled

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.

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
Cancel button	Cancels the procedure

TABLE 45: ADD NODE SCREEN

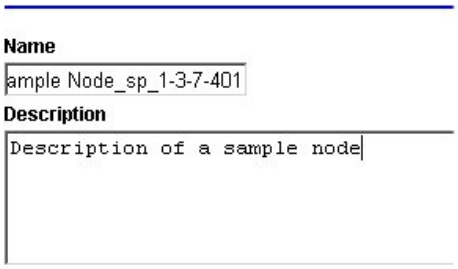


Figure 66: Node Add Screen

2. Type in the **Name** of the Node.
   (Optional) Type in a **description** of the node.
3. 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 SS7 Network Elements

The SS7 network element menu has four main categories:

- Linksets - linksets that are manually created (IMF) and discovered (PMF)
- Associations - are SCTP connections
- Links
- Signaling Points (SPs)

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

About Linksets

Linksets can exist as one or a combination of SS7 links each linkset can contain up to 16 links.

Creating a Linkset

Complete these steps to create a linkset.

Note: Signaling points must be configured before linksets can be created.

1. Select **Node > Signaling Point > Linkset > Add** from the Network Elements tree. The Add linkset screen opens shown in Figure 67: Add Linkset Screen.

Field	Description
Name	Required field used for the name of the linkset
Description	Optional field to describe the linkset
Reset button	Resets the screen to default values
Cancel button	Cancels the procedure
Next button	Opens the next screen/step of the sequence

TABLE 46: ADD LINKSET SCREEN

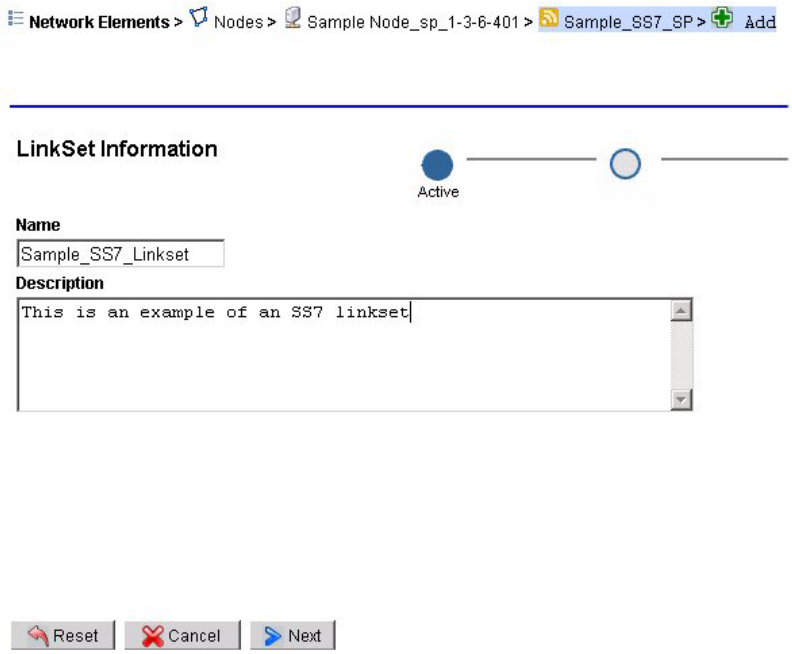


Figure 67: Add Linkset Screen

2. Type in the **Name** of the linkset.
3. (Optional) Type in a **description** of the linkset.
4. Click **Next**.
   The *Signaling Points* screen opens shown in Figure 68: Associating A Linkset To Signaling Points.

Field	Description
SP1	This field contains the originating signaling point that the linkset belongs to
SP2	(Search field) Drop-down list for selecting the second signaling point
Previous button	Opens the preceding screen
Next button	Opens the next screen in the procedure

TABLE 47: SECOND ADD SIGNALING POINT SCREEN

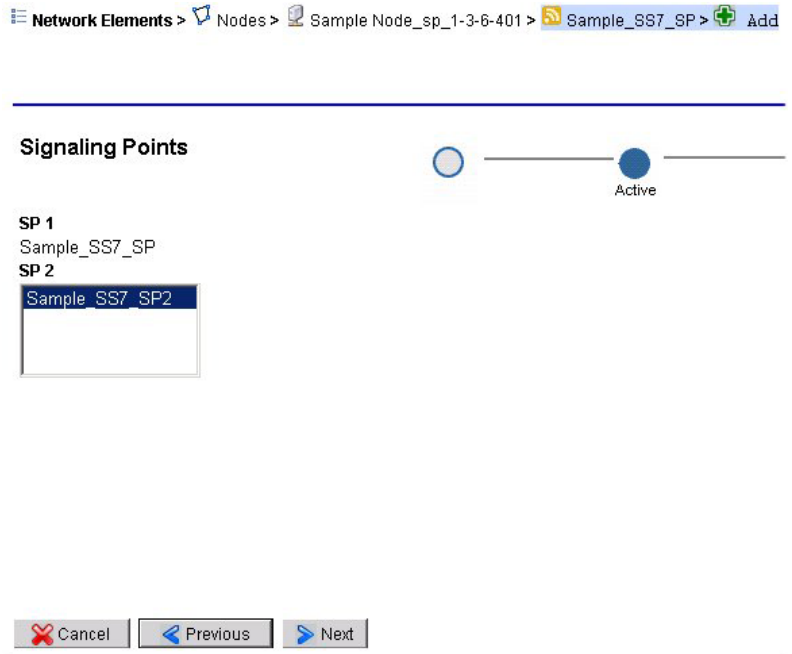


Figure 68: Associating A Linkset To Signaling Points

5. Select a **signaling point** in the SP2 field.
6. Click **Next**.
   The *Additional Information* screen opens shown below.

Field	Description
Linkset Type	(Search field) Drop-down list for selecting the type of linkset
Resource ID Group (optional)	(Search field) Drop-down list for selecting a specific group
Add button	Saves the record to the system
Next button	Opens the Linkset Summary screen

TABLE 48: THIRD ADD SIGNALING POINT SCREEN

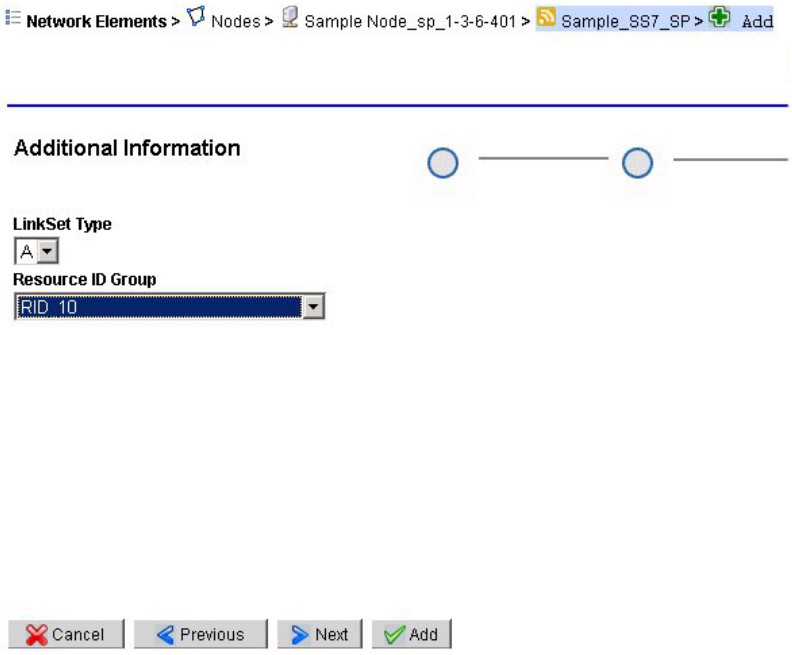


Figure 69: Linkset Additional Information

7. Select a **Linkset Type**.
8. Select a **Resource ID Group**.
   (Auto RID or user-defined RID group see About Resource ID Groups (RID)).
9. Click **Add**.
   The linkset is added to the signaling point shown below.

Figure 70: Linkset List With New Linkset Added

Modifying a Linkset

To modify a linkset, Complete these steps.

Note: For discovered linksets, you can only modify the Name and Description fields.

1. Select the **linkset** to be modified.
2. Select **Modify**.
3. Make the necessary **modifications**.

4. Click **Modify**.
   A prompt appears stating that the linkset was modified.

Deleting a Linkset

Note: If a linkset has links, then the links that belong to that linkset are also deleted at the same time.

Note: If a linkset is the only linkset in the signaling point, then the signaling point is also deleted what that linkset is deleted.

To delete a linkset, complete these steps.

1. Select the **linkset** to be deleted from the list.
2. Select **Delete**.
3. Click **OK** at the prompt, the linkset is deleted.

Modifying RID Group Settings when Modifying a Linkset

This feature enables you to set Auto-RID or Auto Reverse RID settings for a linkset (Auto RID or user-defined RID group see About Resource ID Groups (RID)). Complete these steps to modify the RID Group settings for a linkset.

1. Select the **Node > Linkset** to be modified.
2. Click **Modify**.
3. Click **next** until the Resource ID Group field appears.
   The RID groups defined in the system are displayed under the Resource ID Group drop-down.
4. Select **one** of the two automatically created RID groups.
5. Click **Modify** to save your changes.

Note: You should set the same RID group value for related linksets from mated pair STPs.

Custom Name Override Function

You can choose to have the custom name of a linkset to be the same as the Eagle name. When using this function the values are:

- Enable - the custom name is the same as the Eagle name
- Disable - the custom name is different from the Eagle name

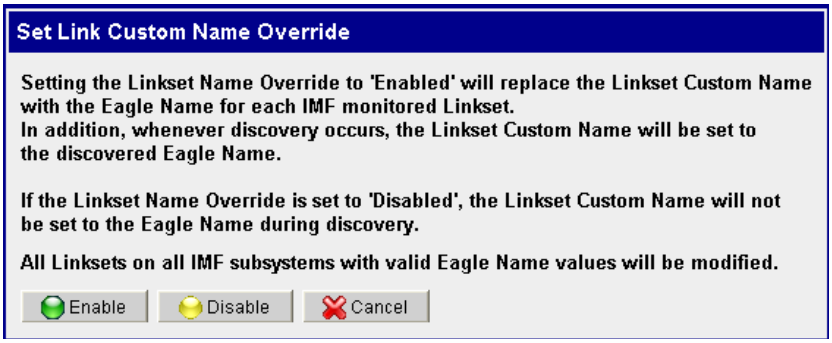


Figure 71: Custom Name Override Function Popup

The function is available on the Linksets list page tool bar.

About SS7 Links

SS7 Links belong to linksets. Links can be created only from manually created linksets, not discovered linksets. CCM also supports links defined on the Eagle E5-E1T1 card that are discovered by IMF. There is a column labeled "Interface Name" that designates the interface id value found during the discovery process.

Note: If a link(s) name is modified, all running feeds, that use the translation of the link names or pointcodes need to be deactivated and activated again for proper functioning.

Creating an SS7 Link

To add a SS7 link Complete these steps.

1. Select **Network Elements > Node > Signaling Point > Linkset > Add** from the Object tree.
   The *Add* screen opens shown in Figure 72: Add Screen.

Field	Description
Name	Required field to name the link
Description	Optional field that can describe the link
Cancel	Cancels the procedure
Next button	Opens the second phase of the setup procedure

TABLE 49: LINK NETWORK VIEW INITIAL SETUP SCREEN

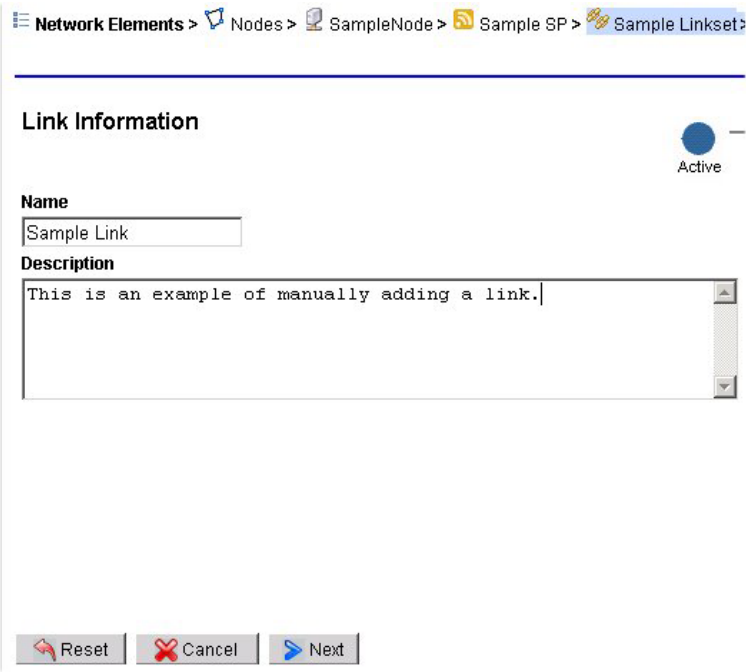


Figure 72: Add Screen

2. Enter the link **Name**.
3. (Optional) Type in a **Description**.
4. Click **Next**.
   The View Type Selection screen opens shown in Figure 73: View Type Selection Screen.

Field	Description
SLC	Drop-down list to choose an integer for the SLC
Interface	Drop-down list to choose the type of interface for the link
Transport Protocol	Drop-down list to choose the TP for the link
Cancel button	Cancels the procedure
Previous button	Returns you to the previous screen
Next button	Opens the Network/Link Summary screen
Add button	Add the link record to the linkset

TABLE 50: LINK NETWORK SETUP PHASE TWO

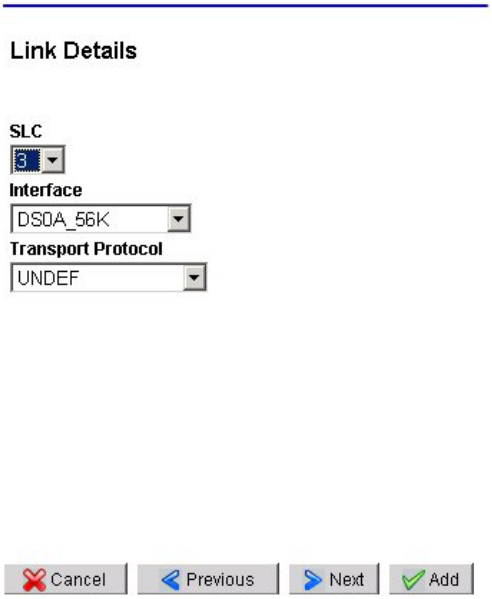


Figure 73: View Type Selection Screen

5. Select the **SLC** from the drop-down menu.
6. Select the **Interface** from the drop-down menu.
7. Select the **Transport Protocol** from the drop-down menu.
8. Click **Add**.
   The link is added to the linkset shown below.

Figure 74: View Type Selection Screen

Note: Click Next to view the Summary screen

Modifying an SS7 Link

Follow these steps to modify a link.

Note: If a link(s) name is modified, all running feeds, that use the translation of the link names or point codes need to be deactivated and activated again for proper functioning.

1. Select **Node > Signaling Point > Linkset > Link** to be modified.
2. Make the necessary **modifications**.
3. Click **Modify**.

The record is modified.

Deleting an SS7 Link

Follow these steps to delete a link.

Note: If a linkset or an association has only one link, then if the link is deleted then the linkset or association is also deleted.

1. Select **Node > Signaling Point > Linkset > Link** to be deleted.
2. Click **Delete**.
3. Click **OK** at the prompt.

The link is deleted.

Configuring SS7 Signaling Points

Signaling points provide a central nexus for SS7 linksets and links. Signaling points are discovered when the subsystem is created and all the elements are discovered. You can create signaling points only on non-discovered nodes.

Note: If a point code(s) is modified, all running feeds that use the translation of the link names or point codes need to be deactivated and activated again for proper functioning.

Creating a SS7 Signaling Point

Complete these steps to create a SS7 signaling point for a node.

1. Select **Network Elements >Nodes > SS7**.
   The *Node List* screen opens showing the node list table with signaling point table.

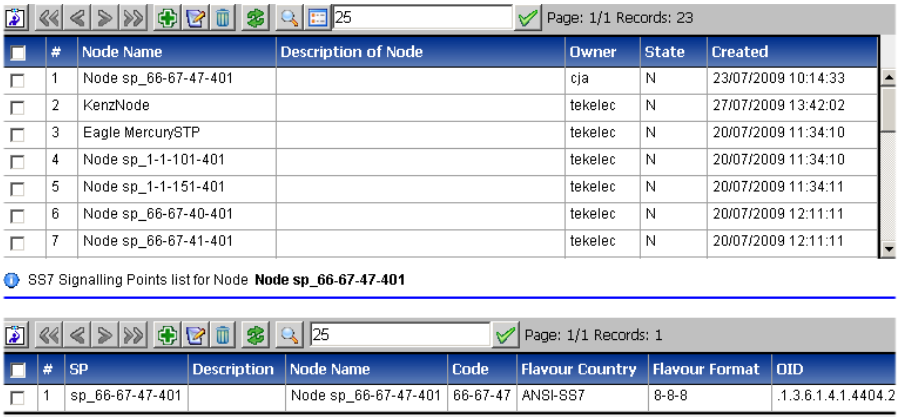


Figure 75: Add Signaling Point Screen

2. Click **Add** on the signaling point tool bar.
   The *IP signaling point add* screen opens.

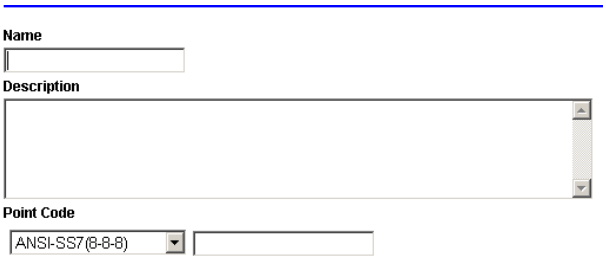


Figure 76: SS7 Signaling Point Add Screen

3. Enter the **Name** of the SS7 signaling point
4. (Optional) Enter a **Description**.
5. Select a **Point Code protocol** from the pull-down list.
6. Enter the **point code**.
7. Click **Add**.
   The SS7 signaling point is added to the Node.

Modifying an SS7 Signaling Point

Complete these steps to modify a SS7 signaling point.

Note: If a point code(s) name is modified, all running feeds, that use the translation of the link names or point codes need to be deactivated and activated again for proper functioning.

1. Select **Network Elements >SS7 >SPs**
2. Select the **SS7 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 SS7 Signaling Point

Complete these steps to delete an SS7 signaling point.

Note: When deleting a signaling point, all links and linksets associated with that signaling point are also deleted.

1. Select **Network Elements > SS7 > SPs**.
2. Select the **SS7 signaling point** to be modified.
3. Select **Delete**.
4. Click **OK** at the prompt.
   A prompt appears stating that the signaling point was deleted.

About GPRS Network Elements

GPRS (General Packet Radio Service) non-node network element menu has two categories:

- Gb links
- Signaling Points (SPs)

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.

About Gb Links

Gb links belong to GPRS nodes.

Adding a Gb Link

Complete these steps to add a Gb link to a GPRS signaling point.

1. Select the **GPRS signaling point** that needs a Gb link.
2. Select **Add** from the pop-up menu.
   The *Add Gb link* screen opens shown below.

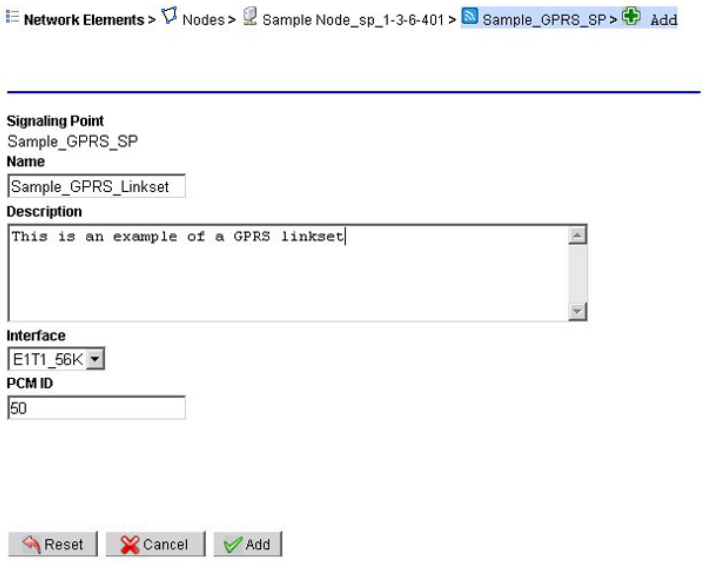


Figure 77: Add Gb Link Screen

Table below describes the Gb link add GUI:

Field	Description
Name	A required alphanumeric field that shows the name of the link
Description	An optional text box used for providing any specific information about the link
Interface	A required pull-down menu for selecting the interface for the link
PCM ID	A required numeric (0-99) field for entering the PCM ID
Add button	Adds the link information to the system
Cancel button	Cancels the procedure
Reset button	Resets the screen to the original state

TABLE 51: GB ADD SCREEN

3. Type in a **Name** for the Gb link.
4. (Optional) Type in a **Description** for the link.
5. Select an **Interface** for the link.
6. Type in a **PCM ID** for the link.
7. Click **Add**.
   The link is added to the signaling point.

Modifying a Gb Link

Follow these steps to modify a link.

1. Select **Node > GPRS Signaling Point > Link** to be modified.
2. Make the necessary **modifications**.
3. Click **Modify**.
   The record is modified.

Delete a Gb Link

Follow these steps to delete a link.

1. Select **Node > GPRS Signaling Point > Link** to be deleted.
2. Click **Delete**.
3. Click **OK** at the prompt.
   The link is deleted.

About GPRS Signaling Points

CCM enables you to configure and manage General Package Radio Service (GPRS) signaling points. GPRS signaling points are discovered when the network is configured. You can create signaling points only on network nodes that you have created, not from discovered nodes. You can only modify, delete and filter discovered signaling points.

Creating a GPRS Signaling Point

Complete these steps to create a GPRS signaling point.

Note: You can only create signaling points from GPRS nodes that you have created, not discovered.

1. Select **Network Elements >Node > GPRS**. The *Nodes list* screen opens with the signaling points list table on the bottom of the screen.

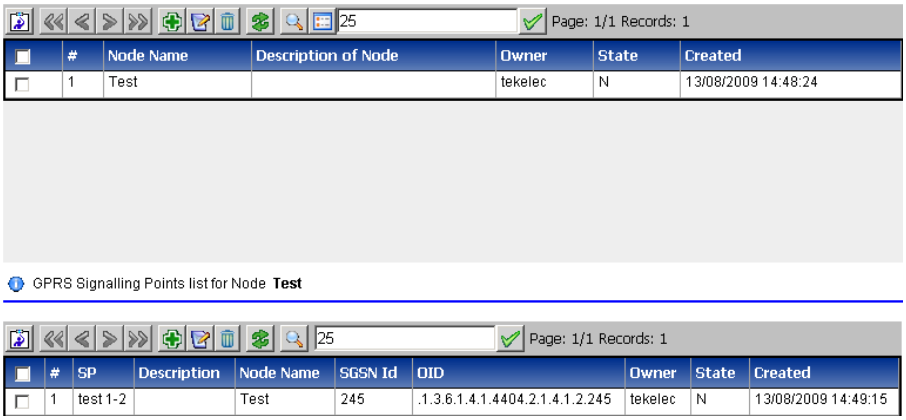


Figure 78: Nodes and Signaling Points List Screen

2. Click **Add** on the signaling points tool bar.
   The *GPRS signaling point add* screen opens

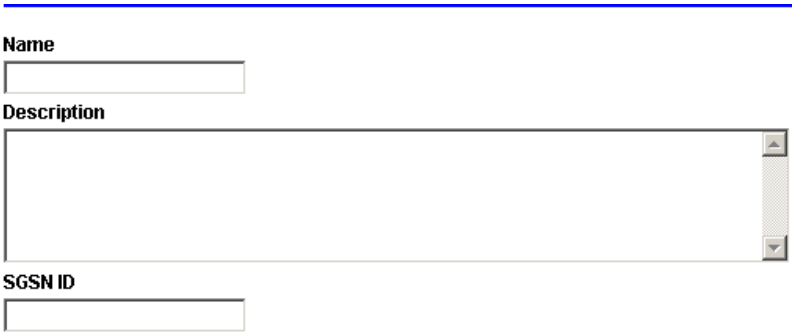


Figure 79: GPRS Signaling Points Add Screen

3. Type the **Name** of the signaling point.
4. (Optional) Type in a **Description**.
5. Type in a **SGSN ID** (this is the number that identifies the Serving GPRS Support Node.

   Note: The ID needs to be a positive integer.

6. Click **Add**. The GPRS signaling point is added to the Node.

Modifying a GPRS Signaling Point

Complete these steps to modify a GPRS signaling point.

1. Select the **GPRS signaling point** to be modified.
2. Select **Modify**.
3. Make the necessary **modifications**.
4. Click **Modify**.
   A prompt appears stating that the signaling point was modified.

Deleting a GPRS Signaling Point

Note: When deleting a signaling point, all links and linksets associated with that signaling point are also deleted.

To delete a GPRS signaling point, complete these steps.

1. Select the **GPRS signaling point** to be deleted from the list.
2. Select **Delete**.
3. Click **OK** at the prompt, the signaling point is deleted.

About IP Network Elements

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.

About IP Signaling Points

CCM enables you to configure IP signaling points. Like other signaling points, IP signaling points are discovered when the network is created. You can only modify, delete and filter IP signaling points.

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.

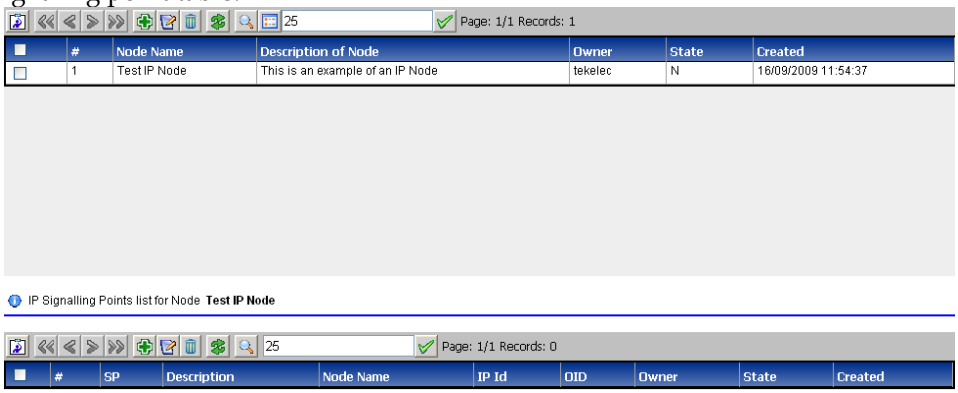


Figure 80: Add Signaling Point Screen

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 delete 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.

IP Card Functional Specifications

The PIC system supports both STC-style and Fast Copy on IMF with both Eagle IPGW as well as IPSG cards.

This table shows the functional expectations on a per card basis.
Note: The cards supported depend on the version of Eagle that is installed on the system. This list is for Eagle release 42.

Application	Hardware	GPL	Protocols	ANSI/ITU	Monitoring Type
SS7IPGW	SSEDCM	SS7IPGW	M3UA	ANSI	STC-STYLE
SS7IPGW	E5-ENET	IPGHC	SUA / M3UA	ANSI	STC-STYLE or Fast Copy
IPGWI	SSEDCM	IPGWI	M3UA	ITU	STC-STYLE
IPGWI	E5-ENET	IPGHC	SUA / M3UA	ITU	STC-STYLE or Fast Copy
IPSG	E5-ENET	IPSG	M2PA / M3UA	ANSI+ITU	STC-STYLE or Fast Copy

TABLE 52: IP CARD SPECIFICATIONS

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**.
6. 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: For IMF subsystems the network elements are automatically discovered and cannot be created manually. 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 **Destination 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 >Application Server**.
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. Associations provide 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 are discovered from an IMF subsystem but can exist as PMF (utilizing traffic classifications) elements. Network element associations are discovered as part of the site creation process.

Note: For IMF subsystems the network elements are automatically discovered and manual creation of elements is not allowed. On the other hand, all elements on a PMF subsystem require manual creation.

Showing Details of an Associations (IMF or PMF)

Complete these steps to show the details (endpoints, associations or links mapped to either an IMF or a PMF association.

1. **Select Network Elements > IP > Associations > IMF or PMF** (depending on what type of association is being researched).
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 (IMF and PMF)

Complete these steps to delete either an IMF or a PMF association.

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

1. Select **Network Elements > IP > Associations > IMF or PMF** (depending on what association needs to be deleted).
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: For IMF subsystems the network elements are automatically discovered and manual creation of elements is not allowed. On the other hand, 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 7: Network View Configuration

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 81: 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.

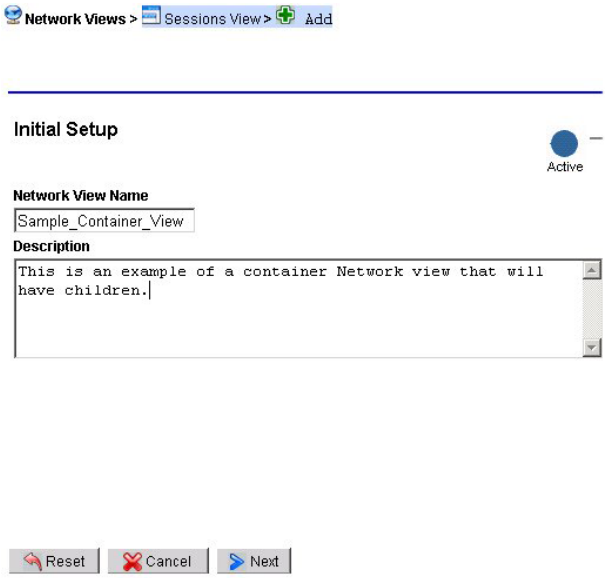


Figure 82: Initial Setup Screen

2. Type in **Network View Name**.
3. (Optional) Type in a **Description**.
4. Click **Next**.
   The *View Type Selection* screen opens shown below.

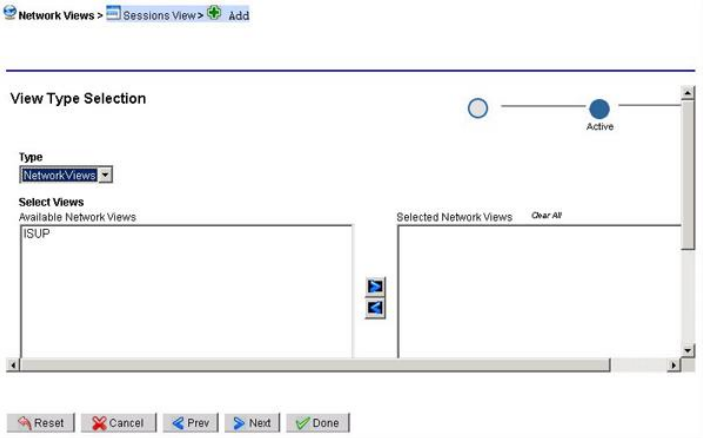


Figure 83: View Type Selection Screen

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. Select **Network View > Session Views > List**.
   The *Network View List* screen opens.

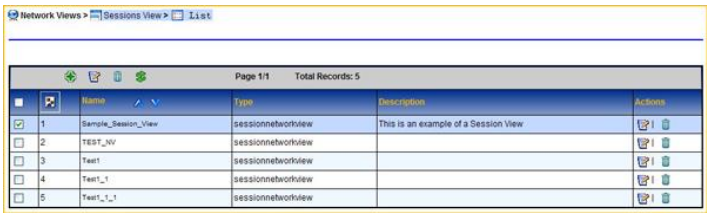


Figure 84: Network View List Screen

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.

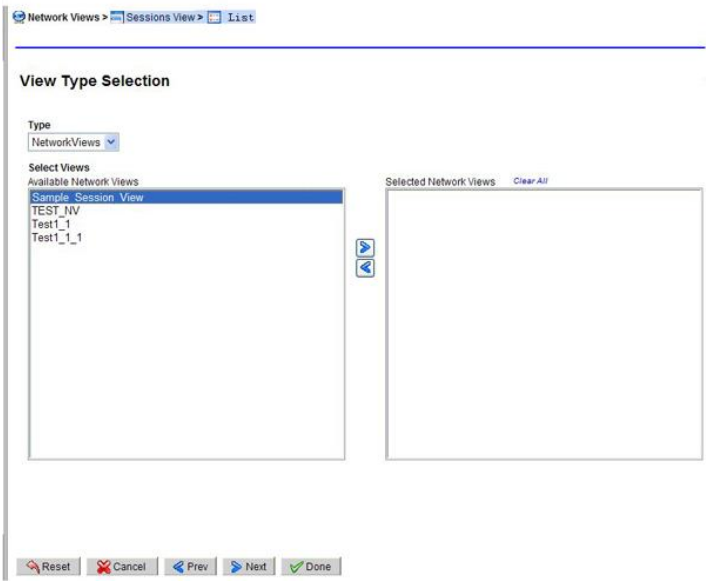


Figure 85: View Type Selection Screen

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 86: Network View Perspective

About Link-based Network Views

Link-based network views (SS7, Gb, IP) can be grouped together to create a view of the network that a system administrator uses for routing link data to the IXP. All links in an SS7 linkset are considered part of any network view containing the linkset. 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 three types of links 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.

- SS7
- GB
- Traffic Classifications (IP streams)

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.

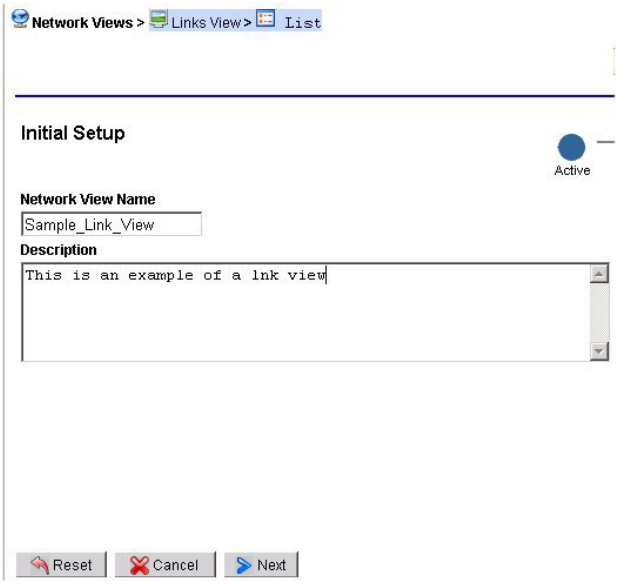


Figure 87: Link Network View Create Info-Initial Setup

2. Type in **Network View Name**.
3. (required) Type in a **Description**.
4. Click **Next**.
   The *View Type Selection* screen opens shown in Figure 88: View Type Selection Screen.
5. Select **Links** from the drop-down menu. The link type screen opens shown below.

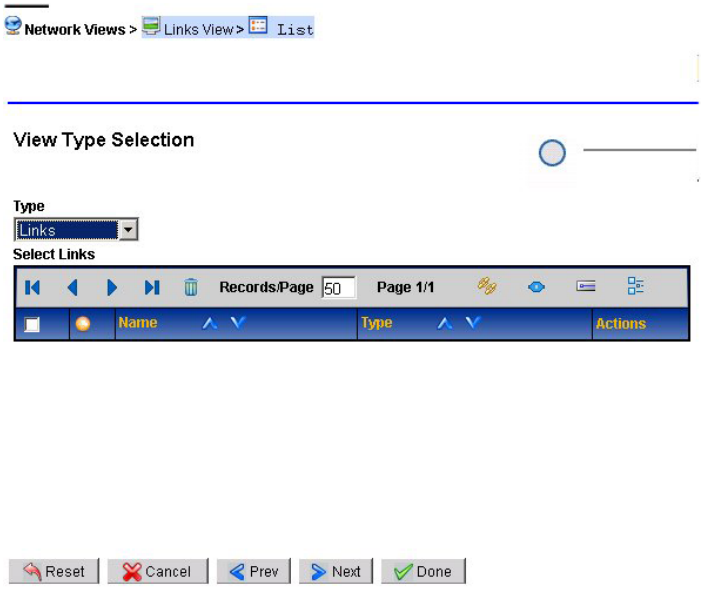


Figure 88: View Type Selection Screen

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

   Note: To add a specific linkset or link type, click on one of the links below.

   a. Adding an SS7 Linkset to a Link View
   b. Selecting Gb Links for a Link View
   c. Selecting Traffic Classifications
   d. Adding SS7 Linksets and Gb Links

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

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

TABLE 53: LINK NETWORK VIEW FIELDS

Adding an SS7 Linkset to a Link View

Complete these steps to add an SS7 linkset to your link view.

Item	Description
Point Code	List of available point codes
Type	Point Code type (A-F)
Resource ID	Alphanumeric field to declare an ID for the linkset
Sites	List field of available sites on point code
Apply Filter	Begins search for parameters selected above
Filtered SS7 Linksets	Lists linksets found.
Select & Close	Selects chosen links
Close	Closes the screen

TABLE 54: SELECT SS7 LINKSET SCREEN

1. Click **Select SS7 Linksets**

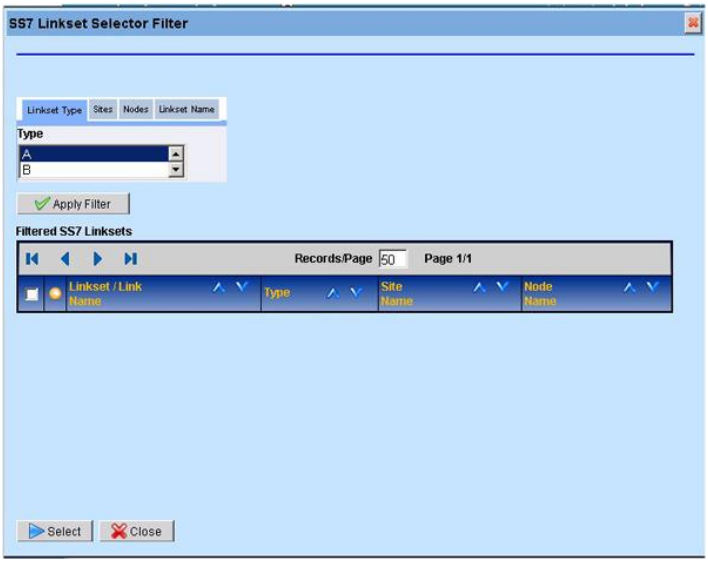


Figure 89: SS7 Linkset Selector Filter Screen

a. Select the **Linkset Type** from the Linkset type tab.
b. Select the **Site** from the Sites tab shown in the figure below.

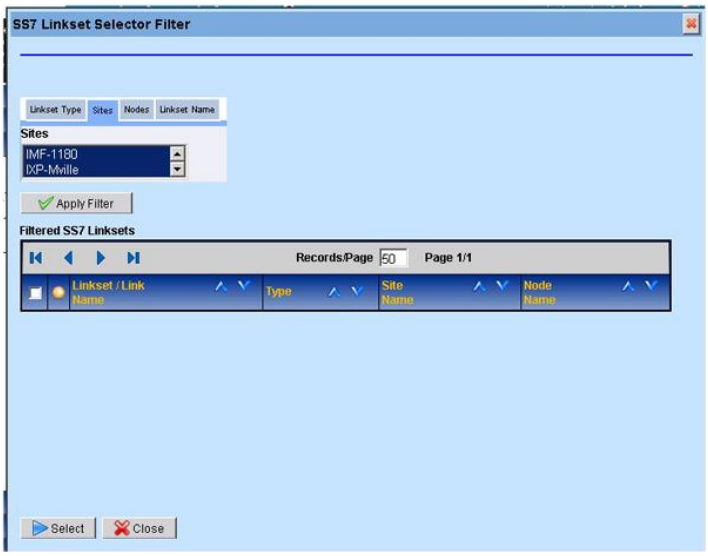


Figure 90: Sites Screen

c. Select the **Node(s)** from the Nodes tab shown in the figure below.

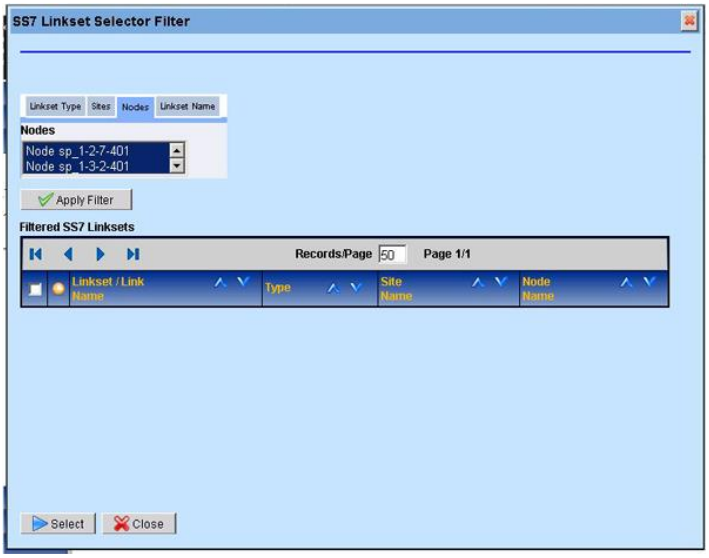


Figure 91: SS7 Node Screen

d. Assign a **Linkset Name** from the Linkset Name tab.

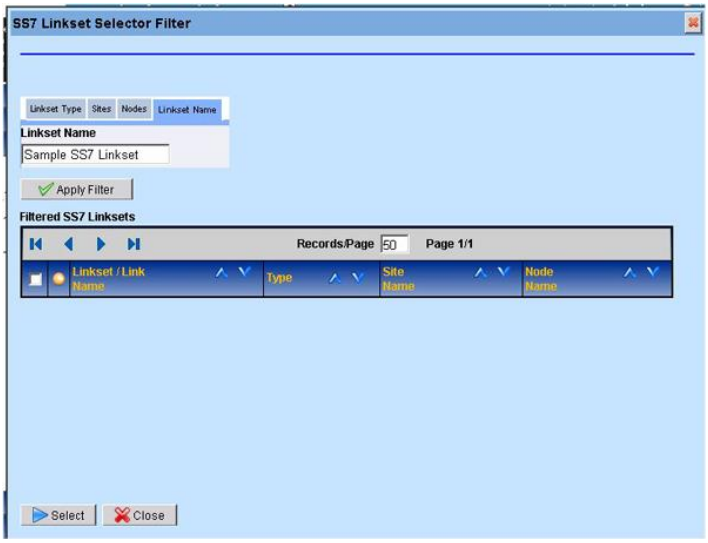


Figure 92: SS7 Linkset Name Screen

a. Click **Apply Filter** to apply the filter to the linkset.
b. Click **Select**.
The *View Type Selection* screen opens with the selected linkset(s).

2. Click **Close**.
The *SS7 linkset* is added to the link view.

Selecting Gb Links for a Link View

Complete these steps to select a Gb link to a link view.

1. Click **Gb link** from View Type Selection screen shown in Figure 93: View Type Selection Screen.
The *Gb Link Selector Filter* shown below opens.

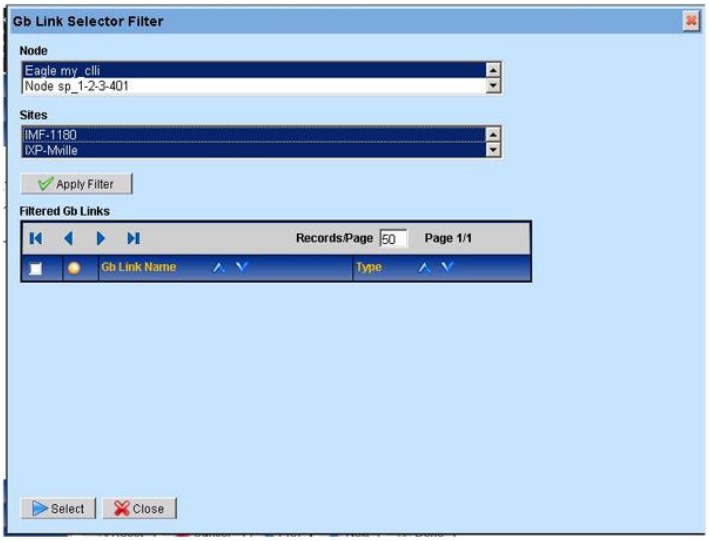


Figure 93: View Type Selection Screen

Item	Description
Node	Shows all the nodes within a network view
Sites	Shows all the sites available in a network view
Apply Filter	Begins search for available Gb links
Filtered Gb Links	Lists all the available links
Select & Close	Selects chosen links
Close	Closes the screen

TABLE 55: SELECT GB LINKS SCREEN

2. Select a **Node**.
3. Select the **Site(s)**.
4. Click **Apply Filter**.
   The search begins.
5. Select the **Gb links** for the link view.
6. Click **Select**.
   The Gb link is selected.
7. Click **Close**.
   The links are added to the network view.

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.

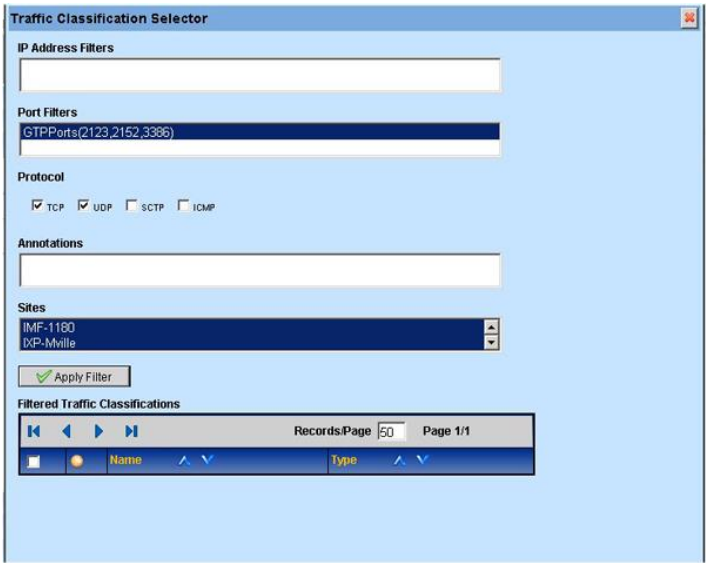


Figure 94: View Type Classification Screen

Item	Description
IP Address Filters	Lists available IP Addresses
Port Filters	Lists available Port Filters
Protocols	Check boxes for the following protocols • TCP • UDP • SCTP • ICMP
Annotations	A specific label or title you add for identification
Apply Filter	Begins search for Input streams
Traffic Classification List	Lists Traffic classifications found in search
Select	Selects chosen links
Close	Closes the screen

TABLE 56: IP STREAM SELECTOR FILTER FIELDS

2. Select **IP Address Filters** from the list.
3. Select the **Port Filters** from the list.
4. Select the **Protocol(s)** for the filter.
5. Click **Apply Filter** to begin the search for available traffic selections.
6. Select the **traffic classification** from the list.
7. Click **Save** to save the selection to the link view.
8. Click **Close** the screen closes.

Adding SS7 Linksets and Gb Links

Complete the following steps to add SS7 linksets & Gb links.

1. Click **Select SS7 and Gb links** from View Type Selection tree.
   The *Link Selector* filter opens.

Figure 95: Link Selector Screen

1. Expand the **Object Tree**.
2. Select the **Link**.
3. Click **Save & Close**.
   The *link* is selected.

Modifying Link-based Network Views

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

1. Select the **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. Select the **network view** to be deleted.
2. Select **Delete** from the popup menu.
3. Click **OK** at the prompt.
   The *session* is deleted.

Chapter 8: xMF Acquisition

About the Acquisition Perspective

Once an xMF (IMF/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 subsystems are visible in the Acquisition object tree (shown in the figure below). In this perspective you can:

- Create monitoring groups linked to monitor linksets
- Create PDU Filters
- Configure Alarms
- Manage Resource ID Groups
- Configure Q.752 counters (Routes Dataflows to Thirdparty ((external)) Data Feeds)

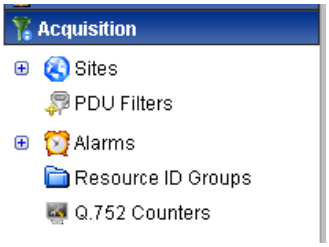


Figure 96: Acquisition Perspective Overview

About xMF Subsystem Management

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

The functions are briefly described in the table.

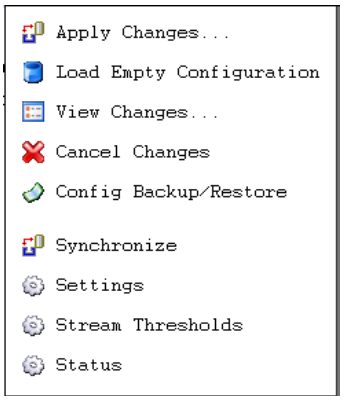


Figure 97: xMF Subsystem Pop-Up Menu

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

Option	Description
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. **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 xMF 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 xMF subsystem.
Status	Enables you to view the status of the system

TABLE 57: XMF SUBSYSTEM POP-UP MENU OPTIONS

Synchronizing an xMF Subsystem

Using the sychronize option, you can discover any new applications or changes to the xMF subsystem.

Complete these steps to sychronize an xMF subsystem.

1. Select **Acquisition > Sites > xMF subsystem (PMF or IMF)** shown below.

Figure 98: Selected XMF Subsystem

2. Right click on the **Subsystem**.
3. Select **Synchronize**.
   The system begins the process. After completion, the status screen opens shown in the figure below.

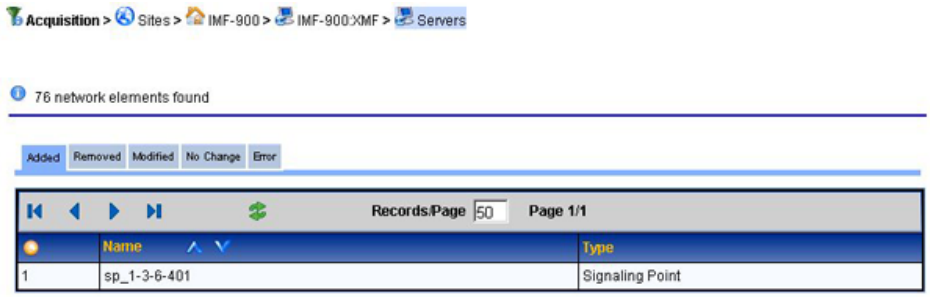


Figure 99: Synchronization Results Screen

You are provided the following information.

- How many elements were found in the subsystem
- What elements were added
- What elements were removed
- What elements were modified
- What elements had no changes
- Any errors that occurred during synchronization

In addition, if it is a PMF subsystem, then you are also notified as to how many cards were found.

Applying Changes to an xMF (IMF) Subsystem

Once changes have been made to an IMF subsystem, click **Apply Changes** on the subsystem right-click menu. The results screen opens:

Figure 100: Apply Changes Screen

The screen has two tabs.

- Configuration Changes - shows all the actions during the process.
- Warnings - shows the changes that may have errors.

Note: In the process of applying changes to an IMF subsystem, the changes are first validated to make sure that no limits have been exceeded. This is especially important for monitoring groups. If the maximum of 512 links and associations has been exceeded, when changes are applied, there will be a warning prompt that appears stating that there is an invalid or exceeded capacity of monitoring groups and it must be corrected before applying changes. The monitoring groups in question will be listed on the prompt. In this situation, the monitoring group(s) in question must be modified. For more information see Modifying Monitoring Groups.

Viewing Changes to an xMF Subsystem

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

1. Select **Acquisition > Site >xMF** 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 xMF Subsystem Automatic Failover

Complete these steps to enable or disable the automatic failover for an xMF subsystem.

1. Select **Acquisition > Site > xMF 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 effect, click **Apply Changes**.

Loading an Empty Configuration on to an xMF 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 xMF subsystem. (For more information, see Avoiding Lost PDU Routes Due to Cancel Changes on an xMF 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 xMF Subsystem

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

Note: Choosing "Cancel Changes" on an xMF subsystem removes the existing configuration (any changes that have occurred) of that subsystem and restores the latest applied (active) configuration which includes Monitoring Groups in the case of IMF or Card/Port/Link Mapping and Traffic Classifications (TCs) in the case of PMF. Feeder Thresholds, xMF subsystem parameters and PDU dataflows are preserved (but the PDU routes are not preserved). This action also enables the "Apply Changes" banner for that xMF 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 NSP Config Manager or NSP Administrator.

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 xMF 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 xMF subsystem is reloaded.
4. Click **Apply Changes** for the xMF subsystem.
   To avoid loss of PDU Routes on the IXP subsystems associated with the xMF subsystem follow steps 5-8.
5. Select the **IXP Subsystem** associated with the xMF 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 (see Restoring Lost PDU Routes Due to Cancel Changes on an xMF Subsystem).

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).
- 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)
- ThresholdKbps - sets the threshold for Kbps for a subsystem

  Note: For ThresholdKbps values, it is recommended that the value range be:

- 100,000 - 500,000 Kbps for a system that has no disk storage
- 10,000 - 50,000 Kbps for a system that has disk storage
- UseGTPFilters - Enables and disables GTP post filtering on PMF. It has two setting values, 0=Disable and 1=Enable. (Enable is the default.)

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 for you to view and edit some xMF parameters on a per-subsystem basis. Initially, the following are the ranges for pre-defined 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	100,000	ThresholdKbps = maximum allowed throughput of xmf AFTER PMIA filtering. If exceeded, the system will start to drop MSUs to protect itself.
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.

Parameter	Default Values	Comment
		Recommended for IMF and PMF/E1T1

TABLE 58: RANGES FOR PRE-DEFINED SUBSYSTEM PARAMETERS

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.

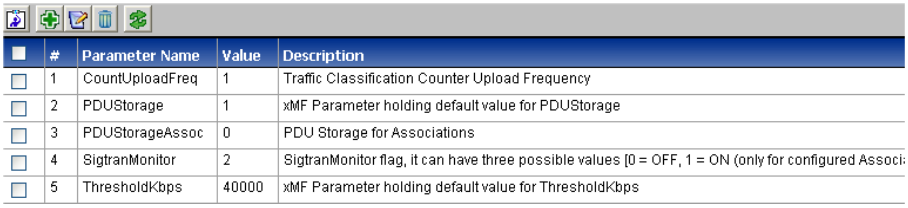
  Note: If IP RAW data should be stored to the disk, then both PDUStorage and PDUStorageAssoc must be enabled. If disabled, the monitored data is stored only to RAM.
- PDUStorageAssoc - the default setting is disabled. If this parameter is enabled, then IP RAW data is stored to the disk.

  Note: This parameter is valid only if PDUStorage is enabled. If it is disabled (default setting), then the monitored IP RAW data 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 101: xMF Subsystem Settings List Screen

3. Click Add on the tool bar.
   The *Add* screen opens.

Figure 102: xMF Subsystem Parameter Add Screen

4. Enter the **Name** of the parameter.
5. Enter the **Value** (integer).
6. (Optional) Enter the **Description**.
7. 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.

1. Select **Acquisition > Sites > xMF** subsystem that needs modification.

2. Right click and select **Settings**.
   The *Settings List* screen opens.
3. Select the **parameter** to be modified.

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

4. Click **Modify** on the tool bar.
   The *Modify* screen opens.
5. (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 xMF subsystem Status

Complete these steps to view the status of subsystem applications.

1. Select the **xMF subsystem** that will have the setting.
2. Select **Status** from the pop-up menu.
3. The *Status List* screen opens.

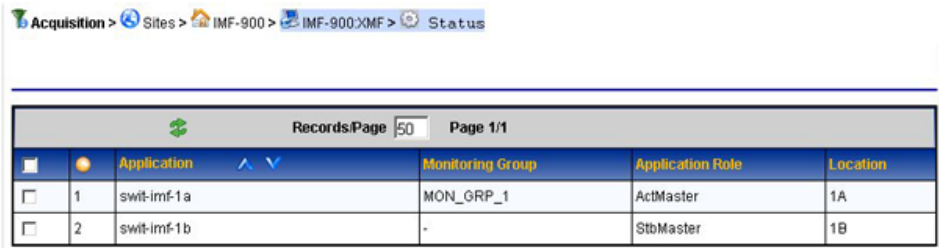


Figure 103: xMF Stream Threshold List Screen

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

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%
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%
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%
mflnHoldOn	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%

TABLE 59: THRESHOLD VALUES

Setting Stream Thresholds

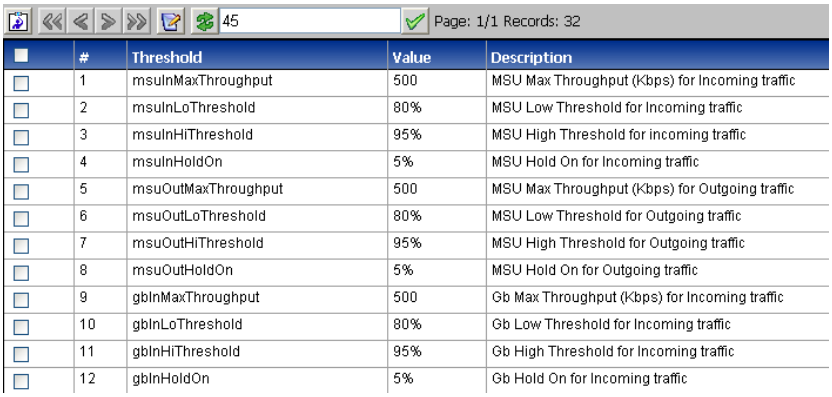
Stream thresholds enable you to set the limit for traffic passing through different Destinations within an xMF subsystem. In CCM you set these limits using the stream threshold option.

Stream threshold alarms are raised for every Stream whenever the traffic for that Stream crosses the specified threshold. The percentages that you set are for the high and low thresholds for the maxThroughput value (the limit of traffic passing through xMF server), that you define for every Stream.

Note: Because thresholds can vary according to the size of your system, it is recommended that you contact your Tekelec representative to set the percentages most compatible for your system.

Complete these steps to set a subsystem stream threshold.

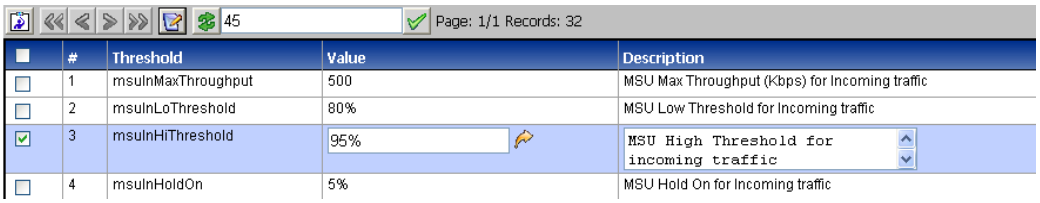
1. Select the **xMF subsystem** or server that will have the setting.
2. Select **Stream Thresholds** from the pop-up menu.
   The *Stream Thresholds List* screen opens.



	#	Threshold	Value	Description
☐	1	msuInMaxThroughput	500	MSU Max Throughput (Kbps) for Incoming traffic
☐	2	msuInLoThreshold	80%	MSU Low Threshold for Incoming traffic
☐	3	msuInHiThreshold	95%	MSU High Threshold for incoming traffic
☐	4	msuInHoldOn	5%	MSU Hold On for Incoming traffic
☐	5	msuOutMaxThroughput	500	MSU Max Throughput (Kbps) for Outgoing traffic
☐	6	msuOutLoThreshold	80%	MSU Low Threshold for Outgoing traffic
☐	7	msuOutHiThreshold	95%	MSU High Threshold for Outgoing traffic
☐	8	msuOutHoldOn	5%	MSU Hold On for Outgoing traffic
☐	9	gbInMaxThroughput	500	Gb Max Throughput (Kbps) for Incoming traffic
☐	10	gbInLoThreshold	80%	Gb Low Threshold for Incoming traffic
☐	11	gbInHiThreshold	95%	Gb High Threshold for Incoming traffic
☐	12	gbInHoldOn	5%	Gb Hold On for Incoming traffic

Figure 104: Stream Threshold List Screen

3. Select the **Stream** to be set.
4. Click **Modify** from the tool bar.
   The *Stream Threshold Modify* screen opens.



	#	Threshold	Value	Description
☐	1	msuInMaxThroughput	500	MSU Max Throughput (Kbps) for Incoming traffic
☐	2	msuInLoThreshold	80%	MSU Low Threshold for Incoming traffic
☑	3	msuInHiThreshold	95%	MSU High Threshold for incoming traffic
☐	4	msuInHoldOn	5%	MSU Hold On for Incoming traffic

Figure 105: Stream Threshold Parameters Screen

5. Set the **Value** for the selected threshold.
6. Click **Apply**.
   The *stream threshold* is modified.

About xMF Applications

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

- Modify an application
- Delete an application
- Manage applications

Adding an E1/T1 (SPAN) Card (PMF)

If E1/T1 cards are being used for a PMF system, these cards have to be manually added and configured.

These procedures are performed from the Acquisition perspective. Complete these steps to add an E1/T1 SPAN card to a PMF subsystem.

1. Select **Acquisition > Site (with PMF subsystem) > subsystem > Server > Cards**.
2. Select **Add** from the pop-up menu.
   The *Add Card* screen appears.

Figure 106: Add Card Screen

3. Select the **Slot Number**.
4. Select the **Hardware Type** to SPAN.
5. Select the **Software Mode**.
   - SS7-T1
   - SS7-E1
   - GB-E1
   - GB-T1
6. Modify the various **parameters** in the port.
7. Select the **Admin. State** (enable/disable).
8. Click **Create** for the Linkset.
   The card is created.

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

Configuring E1/T1 Cards (PMF)

After you have created a PMF subsystem and discovered its applications, you can configure the PMF applications. Complete these steps to configure a PMF application (E1/T1 Span Card).

1. Select **Acquisition > Site (with PMF subsystem) > PMF Subsystem > Server > Cards**.
2. Select the appropriate **Card**.

   Note: E1/T1 Cards will be labeled in numerical order with name of SPAN, for example 1: SPAN.

3. Right-click on the **Card**.
4. Click **Modify**.
   The *Card* screen opens showing the cards ports.

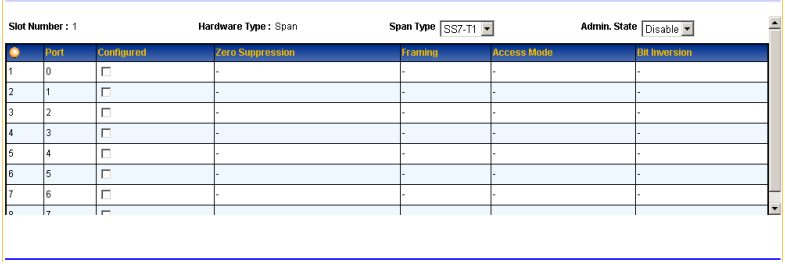


Figure 107: Span Card Screen with Unconfigured Ports

5. Select the port you want to configure by clicking the check box in the Configured column.
   The screen changes to show configurable parameters such as Zero Suppression, Framing, Access Mode and Bit Inversion along with the Channel Link Mapping screen for that port.

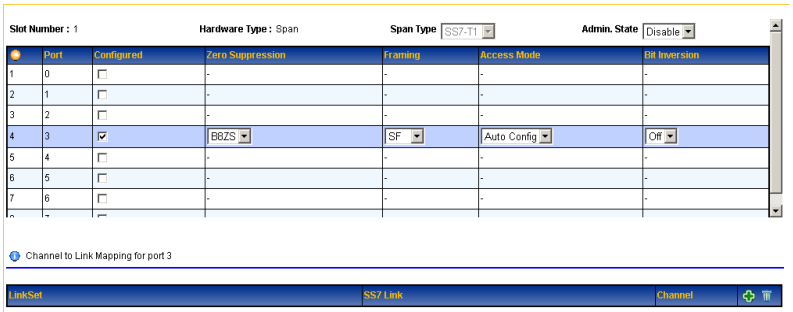


Figure 108: Span Card Configure Screen with Channel Link Mapping Section

6. Modify the various **parameters** in the port.
7. Click the **Add** icon on the tool bar in the Channel to Link Mapping section.

   Note: Only unmonitored links (SS7 and Gb) are shown.

   Note: Other PMF configurations such as site configuration, discovery, network elements (linkset and link), traffic classifications and PDU data flows remain unchanged and remain consistent across the PMF subsystem.

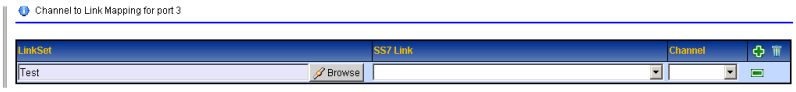


Figure 109: Span Card Configure Screen with Channel Link Mapping Add Screen

8. Click **Browse** for the Linkset.

   Note: You can also use the "auto complete" text box to search the linksets or Gb links quickly if you know the name.

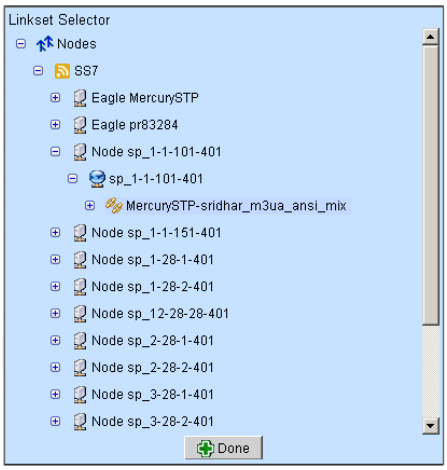


Figure 110: Span Card Configure Screen with Channel Link Mapping Add Screen

When you have selected the linkset, click **Done**.

9. Select the **Link** associated with the linkset.
10. Select the **Port** associated with the linkset.
11. Click **Modify**.
    The card port is configured.

    Make sure to apply the changes to the subsystem when you have finished using the subsystem right-click menu.

Modifying xMF Applications

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

Deleting xMF Applications

Complete the following steps to delete an xMF application.

Note: You cannot delete an IMF application where number of IMF monitoring groups is less than or equal to the number of operational IMF servers.

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 > xMF subsystem > Host > Application**.
2. Select the **application** from the IMF or PMF to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.
   The application is deleted. You must then synchronize the subsystem for the changes to take effect in the system.

About Monitoring Groups (IMF)

A Monitoring Group is used to configure a IMF to monitor specific Linksets and/or Associations.
Once a Linkset/Association is part of a Monitoring Group, the IMF instructs the Eagle to send MSUs/PDUs to the IMF for capturing. When Linksets and/or Associations are monitored by the IMF, the IMF captures the MSUs/PDUs received from Eagle and forwards these to the IXP for processing/storage based on PDU Data Flows Configurations on IMF and Dataflow Processing Configurations on IXP.

Monitoring Groups support Associations for *SigTran Fast Copy* capability. This capability provides efficient configuration and maintenance of the IMF subsystem by integrating it with the Eagle without impacting the internal Eagle IMT bus. In addition, the SigTran data is monitored in real time, similar to the port mirroring with PMF, again with no internal impact to the IMT bus. For more information on supporting and configuring Fast Copy, refer the documentation for Eagle.

Note: Since monitoring groups must be associated with a linkset, you must have existing linksets before you can assign a monitoring group.

Note: Linksets that have not been associated with any monitoring group will not be monitored. It is recommended that when creating an association, you also monitor the other links in the linkset(s).

The monitoring group list page has five columns:

- Groups listed for a site - shows the record number of the monitoring group
- Group Name - shows the name of the monitoring group
- Description - shows a short description of the group (optional).
- Number Links - shows the number of monitored linksets
- Number Associations - shows the number of monitored associations

Automatic Failover Capability

IMF has an automatic failover capability to reduce PDU loss in case of server hardware failure.
Whenever an IMF server fails, the IMF subsystem automatically shifts all the linksets/links monitored by the failed server to an available spare server within the subsystem. In order to support this feature, there needs to be one IMF server (spare) that does not have a monitoring group assigned to it.

The maximum number of monitoring groups you can configure is *equal to the number of servers available in the subsystem*. You can assign linksets to each monitoring group. A linkset can be assigned to only one monitoring group. You can also configure *n-1 monitoring groups* (n is the number of servers), to guarantee one server being available for failover.

Enabling or Disabling Subsystem Failover

Described here are the steps to disable or enable the automatic IMF subsystem failover for a specific IMF subsystem.

Note: The subsystem default is **Enabled**.

To disable an IMF subsystem failover complete the following:

1. Select **Acquisition > Sites >xMF (IMF)** subsystem.
2. Right-click on the **Subsystem**.
3. Select **Disable**.
4. Click **Done**.
5. **Apply Changes** for that subsystem.

   Note: To enable the disabled subsystem failover operation, select **Enable** in step 3.

Considerations When Working with STC/Fastcopy

The following is a list of points one should consider when working with the STC/Fastcopy feature:

- Existing STC links that are monitored remain in the same Monitoring Group.
- Monitored links which were part of an association and are changed back to STC copy will remain in the same Monitoring Group if the linkset belongs to the same Monitoring Group.
- Monitored links that are part of an association and are changed back to STC copy will switch to the same Monitoring Group as part of the linkset if the linkset belongs to a different Monitoring Group.
- Any un-monitored links which are part of an Association and are changed back to STC copy will be added to the same Monitoring Group as the linkset.
- The monitoring group panel in CCM does not show association as a possible selection to monitor if the association no longer contains Fast Copy links. However, the linkset(s) will be available as a possible selection.
- Un-monitored links that switch from STC to an association will be added to the same Monitoring Group as the Association if the association is monitored.
- The Monitoring Group panel is CCM does not show a linkset as a possible selection if all the links in the linkset belong to association(s). However, the Association(s) will be available as a possible selection.
- If a Monitoring Group no longer contains any links, then the Monitoring Group is automatically deleted.
- If a Dataflow no longer contains any links, then the Dataflow is automatically deleted.
- If the movement of linksets or Associations from one Monitoring Group to another results in removal of all routes in one or more Dataflows, then those Datflows are deleted automatically. You will then need to create new or modify existing Dataflows in order to re-route the linksets or Associations.
- Dataflows may need to be modified or added in order to accommodate automatic Monitoring Group changes. The routes within the existing Dataflows may be removed automatically, but may need to be added manually by selecting the necessary linksets or associations.
- The Dataflow Processings and Streams will not be modified or removed automatically due to any automatic changes to Dataflows during the STC-FC switching, although you may need to manually modify or remove the Dataflow Processings later.
- Because associations are included in the calculation of Monitoring Group capacity, it is possible for some of the links that changed from STC to FC to be monitored after the discovery process. For example, the Monitoring Group capacity for a linkset containing 3 M2PA associations and 12 STC links would equate to 18. Therefore, it is highly recommended that after synchronizing the IMF that the Monitoring Groups, Dataflows and number of streams should be verified of changes prior to applying changes to the IMF subsystem. The verification also applies to the load balance on IMF based on Monitoring Groups, Dataflows, and Streams.

- Make sure that you apply changes in CCM when converting STC to Fast Copy or Fast Copy to STC because of the possibility of traffic loss during the synchronization period up until you have applied all changes to the subsystem (modifying or removing Dataflows and Monitoring Groups).

Adding a Monitoring Group (IMF)

Complete these steps to add a Monitoring Group to an IMF subsystem.

1. Select **Acquisition > Sites > Host > xMF (IMF)** subsystem > Server > Monitoring Group.
   The *Monitoring Groups List* screen opens.
2. Click **Add** from the toolbar.
   The *Monitoring Group Add* screen opens.

   Note: There must be monitored links and associations present for the Monitoring Group to be created. If no linksets or Associations are present, they must be added and then the changes applied to the IMF Subsystem.

Field	Description
Group Name	Provides the name of the monitoring group that is being added.
(Optional) Description	Provides some useful information about the monitoring group.
Linksets and Associations Notation	Shows the number of linksets and associations that belong to the IMF subsystem.
Linksets Tab	Shows un-monitored and monitored linksets on the IMF server.
Associations Tab	Shows un-monitored and monitored associations on the IMF server.
Cards Tab	Shows un-monitored and monitored cards on the IMF server.
Reset Button	Resets the screen back to its default status.
Cancel Button	Cancels any changes in progress.
Add Button	Adds the monitoring group to the IMF server.

TABLE 60: ADDING MONITORING GROUP

3. Enter the **Group Name**.
4. (Optional) Enter a **Description**.
5. Select the **Un-monitored Linksets** that will belong to the Monitoring Group.

   Note: Each linkset is listed by name and how many STC links and associations it has. The notation is:

   ```
   linksetname (STC=<n>,ASSOC=<n>)
   ```

   For example,

   ```
   s1cssg-lsto12551 (STC=2,ASSOC=0)
   ```

6. Click the **right arrow** to move the linkset(s) to the monitored linksets field.
7. Click the **Associations** Tab and select the un-monitored association(s).
8. Click the **right arrow** to move the selected association(s) to the monitored field.
9. Click the **Card Tab** and select the un-monitored card(s).
10. Click the **right arrow** to move the selected card(s) to the monitored field.
11. Click **Add**.
    The *Monitoring Group* is added to the list.

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

    Note: You can assign both linksets and associations to a Monitoring Group when you are monitoring more than just SS7 linksets such as SigTran Links.

Moving Linksets and Association Monitoring

This feature provides a shortcut for moving linksets, associations and cards from one Monitoring Group to another.

Complete these steps to move elements of one monitoring group to another Monitoring Group.

1. Select **Acquisition > Sites > xMF (IMF)** subsystem.
2. From the Actions column select **Move Linkset and Association Monitoring** (the icon on the right side of the column).
3. Click the **Tab (Linkset, Association, Card)** for the element that is to be moved.

   Note: Default tab is Linkset.

   This table describes the Move Linkset and Association Monitoring screen columns.

Column	Description
Selection	Provides a check box to select the linkset, association or card.
#	Shows the record number of element within the table.
Component (Linkset, Association, Cards)	Shows the name of the element.
Monitoring Group	Shows the monitoring groups in the system along with a radio button showing what monitoring group the element belongs to. **Note:** The network signaling element(s) will have the monitoring group radio button selected based on the current configuration.

TABLE 61: MOVE LINKSET AND ASSOCIATION MONITORING SCREEN

4. Select the **Element(s)** to be moved.
5. To choose the new Monitoring Group for the selected element(s), click on the **Radio Button** under the desired Monitoring Group heading.

   Note: The list of available Monitoring Groups is based on what has been previously configured. It is therefore possible for the list of monitoring groups to be empty or only have a single Monitoring Group.

6. Click **Done**.
7. Repeat steps 3-6 for each element (Linkset, Association or Card) to be moved.
   For the changes to take effect, right-click on the subsystem and select **Apply Changes**.

Modifying a Monitoring Group (IMF)

Complete these steps to modify a Monitoring Group.

1. Select **Acquisition > Sites > xMF (IMF) subsystem > Server > Monitoring Group**.
2. Select the **Monitoring Group** from the list.
3. Click **Modify**.
   The *Monitoring Group* screen opens.
4. Make the necessary **Modifications**.
5. Click **Modify**.
   For the changes to take effect, right-click on the Subsystem and select **Apply Changes**.

Deleting a Monitoring Group (IMF)

Complete these steps to delete a monitoring group.

Note: To delete a Monitoring Group, the links assigned to that group have to be unassigned before the Monitoring Group can be deleted.

1. Select **Acquisition > Sites >xMF (IMF) subsystem > Server > Monitoring Group**.
2. Select the **Monitoring Group** that is to be deleted.
3. Click **Delete**.

4. Click **OK** at the prompt.
   The Monitoring Group is deleted. You need to **Synchronize** the Subsystem for the changes to take effect.

About Associations (IMF)

Associations refer to SCTP associations within a SIGTRAN (SS7 over IP) network. An association provides the transport mechanism for the delivery of SCCP-User protocol data units and SUA layer peer messages. Associations are similar to a TCP connection, because they support multiple IP addresses at either or both ends (multi-homing). In addition, associations support multiple logical streams (multi-streaming) as well as provide sequenced delivery for user datagram within a single input stream.

Adding an Association (IMF)

Complete these steps to add an association to a Monitoring Group.

1. Select **Acquisition > Sites >xMF (IMF) subsystem > Server > Monitoring Group** to open the Monitoring Group screen.
2. Click **Add** from the tool bar.
   Alternative procedure: **Select Acquisition > Sites > xMF (IMF)** subsystem. **Right-click** on Monitoring Group and select Add.
3. Enter the **Group Name**.
4. (Optional) Type a **Description**.
5. Click the **Associations** tab.
   The *Associations* screen opens showing all un-monitored associations.
6. Select one or more **un-Monitored Associations**
7. Click the **right arrow** to place the Un-monitored associations to the Monitored Associations field.

   Note: The bottom field (Un-monitored Linksets and Associations) shows those elements that are un-monitored but are part of the monitored linkset/Association. This list appears when a linkset is monitored but the Association is not (and vice versa). It is recommended that these related elements be monitored together so as to keep all linksets and Associations in the same group.

8. Select the **Cards** tab.
9. Select one or more **Cards** from the Un-monitored Cards section.
10. Click the **right arrow** to place the Un-monitored Cards to the Monitored Cards field.
11. Click **Add**.
    The monitoring group with associations 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.

About Traffic Classifications (PMF)

A Traffic Classification on PMF is similar to a Monitoring Group on an IMF because the settings made for a Traffic Classification are used by the PMF 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 similar to a Monitoring Group on an IMF in that a Traffic Classification is used by the PMF to process the captured MSUs/PDUs received from the IP probe. 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.

PIC filters IP traffic on the protocols.

- TCP
- UDP
- ICMP
- SCTP
- RTP

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

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 & SS7Tranport) 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:

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.
Duplicate Suppression	Tells whether duplicate IP suppression is activated/deactivated

TABLE 62: TRAFFIC CLASSIFICATION FIELDS

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: If ICMP is selected, no transport or application layers are utilized. Proceed to step 8.)

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.

    Note: To configure Duplicate IP Packets Suppression on a traffic classification Please refer Duplicate IP Packet Suppression Configuration

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: To activate/deactivate Duplicate IP Packets Suppression on a traffic classification Please refer Duplicate IP Packet Suppression Configuration

Note: You must **Apply Changes** to the PMF subsystem for the changes to take effect.

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 effect.

Start capture feature for a Traffic Classifications

1. Select **Acquisition > Sites > PMF subsystem > Host > Application > Traffic Classifications**. The List screen opens.
2. Select the **Ethereal Capture configuration** from the tool bar.
3. The List of active traffic classifications opens and gives current status of capture feature for each traffic classifciation.
4. Select the traffic classification(s) and click on **Start Ethereal Capture** button on the tool bar.
5. Click **OK** at the prompt.
   The **Capture Status** is: Capture is running on PMF [**PMF server name**] and pcap files will be available at */tekelec/capture/completed*
6. When capture is completed, upload the file in */tekelec/capture/completed* from PMF server by using SSH access

Note: the changes takes effect without making an **Apply Changes**.

Stop capture feature for a Traffic Classifications

1. Select **Acquisition > Sites > PMF subsystem > Host > Application > Traffic Classifications**. The List screen opens.
2. Select the **Ethereal Capture configuration** from the tool bar.
3. The List of active traffic classifications opens and gives current status of capture feature for each traffic classifciation.
4. Select the traffic classification(s) on which capture has been enabled and click on **Stop Ethereal Capture** button on the tool bar.
5. Click **OK** at the prompt.
   The Capture Status is: Capture is not running on PMF [**PMF server name**] and pcap files will be available at */tekelec/capture/completed*
7. Upload the file in */tekelec/capture/completed* from PMF server by using SSH access

Note: the changes takes effect without making an **Apply Changes**.

Modify capture feature Parameters

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

2. Select the **Ethereal Capture configuration** from the tool bar.
3. The List of active traffic classifications opens and gives current status of capture feature for each traffic classifciation.
4. Click on **Capture Parameters** button on the tool bar.
   The capture parameters screen opens:
   - **Capture File Location**: indicates the path where the competed captured are stored on PMF (read only)
   - **File Size In MB**: size of the capture files in Mbytes, default: 10 (read/write)
   - **Auto Rollover**: enable or disable the auto rollover function. If enable, then continue the capture when **File Size In MB** has been reached by removing oldest file in a circular manner. By default, auto rollover function is disabled and the capture is stopped when **File Size In MB** has been reached.
5. Click **Update** to validate the changes.
6. Click **Close**.

   Note: Capture parameters have been modified and will be taken into account during subsequent startup of capture process.

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.

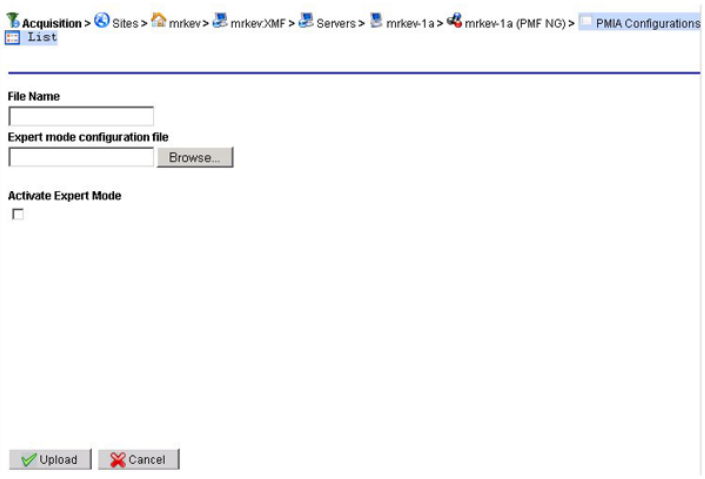


Figure 111: PMIA Screen

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 *PMIA 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 (IMF/PMF) to IXP. You create a DTS transport that defines the route (the IP address and protocol derived from the DTS datasource (an IP address and port on an IMF or 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.

Figure 112: DTS List Screen

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

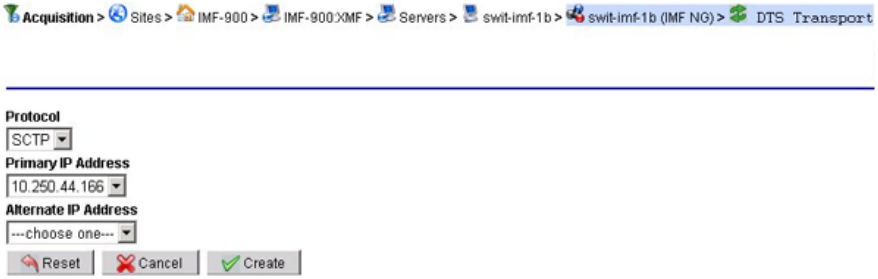


Figure 113: DTS Add Screen

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 four protocol types: SS7, IP, GPRS Gb and SIGTRAN protocols. These protocols 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 PIC, 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.

- GPRS Gb Protocol Filters
  - DLCI
  - SAPI
  - Combination
- IP Protocol Filters
  - PORT
  - IP Address
  - Combination
  - SAPI
  - VLAN
- SS7 Protocol Filters
  - SSN
  - PC
  - GT
  - Combination
  - RAW
- SigTran Protocol Filters
  - Association
  - SS7 Protocol
  - Combination
- SigTran SS7 Protocol Filters
  - Point Code (PC)
  - Service Information Octet (SIO)
  - Global Title Filter (GT)
  - Subsystem Number (SSN)

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

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

TABLE 63: MSU AND EMP CORESSPONDANCE VALUES

About SS7 Subsystem Number (SSN) Filters

SSN Filters are designed to filter PDU data related to one or more subsystem numbers.

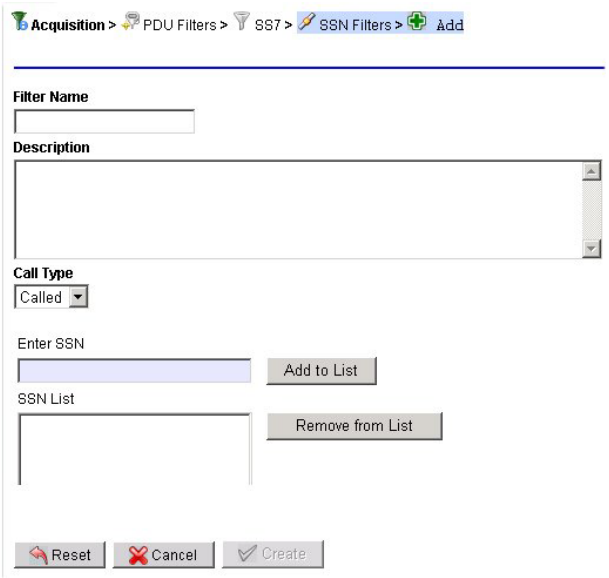


Figure 114: Add SSN Filter Screen

About SS7 Filters

There are five types of SS7 Filters:

- SSN: Filters for data associated with one or more subsystem numbers
- Point Code: Filters for data with one or more point codes, or a point code range.
- Global Title: Filters for data associated with one or more full or partial phone numbers.
- Combination: Filters for data based on any combination of the other four SS7 Filter types.
- Raw: Free-format Filter that allows a user to configure filter criteria.

Adding an SSN Filter

1. Select **Acquisition > PDU filters > SS7 > SSN filters**.
2. Click **Add** from the *right-click* menu.
3. (Optional) Enter a **Description**.
4. Enter in the **Filter Name**.
5. Select the **Call Type** (Called, Calling or Both)

6. Type in the **SSN** in the Enter SSN field.
7. Click **Add** to List.
   The *SSN* appears in the SSN List field.
   To add multiple SSN's to a filter, repeat steps 6-7.
8. Click **Create** to accept the values.
   The *SSN Filter* is added to the object tree.

Add SSN Filter Field Descriptions

Field	Description
Filter Name	User assigned filter name. Clicking on this opens the Add / Modify SSN Filter screen.
Call Type	Indicates call direction it can be: • called • calling • both
Enter SSN	This field is for typing in a Sub System Number
Add to List	Clicking on this adds the SSN to the SSN List.
Remove from List	Clicking on this will remove the SSN from the SSN List.
Create	Clicking on this saves the information entered.

TABLE 64: ADD SSN FILTER SCREEN FIELDS

Removing a SSN from an SSN Filter List

To remove an SSN from the *SSN List* list, complete these steps.

1. Select the **SSN** from the list
2. Click **Remove from List**.
   The SSN is deleted from the list.
3. Click **Create/Modify**.

Modifying an SSN Filter

1. Select **Acquisition > PDU filters > SS7 filters > SSN** from the object tree.
2. Click **Modify** from the *right-click* menu.
   The *Modify* screen opens
3. Make the appropriate **Modifications**.
4. Click **Modify**.
   The changes are saved.

Deleting an SSN Filter

Note: You cannot delete an SSN Filter is there are any Dataflows associated with it. You must first delete the Dataflow(s) and then delete the filter.

1. Select **Acquisition > PDU filters > SS7 filters > SSN** from the object tree.
2. Click **Delete** from the *right-click* menu.
3. Click **OK** at the prompt.
   The *Filter* is deleted.

   Note: All the PDU Dataflows using this filter are affected by the change.

About Global Title (GT) Filters

Global Title Filters specify data associated with one or more full or partial phone numbers.

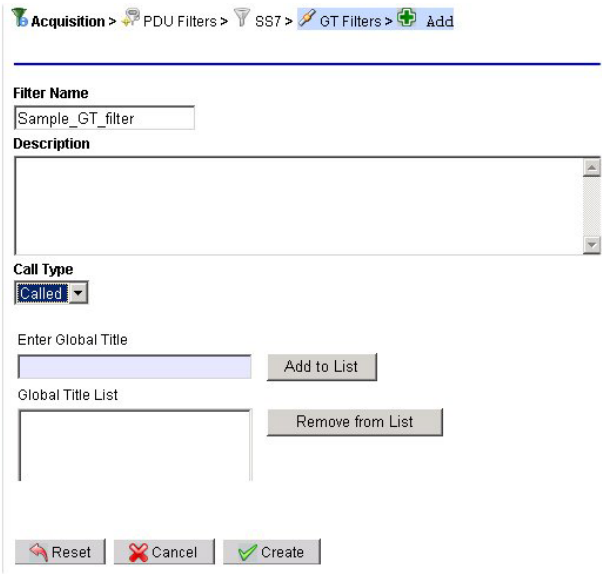


Figure 115: Global Title (GT) Filter

The table describes the fields on the Add Global Title Filter screen.

Field	Description
Filter Name	User assigned Global Title filter name.
Call Type	Indicates call direction. • Calling: Global Title is associated with the party that made the call. • Called: Global Title is associated with the party that was called. • Both: Associates with both call and called
Enter Global Title	Type in a numeric value, or a numeric value ending with * (wildcard).
Add to List button	Adds data entered in the Enter Global Title field to the Global Title list field.
Global Title List	Shows all of the Global Title values assigned to the same Global Title filter. Values can be added to or deleted from this list.
Remove from List button	Removes highlighted Global Titles from the Global Title List field. Multiple Global Titles can be removed at the same time.
Create button	Saves information entered.

TABLE 65: ADD GLOBAL TITLE FILTER SCREEN FIELDS

Adding a GT Filter

Complete these steps to add a GT Filter.

1. Select **GT Filters** from the SS7 submenu.
2. Click **Add** from the submenu.
   The *Add Global Title Filter* screen opens.
3. Type in the **Filter Name**.
4. Select the **Call Type** from the drop-down menu (Called, Calling, Both).
5. Type in a **Global Title** name.
   (Or select one from an existing list by typing the first letter of the global title.)
6. Click **Add** to List.
   The title is added to the list.
7. Click **Create**.
   The title appears in the GT filter object-tree list in alphanumerical order.

   Note: To add more than one title, repeat steps 5-7.

Modifying a GT Filter

Complete these steps to modify GT Filter.

1. Select the **GT Filter** that needs modification.

2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The changes are saved.

Deleting a GT Filter

Complete these steps to delete a GT Filter.

1. Select the **Resource ID Group** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *Filter* is deleted.

About Point Code (PC) Filters

Point Code Filters specify data associated with one or more point codes or a point-code range. A point code is a unique SS7 address that identifies a SS7 signaling point. A point code has three segments. Each segment of the point code must contain a number between 0 and 255.

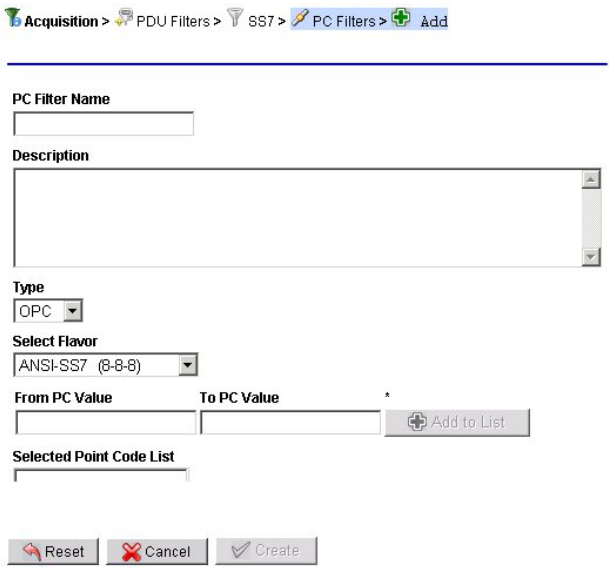


Figure 116: Point Code Filter Create/Modify Information Screen

The table describes the fields on the Point Code Filter Create/Modify Information screen.

Field	Description
PC Filter Name	User assigned name for the Point Code filter.
Description	Enter a description.
Type	Choices are: • OPC. • DPC. • Both.
Select Flavor From	Protocol / flavor of the point code for the specified point code or point code range.
Add to List	Clicking on this adds the Point Code to the Point Code List.
Remove from List	Clicking on this will remove the Point Code from the Point Code List.
Create	Saves filter information to the system.

TABLE 66: POINT CODE FILTER CREATE/MODIFY INFORMATION SCREEN FIELDS

Adding a PC Filter

Complete these steps to add a PC Filter.

1. Select **PC Filters** from the SS7 submenu.
2. Click **Add** from the pop-up menu.

The *Add PC Filter* screen opens.

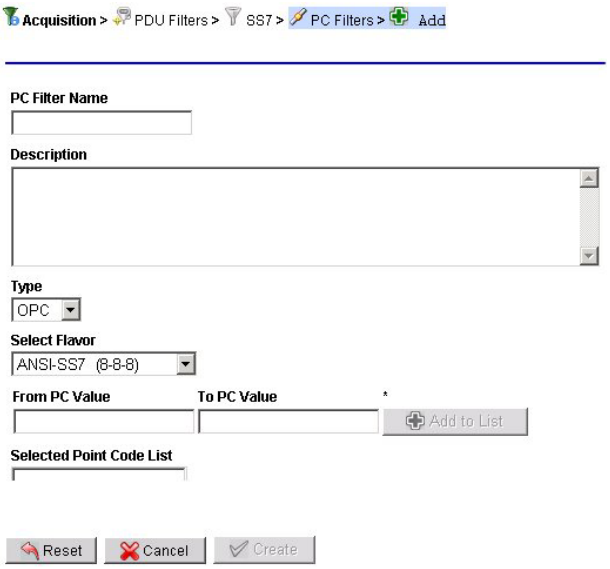


Figure 117: Add PC Filter Screen

3. Type in the **PC Filter Name**.
4. (Optional) Type in a **description** of the filter.
5. Select the **Type** of filter (OPC, DPC, Or Both).
6. Select the **Flavor** to be used.
7. Enter the **From PC Value**.
8. Select the **To PC Value**.
9. Click **Add** to List to add it to the Selected Point Code List.
10. Click **Create**.
    The *Point Code (PC) Filter* is added to the list in alphanumerical order.

Removing a Point Code

Complete these steps to remove a point code.

1. Select the **Point Code record** that needs modification.
2. Select the **Point Code** from the list.
3. Click **Remove** from List.
   The *Point Code* is removed.
4. Click **Done** to save the changes.

Modifying a Point Code Filter

Complete these steps to modify a Point Code filter.

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

Deleting a Point Code Filter

Complete these steps to delete a Point Code filter.

1. Select the **Resource ID Group** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The group is deleted.

About Raw Filters

Raw Filters allow you to configure filtering criteria. Using this filter you can take advantage of filtering features not otherwise available from the GUI screen. Raw Filters use a free-format input in a 'where Clause' like string. This is done through a message match string with imbedded mnemonics.

In order to use the Raw Filter section of the GUI, you should know how to write 'where Clause' like strings, interpret mnemonics, and convert data into binary and hexadecimal format.

WARNING: If you do not know how to write 'whereClause' like strings, interpret mnemonics, and convert data into binary and hexadecimal format, do not attempt to use this GUI feature or you may experience unpredictable results.

Syntax

The following syntax tree describes the 'whereClause' format of the input for Raw Filters.

whereClause:

lexpression

lexpression:

lprimary
lexpression or lexpression
lexpression and lexpression
not lexpression

lprimary:

expression comparator expression
expression between expression and expression
expression not between expression and expression
expression in (valueList)
expression not in (valueList)
expression in substitutionValueSet
expression not in substitutionValueSet
expression like string
expression not like string

comparator:

= < > <= >= <> !=

valueList:

constant
constant, valueList

expression:

term
term binaryOp expression
unaryOp expression
(expression)

term:

constant
fieldSpecifier

constant:

decimalConstant (e.g., -89.7)

integerConstant (e.g., -897)
string (e.g., 'hello world')
substitutionValue

substitutionValue:

%l.subTag (e.g., %l.aLong)
%s.subTag (e.g., %s.aString)
%f.subTag (e.g., %f.aFloat)

substitutionValueSet:

%L.subTag (e.g., %L.aLongSet)
%S.subTag (e.g., %S.aStringSet)
%F.subTag (e.g., %F.aFloatSet)

fieldSpecifier:

fldName (e.g., name)
fldName [unsignedValue] (e.g., name[5])

binaryOp:

& >> <<
|
* / %
+ -

unaryOp:
+ -

Mnemonics: The PMF subsystem has its own set of mnemonics that are used during Raw Filter creation. The mnemonics are used to specify what data you want to filter. The following table describes the mnemonics available for use with the Raw Filter Configuration page. Refer to this table for more information.

Field	Description	Value Entry Format
AIN_CALLED	Advanced Intelligent Network Called Number	Phone Number
AIN_CALLING	Advanced Intelligent Network Calling Number	Phone Number
AIN_CHARGE	Advanced Intelligent Network Charge Number	Phone Number
AIN_DIRECTORY	Advanced Intelligent Network Directory Number	Phone Number
AIN_MT	Advanced Intelligent Network Message	Hex
AIN_TRUNK_GROUP_ID	Advanced Intelligent Network Trunk Group Identifier	Hex
ANSI_BILLING	American National Standards Institute Billing ID	Decimal
ANSI_CALLED	American National Standards Institute Called Number	Phone Number
ANSI_CALLING	American National Standards Institute Calling Number	Phone Number
ANSI_CARRIER	American National Standards Institute Carrier Digits	Decimal
ANSI_DIGITS_TYPE	American National Standards Institute Digits Type	Decimal
ANSI_LATA	American National Standards Institute Local Access Transport Area	Decimal
ANSI_ROUTING	American National Standards Institute Routing Number	Decimal
ANSI_SERVICE_KEY	American National Standards Institute Service Key	Decimal
ANSI_SERVKEY_BILLING	American National Standards Institute Billing Number within Service Key Parameters	Decimal
ANSI_SERVKEY_CALLED	American National Standards Institute Called Number within Service Key Parameters	Decimal
ANSI_SERVKEY_CALLING	American National Standards Institute Calling Number within Service Key Parameters	Decimal
ANSI_SERVKEY_CLGDIRNUM	American National Standards Institute Calling Directory Number within Service Key Parameter	Decimal

Field	Description	Value Entry Format
ANSI_SERVKEY_DEST	American National Standards Institute Destination Number within Service Key Parameter	Decimal
BICC_CIC	Bearer Independent Call Control Call Instance Code	Reverse Hex
BSSAP_DISCR	GSM Base Station Application Part Discriminator	Decimal
BSSMAP_CAUSE	GSM Base Station Mobile Application Part Cause Value	Reverse Hex
BSSMAP_CI	GSM Base Station Mobile Application Part Cell Identifier	Hex
BSSMAP_CIC	GSM Base Station Mobile Application Part Circuit Identification Code	Reverse Decimal
BSSMAP_LAC	GSM Base Station Mobile Application Part Location Area Code	Reverse Hex
BSSMAP_MCC	GSM Base Station Mobile Application Part Mobile Country Code	Phone Number
BSSMAP_MNC	GSM Base Station Mobile Application Part Mobile Network Code	Phone Number
BSSMAP_MOBILE_ID	GSM Base Station Mobile Application Part Mobile Identifier	Phone Number
BSSMAP_MT	GSM Base Station Mobile Application Part Message Type	Hex
BSSMAP_TMSI	GSM Base Station Mobile Application Part Temporary Mobile Subscriber Identifier	Phone Number
CLASS_CALLED	ANSI Class Features Called Number	Phone Number
CLASS_CALLING	ANSI Class Feature Calling Number	Phone Number
CNAM_CALLING	ANSI Calling Name Delivery Feature	Phone Number
CNAM_CALLING_PRE	ANSI Calling Name Calling Number Presentation Indicator	Decimal
DPC	Destination Point Code	Point Code
DTAP_CALLED_PTY	GSM Direct Transfer Application Part Called Party	Phone Number
DTAP_CALLING_PTY	GSM Direct Transfer Application Part Calling Party	Phone Number
DTAP_CAUSE	GSM Direct Transfer Application Part Cause Code	Hex
DTAP_MAP_OPER	GSM Direct Transfer Application Part Map Operation Code	Hex
DTAP_MOBILE_ID_MM	GSM Direct Transfer Application Part Mobility Management Mobile ID	Phone Number
DTAP_MOBILE_ID_RR	GSM Direct Transfer Application Part Radio Resources Mobile ID	Phone Number
DTAP_MT	GSM Direct Transfer Application Part Message Type	Hex
DTAP_SS_DATA	GSM Direct Transfer Application Part Supplementary Services Data	Text String
DTAP_TMSI_MM	GSM Direct Transfer Application Part Mobility Management Temporary Mobile Subscriber ID	Phone Number
DTAP_TMSI_RR	GSM Direct Transfer Application Part Radio Resources Temporary Mobile Subscriber ID	Phone Number
DTAP_TRANS_FLAG	GSM Direct Transfer Application Part Transaction Flag	Decimal
DTAP_TRANS_ID	GSM Direct Transfer Application Part Transaction Identifier	Decimal
DTAPCC_MT	GSM Direct Transfer Application Part Call Control Message Type	Hex
DTAPCM_TYPE	GSM Direct Transfer Application Part Call Control Service Type	Hex
DTAPMM_MT	GSM Direct Transfer Application Part Mobility Management Message Type	Hex
DTAPRR_MT	GSM Direct Transfer Application Part Radio Resources Message Type	Hex
DTAPSMS_ADDR	GSM Direct Transfer Application Part Short Message Service Address	Phone Number

Field	Description	Value Entry Format
DTAPSMS_MT	GSM Direct Transfer Application Part Short Message Service Message Type	Hex
DTAPSS_MT	GSM Direct Transfer Application Part Supplementary Services Message Type	Hex
GENERIC_NAME	ANSI Calling Name Delivery Feature Generic Name	Text String
GENERIC_NAME_PRE	ANSI Calling Name Delivery Feature Generic Name Presentation Indicator	Decimal
GSMA_MOBILE_ID	Global System for Mobile Communication A-Interface Mobile ID	Decimal
GSMA_TMSI	Global System for Mobile Communication Temporary Mobile Subscriber ID	Decimal
INAP_CALLED_DIGITS	Intelligent Network Application Part Called Number Digits	Phone Number
INAP_CALLING_DIGITS	Intelligent Network Application Part Calling Number Digits	Phone Number
INAP_DIALED_DIGITS	Intelligent Network Application Part Dialed Digits	Phone Number
INAP_ORIG_CALLED_DIGITS	Intelligent Network Application Part Originating Called Digits	Phone Number
IS41_BILLID	ANSI-41 Billing ID	Hex
IS41_CALLED	ANSI-41 Called Party	Phone Number
IS41_CALLING	ANSI-41 Calling Party	Phone Number
IS41_CALLING_DIGITS1	ANSI-41 Calling Party Number Digits 1	Phone Number
IS41_CALLING_DIGITS2	ANSI-41 Calling Party Digits 2	Phone Number
IS41_CALLING_NUMBER	ANSI-41 Calling Number	Phone Number
IS41_CALLING_STR1	ANSI-41 Calling Number String 1	Text String
IS41_CALLING_STR2	ANSI-41 Calling Number String 2	Text String
IS41_CARRDIG	ANSI-41 Carrier Digits	Phone Number
IS41_CARRIER	ANSI-41 Carrier Digits	Phone Number
IS41_CARRIER_IS_TL	ANSI-41 Carrier Digits	Phone Number
IS41_CARRIER_LC_TL	ANSI-41 Carrier Digits	Phone Number
IS41_CARRIER_PARAM	ANSI-41 Carrier Digits Parameters	Decimal
IS41_CARRIER_PS_TL	ANSI-41 Carrier Digits	Phone Number
IS41_DEST_ALL	ANSI-41 Destination Digits	Phone Number
IS41_DEST_IS_TL	ANSI-41 Destination Digits	Phone Number
IS41_DEST_LC_TL	ANSI-41 Destination Digits	Phone Number
IS41_DEST_PARAM	ANSI-41 Destination Digits Parameters	Decimal
IS41_DEST_PS_TL	ANSI-41 Destination Digits	Phone Number
IS41_DESTINATION	ANSI-41 Destination Digits	Phone Number
IS41_ESN	ANSI-41 Electronic Serial Number	Reverse Hex
IS41_ESN_IS_TL	ANSI-41 Electronic Serial Number	Reverse Hex
IS41_ESN_LC_TL	ANSI-41 Electronic Serial Number	Reverse Hex
IS41_ESN_MFG_CODE	ANSI-41 Electronic Serial Number Manufacturing Code	Hex
IS41_ESN_MFG_CODE_IS_TL	ANSI-41 Electronic Serial Number Manufacturing Code	Hex
IS41 ESN MFG CODE LC TL	ANSI-41 Electronic Serial Number Manufacturing Code	Hex
IS41 ESN MFG CODE PS TL	ANSI-41 Electronic Serial Number Manufacturing Code	Hex
IS41_ESN_MFG_CODE_TL	ANSI-41 Electronic Serial Number Manufacturing Code	Decimal
IS41_ESN_PS_TL	ANSI-41 Electronic Serial Number Manufacturing Code	Reverse Hex
IS41_MDN	ANSI-41 Mobile Directory Number	Phone Number
IS41_MDN_ALL	ANSI-41 Mobile Directory Number	Phone Number
IS41_MDN_IS_TL	ANSI-41 Mobile Directory Number	Phone Number

Field	Description	Value Entry Format
IS41_MDN_LC_TL	ANSI-41 Mobile Directory Number	Phone Number
IS41_MDN_PARAM	ANSI-41 Mobile Directory Number	Decimal
IS41_MDN_PS_TL	ANSI-41 Mobile Directory Number	Phone Number
IS41_MIN	ANSI-41 Mobile Identification Number	Phone Number
IS41_MIN_ALL	ANSI-41 Mobile Identification Number	Phone Number
IS41_MIN_IS_TL	ANSI-41 Mobile Identification Number	Phone Number
IS41_MIN_LC_TL	ANSI-41 Mobile Identification Number	Phone Number
IS41_MIN_PARAM	ANSI-41 Mobile Identification Number	Decimal
IS41_MIN_PS_TL	ANSI-41 Mobile Identification Number	Phone Number
IS41_MY_TYPE	ANSI-41 System My Type Code	Hex
IS41_ROUT	ANSI-41 Routing Digits	Phone Number
IS41_ROUT_ALL	ANSI-41 Routing Digits	Phone Number
IS41_ROUT_IS_TL	ANSI-41 Routing Digits	Phone Number
IS41_ROUT_LC_TL	ANSI-41 Routing Digits	Phone Number
IS41_ROUT_PS_TL	ANSI-41 Routing Digits	Phone Number
IS41_ROUTING	ANSI-41 Routing Digits	Phone Number
IS41_ROUTING_PARAM	ANSI-41 Routing Digits	Decimal
IS41_SENDERID	ANSI-41 Sender Identification Number	Phone Number
IS41_SMS_ODA	ANSI-41 Short Message Service Original Destination Address	Phone Number
IS41_SMS_OOA	ANSI-41 Short Message Service Original Originating Address	Phone Number
ISUP_CALL_CAT	ISDN User Part Calling Party's Category	Hex
ISUP_CALLED	ISDN User Part Called Number	Phone Number
ISUP_CALLING	ISDN User Part Calling Number	Phone Number
ISUP_CARR_ID	ISDN User Part Carrier Identification	Phone Number
ISUP_CHARGE	ISDN User Part Charge Number	Phone Number
ISUP_CHG_NAT	ISDN User Part Charge Number Nature of Address Identifier	Hex
ISUP_CIC	ISDN User Part Circuit Identifier Code	Decimal
ISUP_CLD_NAT	ISDN User Part Called Party Nature of Address Identifier	Hex
ISUP_CLG_NAT	ISDN User Part Calling Nature of Connection Continuity	Hex
ISUP_CONTINUITY	ISDN User Part Continuity Indicators	Decimal
ISUP_COT	ISDN User Part Called Nature of Connection Continuity	Decimal
ISUP_GEN_ADDR	ISDN User Part Generic Address	Phone Number
ISUP_GEN_DIGITS	ISDN User Part Generic Digits	Phone Number
ISUP_GEN_NAME	ISDN User Part Generic Name	Text String
ISUP_INTERNATL	ISDN User Part International Indicator	Decimal
ISUP_INTERWRK	ISDN User Part Interworking Indicator	Decimal
ISUP_JURISDICTION	ISDN User Part Jurisdiction	Phone Number
ISUP_MT	ISDN User Part Message Type	Hex
ISUP_OLI	ISDN User Part Originating Line Information	Hex
ISUP_ORIG_CALLED	ISDN User Part Original Called Number	Phone Number
ISUP_PORTDIR	ISDN User Part Ported Directory Number	Phone Number
ISUP_QOR	ISDN User Part Forward Call Query on Release (QOR) Attempt Indicator	Decimal
ISUP_REL_CAUSE	ISDN User Part Release Cause	Decimal
ISUP_TNS	ISDN User Part Transit Network Selection	Phone Number
ISUP_TRN	ISDN User Part Forward Call Ported Number Translation Indicator	Decimal
ISUP_USI	ISDN User Part User Service Information	Hex
LIDB_BILL_NAT	Line Information Data Base Bill Network Address Translation Billing Number	Hex

Field	Description	Value Entry Format
LIDB_CCAN_SERV_DENY	Line Information Data Base Calling Card Account Number Service Denial Indicator	Hex
LIDB_CCSAN_NUM	Line Information Data Base Calling Card Subaccount Number	Phone Number
LIDB_CLD_NAT	Line Information Data Base Called Number Nature of Address	Hex
LIDB_CLD_PLN_ENC	Line Information Data Base Called Number	Hex
LIDB_CLG_NAT	Line Information Data Base Calling Nature of Address	Hex
LIDB_CLG_PLN_ENC	Line Information Data Base Calling Number	Hex
LIDB_COLLECT_ACC	Line Information Data Base Collection Acceptance Indicator	Decimal
LIDB_COMPANY_ID	Line Information Data Base Company ID	Phone Number
LIDB_ERROR_CODE	Line Information Data Base (TCAP) Error Code	Hex
LIDB_ERROR_MT	Line Information Data Base (TCAP) Error Code Tag	Hex
LIDB_MT	Line Information Data Base Message	Hex
LIDB_PIN	Line Information Data Base Personal Identification Number	Phone Number
LIDB_PIN_RESTRICT	Line Information Data Base Personal Identification Number Restriction Indicator	Hex
LIDB_PIN_SERV_DENY	Line Information Data Base Personal Identification Number Service Denial Indicator	Hex
LIDB_PROBLEM_CODE	Line Information Data Base Problem Code	Hex
LIDB_RECORD_STAT	Line Information Data Base Record Status Indicator	Hex
LIDB_THIRD_ACC	Line Information Data Base Third Number Acceptance Indicator	Decimal
LIDB_TXID	Line Information Data Base Transaction ID	Hex
LIDBQ_BILLING	Line Information Data Base Billing Number	Phone Number
LIDBQ_CALLED	Line Information Data Base Called Number	Phone Number
LIDBQ_CALLING	Line Information Data Base Calling Number	Phone Number
LIDBQ_MT	Line Information Data Base Query Message Type	Hex
LIDBR_MT	Line Information Data Base Response Message Type	Hex
MAP_HANDOVER	GSM Mobile Application Part Handover Number	Phone Number
MAP_IMEI	GSM Mobile Application Part International Mobile Equipment Identity	Phone Number
MAP_IMSI	GSM Mobile Application Part International Mobile Subscriber Identity	Phone Number
MAP_MSC	GSM Mobile Application Part Mobile Service Center Number	Phone Number
MAP_MSISDN	GSM Mobile Application Part Mobile Station ISDN Number	Phone Number
MAP_PRPHO_CID	GSM Mobile Application Part Prepare Handover Cell Identity	Reverse Hex
MAP_PRPHO_LAC	GSM Mobile Application Part Prepare Handover Location Area Code	Reverse Hex
MAP_ROAM	GSM Mobile Application Part Roaming Number	Phone Number
MAP_TMSI	GSM Mobile Application Part Temporary Mobile Subscriber Identity	Phone Number
MAP_VLR	GSM Mobile Application Part Visitor Location Registry Number	Phone Number
N00_ORIG_LATA	TR-533 Origination Local Access Transport Area	Phone Number
N00_ORIG_TYPE	TR-533 Originating Station Type	Hex
N00Q_CALLED	TR-533 Called Number	Phone Number
N00Q_CALLING	TR-533 Calling Number	Phone Number
N00Q_CARRIER	TR-533 Carrier ID	Phone Number

Field	Description	Value Entry Format
N00Q_ROUTING	TR-533 Routing Number	Phone Number
NETTST_MT	Network Test and Maintenance Message Type	Hex
OPC	Originating Point Code	Point Code
SCCP_CLD_ADDRESS	Signaling Connection Control Party Called Address	Phone Number
SCCP_CLD_IND	Signaling Connection Control Part Called Party Address Indicator	Decimal
SCCP_CLG_ADDRESS	Signaling Connection Control Part Calling Party Address	Phone Number
SCCP_CLG_IND_OCT	Signaling Connection Control Part Calling Party Address Indicator Octet	Decimal
SCCP_CLG_PC	Signaling Connection Control Part Calling Party Point Code	Point Code
SCCP_CLG_SSN	Signaling Connection Control Part Calling Party Subsystem Number	Decimal
SCCP_DLR	Signaling Connection Control Part Destination Local Reference	Hex
SCCP_GTI	Signaling Connection Control Part Global Title Indicator	Decimal
SCCP_MT	Signaling Connection Control Part Message Type	Hex
SCCP_RET_CAUSE	Signaling Connection Control Part Return Cause	Hex
SCCP_RTE_IND	Signaling Connection Control Part Routing Indicator	Decimal
SCCP_SLR	Signaling Connection Control Part Source Local Reference	Hex
SCCP_SSN	Signaling Connection Control Part Called Party Subsystem Number	Decimal
SCCP_SSN_TT	Signaling Connection Control Part Called Party Subsystem Number (if not equal to zero) or Translation Type	Decimal
SCCP_TT	Signaling Connection Control Part Translation Type	Decimal
SCCPM_MT	Signaling Connection Control Part Message Type	Hex
SI	Message Transfer Part Level Three Service Indicator	Decimal
SIGNET_CPC	Signaling Network Concerned Point Code	Point Code
SIGNET_CSLC	Signaling Network Concerned Signaling Link Code	Decimal
SIGNET_MT	Signaling Network Message Type	Hex
SLS	ISUP/TUP Signaling Link Selection	Decimal
TCAP_1ST_PARAM	Transaction Capabilities 1st Application Level Parameter within the Component portion of the TCAP message	Hex
TCAP_ABORT_CAUSE	Transaction Capabilities Application Part Abort Cause	Hex
TCAP_COMP_MT	Transaction Capabilities Application Part Component Type	Hex
TCAP_DEST_TID	Transaction Capabilities Application Part Destination transaction ID	Reverse Hex
TCAP_ERROR	Transaction Capabilities Application Part Error Code	Hex
TCAP_FLAVOR	ITU Standard =3, ANSI Standard=7	Decimal
TCAP_INVOKE_ID	Transaction Capabilities Application Part Invoke ID	Decimal
TCAP_MT	Transaction Capabilities Application Part Transaction/Package Type	Hex
TCAP_OPER	Transaction Capabilities Application Part Operation Code	Hex
TCAP_ORIG_TID	Transaction Capabilities Application Part Originating Transaction ID	Reverse Hex
TUP_CALL_CAT	Telephone User Part Calling Party's Category	Decimal
TUP_CALLED	Telephone User Part Called Number	Phone Number
TUP_CALLING	Telephone User Part Calling Number	Phone Number
TUP_CIC	Telephone User Part Circuit Identification Code	Decimal

Field	Description	Value Entry Format
TUP_INTERNATL	Telephone User Part International Indicator	Decimal
TUP_INTERWRK	Telephone User Part Interworking Indicator	Decimal
TUP_MT	Telephone User Part Message Type	Hex
TUP_REL_CAUSE	Telephone User Part Release Cause	Decimal

TABLE 67: RAW FILTER CONFIGURATION MNEMONICS

Raw Filter Value Entry Formats

Raw filtering is not a direct input operation. When you set up a Raw Filter, you must translate the data you are filtering for into a format the PMF subsystem can understand. Each Raw Filter value entry category has its own formatting rules. There are seven categories:

- Phone Number
- Point Code
- Decimal
- Reverse Decimal
- Hex
- Reverse Hex
- Text String

Phone Number

The PMF subsystem uses Telephony Binary Coded Decimal (TBCD) encoding for phone numbers. This means that phone numbers are encoded from right to left and top to bottom. If you want to search for a phone number, the user must filter for the number in this format. For example, if you want to search for the phone number string 1234 then you must input 0x2143.

- 0x: Indicator that what follows is a hexadecimal indicator.
- 2143: Phone number string 1234 in top-bottom, left-right format.

For odd numbers, such as 123-4567, an extra zero must be added to the string in order to account for the zero filler digit in the Octet. So the proper format is: 0x21436507.

- 0x: Indicator that what follows is a hexadecimal indicator.
- 214365: Phone number string 123456 in top-bottom, left-right format.
- 07: Phone number string 70 in top-bottom, left-right format, with extra zero to account for zero filler digit.

Point Code

Point codes need to be translated into the appropriate binary format, then converted to a hex number, or the decimal equivalent of the hex number.

MTP3

Unlike most point codes, MTP3 point codes are translated into binary format starting with the first number and working toward the last number. Once each point code segment is translated into the appropriate binary format, each binary number must be translated into either a hexadecimal number or its decimal equivalent. The PMF subsystem deals with two different Octet patterns.

ANSI

ANSI point codes are divided into three consecutive 8-bit binary Octets. So, point code 7-200-6 should be translated into:

- 7 in 8-bit: 00000111.
- 200 in 8-bit: 11001000.
- 6 in 8-bit: 00000110.

Next, use a scientific calculator to determine the hexadecimal of each number, or the decimal equivalent. For 7-200-6 this would equal:

- Hexadecimal: 07C806.
- Decimal: 509958.

So to build a raw filter for the MTP3 point code in ANSI you would use Relevant_mnemonic = 509958.

ITU

ITU point codes are divided into three segments. The first is 3-bit binary. The second is 8-bit binary. The last segment is 3-bit binary. So, point code 7-200-6 should be translated into:

- 7 in 3-bit: 111
- 200 in 8-bit: 11001000
- 6 in 3-bit: 110

Next, use a scientific calculator to determine the hexadecimal of each number, or the decimal equivalent. For 7-200-6 this would equal:

- Hexadecimal: 3E46
- Decimal: 15942

So to build a raw filter for the point code in ITU you would use Relevant_mnemonic = 15942

Non MTP3

For all point codes other than MTP3, the point code values need to be translated in 'reverse' order. For example, point code 7-200-6, should be translated into binary starting with 6 in 3-bit, 200 in 8-bit, and 7 in 3-bit.

ANSI

ANSI is divided into three consecutive 8-bit binary Octets. So, point code 7-200-6 should be translated into:

- 6 in 8-bit: 00000110
- 200 in 8-bit: 11001000
- 7 in 8-bit: 00000111

Next, use a scientific calculator to determine the hexadecimal of each number, or the decimal equivalent. For 7-200-6 this would equal:

- Hexadecimal: 06C807
- Decimal: 444423

So to build a raw filter for the point code in ANSI you would use Relevant_mnemonic = 444423

ITU

ITU is divided into three Octets. The first is 3-bit binary. The second is 8-bit binary. The last Octet is 3-bit binary. So, point code 7-200-6 should be translated into:

- 6 in 3-bit: 110
- 200 in 8-bit: 11001000
- 7 in 3-bit: 111

Next, use a scientific calculator to determine the hexadecimal of each number, or the decimal equivalent. For 7-200-6 this would equal:

- Hexadecimal: 3647
- Decimal: 13895

So to build a raw filter for the point code in ITU you would use Relevant_mnemonic = 13895

Decimal

This is the only data type which is entered directly. To build a raw filter for a decimal type mnemonic for the value 584, you would enter Relevant_mnemonic = 584.

Reverse Decimal

A Reverse Decimal must first be converted into to a hex number, then the Octets must be reversed. You can use a scientific calculator to determine the hex equivalent of any decimal. For example, a value of 61873 would be:

- Hex: f1b1.
- Reversed to: b1f1

So to build a raw filter for a reverse decimal type mnemonic you would use Relevant_mnemonic = 0xb1f1.

Hex

Hex values are entered with a leading 0x to indicate hex. For example, a value of 842ea35c would be entered as

- 0x: Indicator that what follows is a hexadecimal indicator
- 842ea35c: Hex number

So to build a raw filter for a hex type mnemonic you would use Relevant_mnemonic = 0x842ea35c.

Reverse Hex

These are entered the same as Hex numbers above, except the Octets are reversed. For example, a value of 842ea35c would be entered as

- 0x: Indicator that what follows is a hexadecimal indicator
- 5ca32e84: Hex number with Octets reversed

So to build a raw filter for a reverse hex type mnemonic you would use Relevant_mnemonic = 0x5ca32e84

Text String

Text String is a series of successive ASCII characters. Please consult a standard ASCII character-code mapping table for the correct values. For example, to build a raw filter for the Text String "My Example" you would use Relevant_mnemonic = 0x4d79204578616d706c65.

Example of a SCCP Raw Filter

Shown here is an example of an SCCP protocol Raw Filter that can be created using the raw filter page.

Protocol	Raw Filter Value
MAP	**(TCAP_FLAVOR=3)**
IS41	**((TCAP_FLAVOR=7) and (TCAP_1ST_PARAM !=97))**
INAP	**((TCAP_FLAVOR=3) and (SCCP_SSN=241))**
CAMEL	**((TCAP_FLAVOR=3) and ((SCCP_SSN=5) or (SCCP_SSN=146)))**

TABLE 68: SCCP RAW FILTER EXAMPLE

The figure below shows the *Add Raw Filter* screen

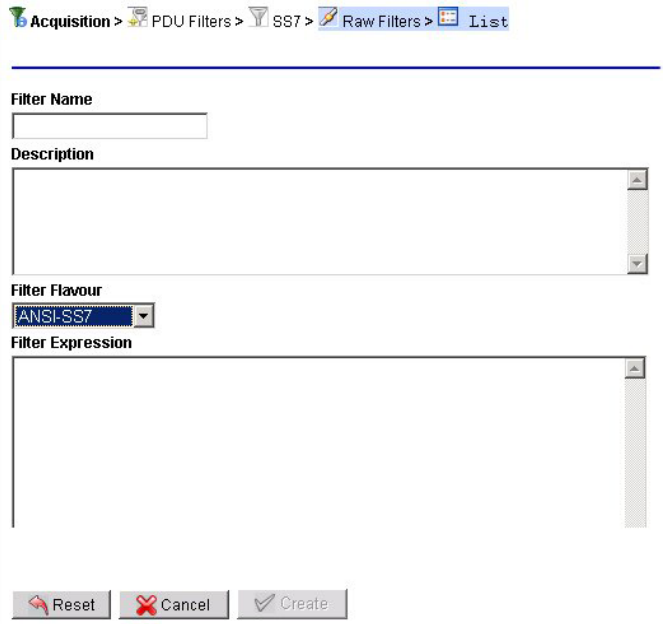


Figure 118: Add Raw Filter Screen

The following table describes the fields on the *Add Raw Filter* screen.

Field	Description
Filter Name	User defined name for filter.
Description	Enables you to add a description of the filter for added information.
Filter Flavour	Protocol / Flavour of the raw filter.
Filter Expression	Allows a user to enter data that will create a new filter. The data must be in syntax supported by the current PMF release. When the Accept button is clicked, the information in the Filter Expression window becomes the new Raw filter.
Create button	Creates or modifies filter based on the information shown in the Filter Expression field.

TABLE 69: ADD RAW FILTER SCREEN FIELDS

Adding a Raw Filter

Complete these steps to add a RAW filter.

1. Select **RAW Filters** from the SS7 submenu.
2. Click **Add** from the submenu. The *Add RAW Filter* screen opens.
3. Type in the **Filter Name**.
4. Select a **Filter Flavor** from the pull-down menu.
5. Type in a **Filter Expression**.
6. Click **Accept**. The filter is added to the RAW filter object tree in alphanumerical order.

Modifying Raw Filters

1. Select the **RAW Filter** to be modified.
2. Select **Modify** from the menu.
3. Make the necessary **modifications**.
4. Click **Modify**. The filter is modified

Deleting a Raw Filter

Complete these steps to delete a Raw filter.

1. Select the **RAW Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt. The filter is deleted.

About Combination Filters

Combination filters are for data based on any combination of the other four SS7 filter types.

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.

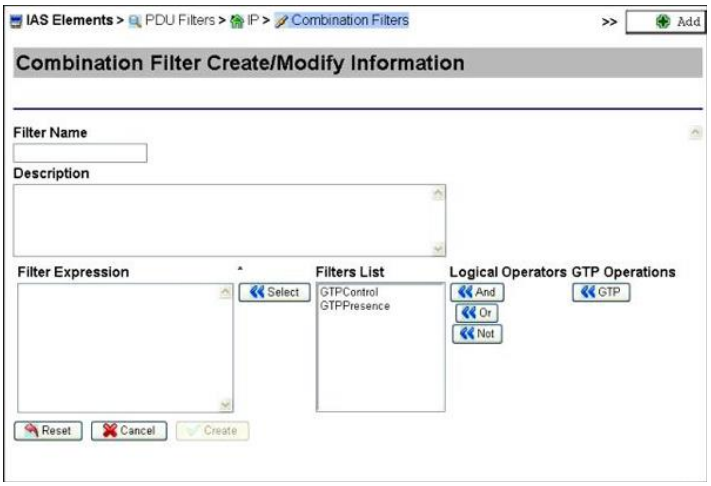


Figure 119: Add Combination Filter Screen

The table describes the fields on the *Combination* Filter *Create/Modify* Information screen.

Field	Description
Filter Name	User-defined name for filter.
Description	Provides pertinent information about the filter.
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.
Left arrow button	Moves highlighted filter into Filter Expression box.
Filters List	List of existing filters a user can combine.
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.
Create button	Saves information entered.

TABLE 70: ADD/MODIFY COMBINATION FILTER SCREEN FIELDS

Adding an SS7 Combination PDU Filter

Complete these steps to add a combination filter.

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.

1. Select **Acquisition > PDU Filters**.
2. Click **Add** from the PDU Filter tool bar.
3. From the PDU Filter Family tab, select **SS7 - Signaling System 7**.
4. Click **Next**.
5. From the SS7 tab, select **Combination - Combination Filter**.
6. Click **Next**.
7. Type in the **Filter Name**.
8. (Optional) Type in a **Description**.
9. Click **Select** to select a Filter Expression.
10. Click the appropriate **Logical Operator** for the **Filters List** (And, Or, Not).
11. Click **Finish**.
    The Combination filter is appears in the Combination Filters object tree in alphanumerical order.

Modifying a Combination PDU Filter

Complete these steps to modify a combination filter.

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

Deleting a Combination PDU Filter

Complete these steps to delete a combination filter.

1. Select the **Combination Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The filter is deleted.

About GPRS Gb Filters (PMF)

The General Packet Radio Service (GPRS) Gb Filters option allows you to define the three types of filters in this type of protocol. The three types of filters are:

- Data Link Collection Identifier (DLCI) filters
- Service Access Point Identifier (SAPI) filters
- Combination filters

CCM provides a separate wizard to configure each of these Filters in this protocol.

You must provide a list of Data Link Collection Identifier DLCI values to filter at the Dataflow level. The DLCI is a field in the Frame Relay header in the GPRS Gb packet.

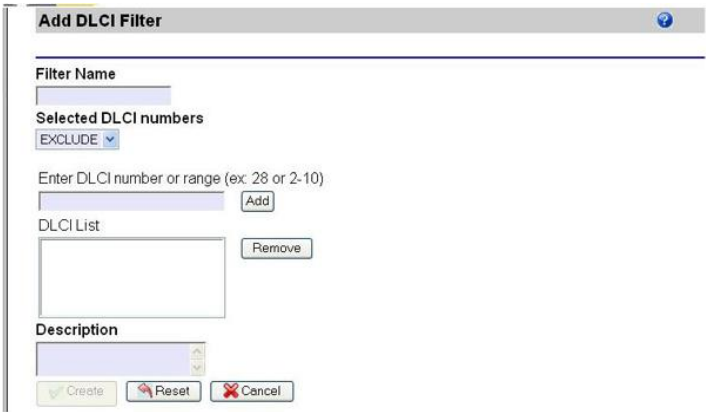


Figure 120: Add Gb DLCI Filter Screen

This table describes the fields in the DLCI filter screen.

Field	Description
Filter Name	User assigned name for the DLCI Filter.
Description (Optional)	Provides a description of the DLCI filter
Selected DLCI numbers	Drop-down menu to Include or Exclude a range of DLCI numbers.
Enter DLCI number or range	Type in either a single DLCI number or a range of DLCI numbers.
Add to list button	Adds the information entered DLCI number or range to the DLCI List.
DLCI List	Contains all of the user-specified DLCI numbers and/or ranges of DLCI numbers. You can add multiple DLCI numbers and/or ranges to this list, or remove DLCI numbers and/or ranges from the list. All DLCI numbers and/or ranges in this list at the time of the filter creation will be

Field	Description
	used to filter data.
Remove from list button	Deletes DLCI numbers and/or DLCI number ranges, from the DLCI List field.
Create / Reset / Cancel	• Create: Creates and saves the DLCI Filter information. • Reset: Changes back to the original DLCI filter settings. • Cancel: No information is saved for this filter.

TABLE 71: ADD DLCI FILTER SCREEN FIELDS

Adding a Gb DlCI Filter

To add a Gb DLCI Filter, complete these steps.

1. Select **DLCI Filters** from the GB submenu.
2. Click **Add** from the submenu.
   The Gb DLCI Filter screen opens.

Note: You must provide a list of Data Link Collection Identifier DLCI values to filter at the Dataflow level. The DLCI is a field in the Frame Relay header in the GPRS Gb packet.

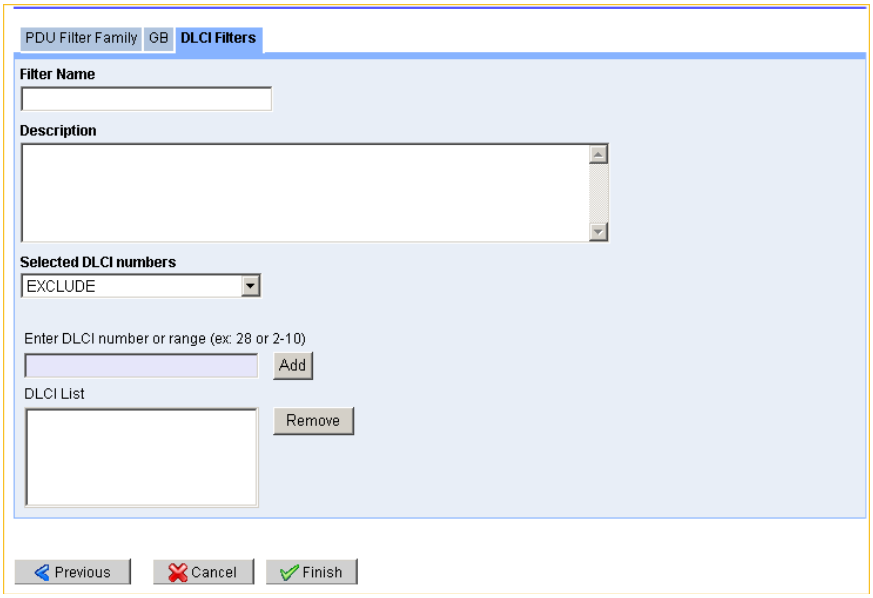


Figure 121: Gb DLCI Filter Screen

This table describes the fields in the DLCI Filter screen.

Field	Description
Filter Name	User assigned name for the DLCI Filter.
Description (Optional)	Provides a description of the DLCI filter
Selected DLCI numbers	Drop-down menu to Include or Exclude a range of DLCI numbers.
Enter DLCI number or range	Type in either a single DLCI number or a range of DLCI numbers.
Add to list button	Adds the information entered DLCI number or range to the DLCI List.
DLCI List	Contains all of the user-specified DLCI numbers and/or ranges of DLCI numbers. You can add multiple DLCI numbers and/or ranges to this list, or remove DLCI numbers and/or ranges from the list. All DLCI numbers and/or ranges in this list at the time of the filter creation will be used to filter data.
Remove from list button	Deletes DLCI numbers and/or DLCI number ranges, from the DLCI List field.
Create / Reset / Cancel	• Create: Creates and saves the DLCI Filter information. • Reset: Changes back to the original DLCI filter settings. • Cancel: No information is saved for this filter.

TABLE 72: ADD DLCI FILTER SCREEN FIELDS

3. Type in the **Filter Name**.
4. Select a **DLCI Number Function** from the pull-down menu.
5. Type in an **DLCI Number** or **Number Range**.
6. Click **Add**.
   The *number* or *range* appears in the ID List field.
7. (Optional) Type in a **Description** of the DLCI filter.
8. Click **Create**.
   The *filter* is added to the GB DLCI filter object tree in alphanumerical order.

Removing a number or number range from the List

To remove a DLCI number or number range, complete these steps.

1. Select the **DLCI Record** that needs modification.
2. Click **Edit**.
3. Select the **Number** or **Range** from the DLCI number list.
4. Click **Remove**.
   The *number* or *range* is removed.
5. Click **Done** to save the changes.

Modifying a Gb DlCI filter Record

Complete these steps to modify a Gb DLCI filter.

1. Select the **Gb DLCI Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a Gb DLCI Filter

Complete these steps to delete a Gb DLCI filter.

1. Select the **Gb DLCI Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *filter* is deleted.

Adding a Gb SAPI Filter (PMF)

Complete these steps to add a Gb 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 **GPRS** from the list.
4. Click **Next**.
   The *Gb* tab appears.
5. Select **SAPI Filter** from the list.
6. Click **Next**
   The *SAPI* Filters tab appears.

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

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 with options to Include or Exclude a range of SAPI numbers. (More than one) **Note:** The range of SAPI numbers is 0-15.
SAPI filter	Radio button to select a SAPI filter.
No SAPI filter	Radio button to select if there is no SAPI filter.
Add to List	After typing in a number, click this button to add the SAPI number to the List field.
Remove from List	Select a number from the List field and click this button to remove the number from the List field.
Previous / Finish / Cancel (Not shown)	• Finish: Creates and saves the SAPI Filter information. • Previous: Takes you back to the previous screen. • Cancel: No information is saved for this filter.

TABLE 73: ADD GB SAPI FILTER SCREEN FIELDS

7. Type in the **Filter Name**.
8. (Optional) Enter the **Description**.
9. Select a **SAPI Number Function** from the pull-down menu.
10. Select to use or not use a **SAPI Filter**.
11. (Optional) If SAPI filter is selected, type in **SAPI Numbers**, (one at a time) and click **Add** to list.

    Note: Range is 0-15.

    Note: To remove SAPI numbers, select number(s) in the List field and click **Remove from List**.

12. Click **Finish**.
    The *filter* is added to the PDU filter list screen.

Modifying a Gb DlCI filter Record

Complete these steps to modify a Gb DLCI filter.

1. Select the **Gb DLCI Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a Gb DLCI Filter

Complete these steps to delete a Gb SAPI filter.

1. Select the **Gb SAPI Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *filter* is deleted.

Adding a GPRS Combination PDU Filter

Complete these steps to add a combination filter.

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.

1. Select **Acquisition > PDU Filters**.
2. Click **Add** from the PDU Filters tool bar.
3. From the PDU Filter Family tab, select **GPRS - General Packet Radio Service**.
4. Click **Next**.
5. From the GB tab, select **Combination - Combination Filter**.

6. Click **Next**.
7. Type in the **Filter Name**.
8. (Optional) Type in a **Description**.
9. Click **Select** to select a Filter Expression.
10. Click the appropriate **Logical Operator** for the **Filters List** (And, Or, Not).
11. Click **Finish**.
    The *GPRS Combination Filter* appears in the *Combination Filters object tree* in alphanumerical order.

Modifying a Gb Combination PDU Filter

Complete these steps to modify a Gb Combination filter.

1. Select the **Gb Combination Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a Gb Combination PDU Filter

Complete these steps to delete a Gb Combination PDU filter.

1. Select the **Gb Combination PDU Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The filter is deleted.

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 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.

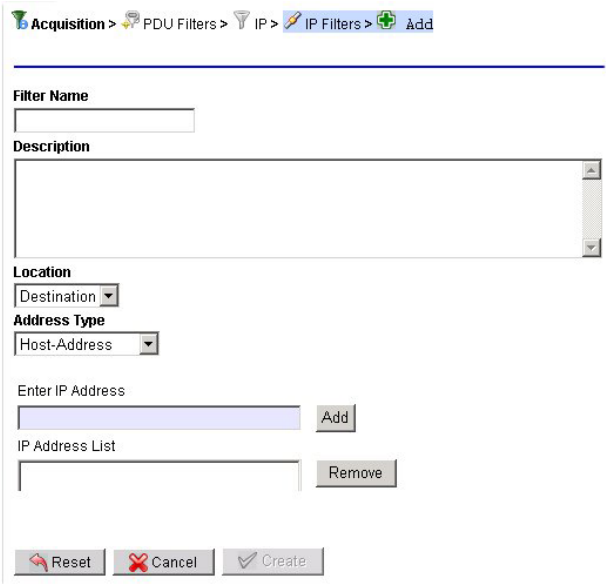


Figure 122: Add IP Address Filter Screen

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: • 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.

TABLE 74: ADD/MODIFY PORT FILTER SCREEN FIELDS

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.

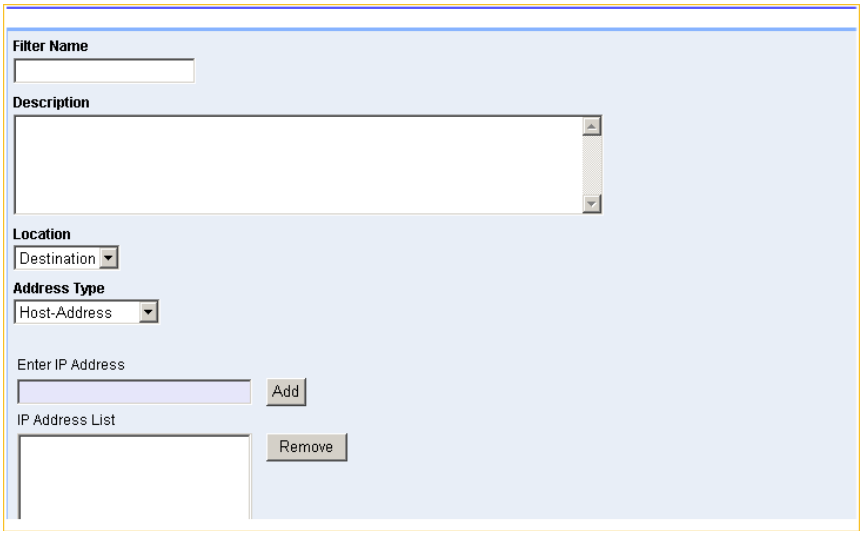


Figure 123: IP Filters Screen

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: • Destination: Outgoing IP ports. • Source: Incoming IP ports.
Address Type	Select one of the following from the drop-down menu • 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.
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)	Cancels the procedure with no information saved.

TABLE 75: IP FILTER SCREEN FIELDS

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 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**.
5. The *changes* are saved.

Deleting a IP Address 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 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.

Figure 124: 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 a 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.

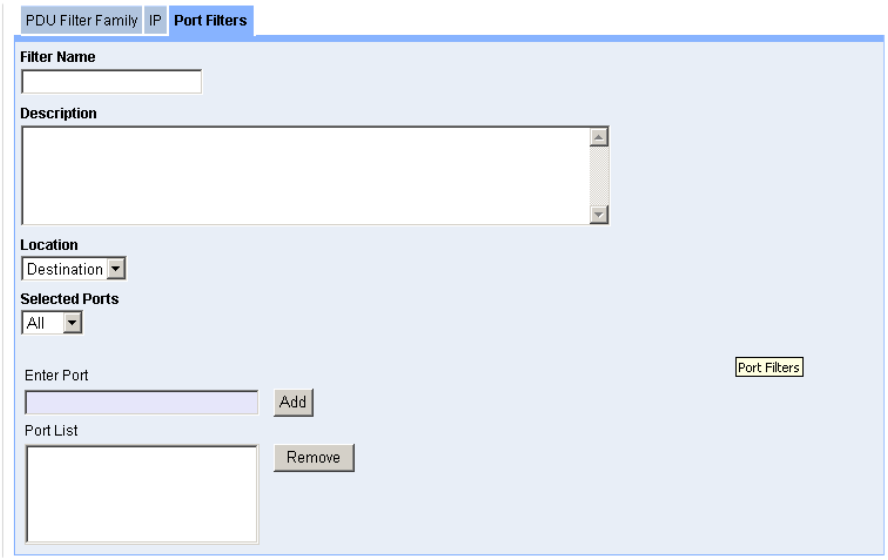


Figure 125: Add Port Filter Screen

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

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: • Destination: Outgoing IP ports. • Source: Incoming IP ports.
Selected ports	This is a drop-down menu option with the following selections: • 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.
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.

TABLE 76: PORT FILTER SCREEN FIELDS

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.

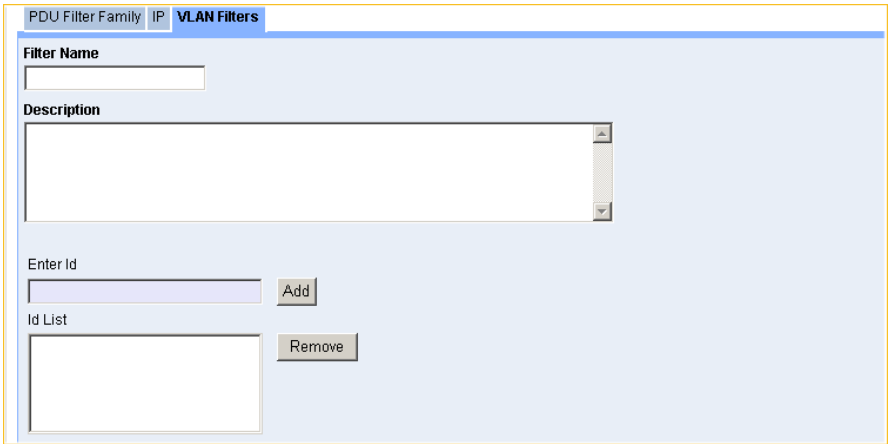


Figure 126: Add IP VLAN Filter Screen

The table describes the fields on this screen.

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.

TABLE 77: VLAN FILTER SCREEN FIELDS

1. Type in the **Filter Name**.
2. (Optional) Type in a **Description** of the VLAN Filter.
3. Type in an **ID** in the Enter ID field.
4. Click **Add**.
   The *ID* appears in the *ID List* field.
5. 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.

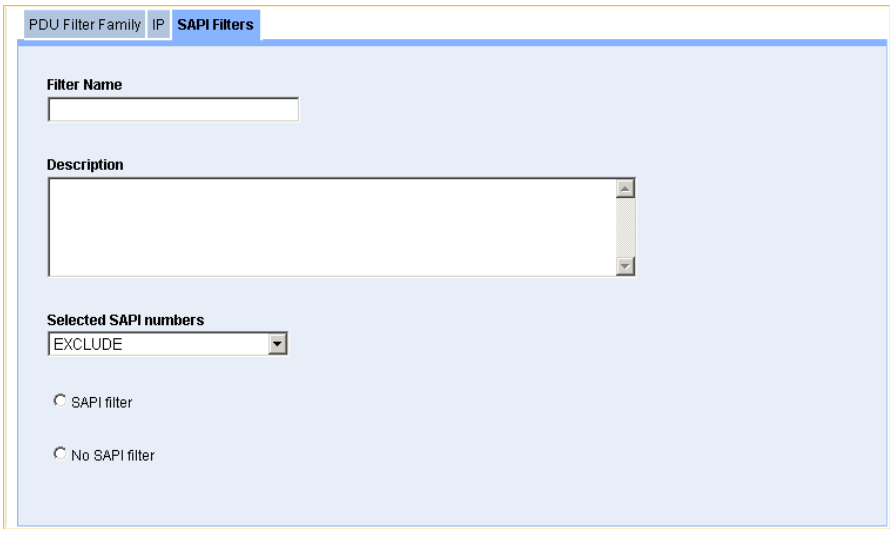


Figure 127: Add SAPI for Gb over IP Filter Screen

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

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)	• Finish: Creates and saves the SAPI Filter information. • Previous: Takes you back to the previous screen. • Cancel: No information is saved for this filter.

TABLE 78: ADD SAPI FILTER FOR GP OVER IP SCREEN FIELDS

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.

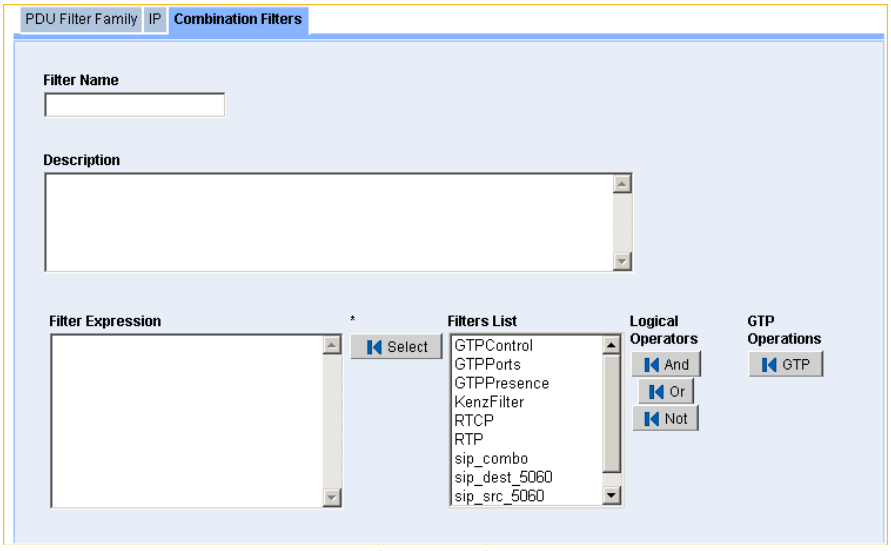


Figure 128: Combination Filters Screen

The table describes the fields on this screen.

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

Field	Description
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. • 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.

TABLE 79: COMBINATION FILTER SCREEN FIELDS

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)

    If applicable, click to select a **GTP Operation** and specify the **GTP Expression** within the parenthesis.

    Note: Example of a correct GTP Combination Filter: GTP (src5000 and dest500) or GTPControl.

    Note: 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 SigTran Protocol Filters

There are four categories of SigTran Protocol filters:

- Association Filters - Stream Control Transmission protocol (SCTP) filters as well as other Association Filters
- SS7 Protocol Filters - Point Code (PC), Service Information Octet (SIO), Global Title (GT) and Subsystem Number (SSN) Filters
- Combination - Filters for data based on any combination of the other SigTran Filter Types.

About SigTran Association Filters

There are two types of SigTran Association filters:

- Stream Control Transmission protocol (SCTP) filters
- Other Association filters

Adding a SigTran SCTP PDU Filter

Complete these steps to add a SigTran SCTP PDU filter.

1. Select **Acquisition > PDU Filters** from the object menu.
   The *PDU Filters* list screen opens.
2. Click **Add**.
   PDU Filter Family screen opens.
3. Select **SigTran - Protocol**
4. Click **Next**.
   The *SigTran* screen opens.
5. Select **SCTP Association Filter**.
6. Click Next.
   The *SigTran Association Filters* screen opens.

   The table describes the fields on this screen.

Field	Description
Filter Name	Alphanumeric field providing name of the filter
Description	(Optional) Alphanumeric field for short description of the filter
IP Protocol ID	Pull-down list (SCTP only selection).
Local Port	Numeric field that provides location of port.
Local IP Address	IP address for local port
Remote Port	Numeric field that provides port for association
Remote IP Address	IP address for the remote port for association
Add to List	Button to add association to list
Association List	List box showing associations
Remove from List	Button to remove selected associations from list

TABLE 80: SCTP ASSOCIATION FILTER SCREEN FIELDS

7. Enter the **Filter Name**.
8. (Optional) Enter a **Description** of the SCTP filter.
9. Select the **IP Protocol ID**
10. Enter a **Local Port**.
11. Enter the **Local IP Address**.
12. Enter the **Remote Port**.
13. Enter the **Remote Port IP Address**
14. Click **Add to List** to add the association to the *Association List*.
    a. Repeat steps 11-15 to add more associations.
15. Click **Finish**.
    The filter appears in the PDU filter list.

16. **Apply Changes** to the xMF system to update the system.

Modifying a SigTran SCTP PDU Filter

Complete these steps to modify a SigTran SCTP filter.

1. Select the **SigTran SCTP Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a SigTran SCTP PDU Filter

Complete these steps to delete a SigTran SCTP filter.

1. Select the **SigTran SCTP Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
4. The *filter* is deleted.

Adding a SigTran Other Association PDU Filter

Complete these steps to add a SigTran Other Association 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 **SigTran Filter**
4. Click **Next**.
   The *SigTran* screen opens.
5. Select **SigTran Other Association**.
6. Click **Next**.
   The *SigTran OtherProt Assoc Filter* screen opens.

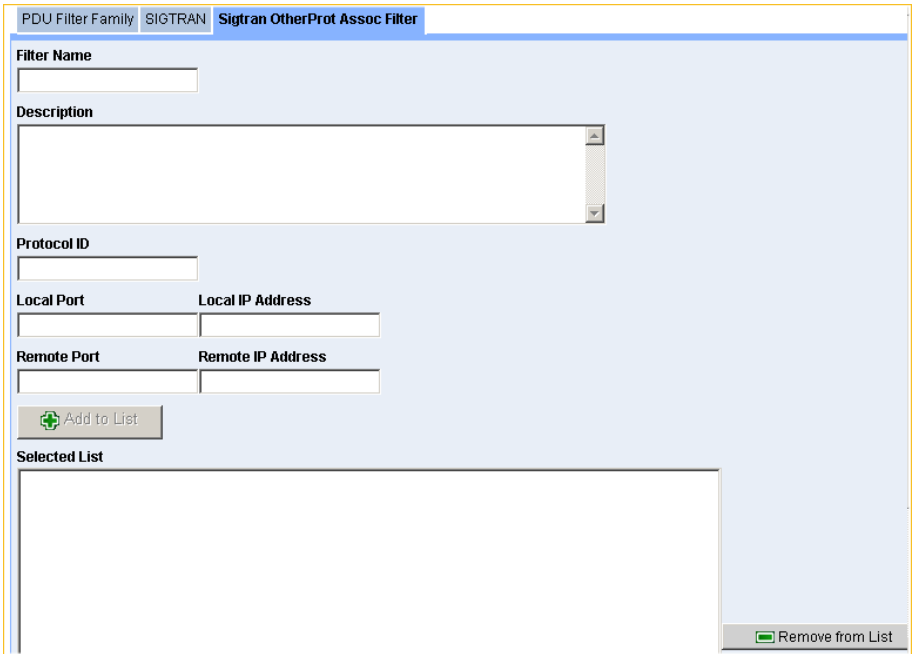


Figure 129: SigTran OtherProt Assoc Filter Screen

The table describes the fields on this screen.

Field	Description
Filter Name	Alphanumeric field providing name of the filter
Description	(Optional) Alphanumeric field for short description of the filter
IP Protocol ID	Pull-down list (SCTP only selection).
Local Port	Numeric field that provides location of port.
Local IP Address	IP address for local port
Remote Port	Numeric field that provides port for association
Remote IP Address	IP address for the remote port for association
Add to List	Button to add association to list
Association List	List box showing associations
Remove from List	Button to remove selected associations from list

TABLE 81: SIGTRAN OTHERPROT ASSOC FILTER SCREEN FIELDS

7. Type in the **Filter Name**.
8. (Optional) Type in a **Description** of the VLAN filter.
9. Enter in an **IP Protocol ID** (positive number).
10. (Optional) Enter **Local Port** and **Local IP Address**.
11. (Optional) Enter **Remote Port** and **Remote IP Address**.
12. (If ports and addresses have been entered) Click **Add** to List.
13. Click **Finish**.
    The *filter* is added.

Modifying a SigTran Other Association PDU Filter

Complete these steps to modify a SigTran Other Association filter.

1. Select the **SigTran Other Association Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The changes are saved.

Deleting a SigTran Other Association PDU Filter

Complete these steps to delete a SigTran Other Association filter.

1. Select the **SigTran Other Association Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *filter* is deleted.

About SigTran SS7 Protocol Filters

There are four types of SigTran SS7 filters:

- Point Code (PC)
- Service Information Octet Filter (SIO)
- Global Title (GT)
- Subsystem Number (SSN)

Adding a SigTran SS7 PC PDU Filter

Complete these steps to add a SigTran SS7 Point Code 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 **SigTran Filter**
4. Click **Next**.
   The *SigTran* screen opens.
5. Select **SS7 Protocol Filter**.
   The *SigTran SS7 Filters* screen opens.
6. Select **Point Code Filter**.
7. Click **Next**.
   The *SigTran PC Filters* screen opens.

   The table describes the fields on this screen.

Field	Description
Filter Name	User-defined name for filter.
Description	Enables you to describe the characteristics of the filter
Select Flavor	Provides the protocol for specified point code or point code range
Protocol	Shows the protocols you can use: • M2PA/SCTP • M3UA/SCTP • M2UA/SCTP
PC Type	Lists the types of point codes: • PC • OPC • DPC
Point Code	Enter point code(s) to be used
Add to List	Adds the Id information entered to the Association List.
Remove from List	Removes the selected port from the Association List.
PC List	Lists the added point codes
Logical Operators	Provides the following operators: • And = conjunction between two sub-filters • Or = disjunction between two sub-filters • Not = operator means negation of the sub-filter • ( ) = used to group sub-filters and modify the priority of operators
Filter Expression	Shows the finished expression to be used
Finish button (not shown)	Saves filter settings based on the information shown in the Filter Expression field.

TABLE 82: SIGTRAN PC FILTER SCREEN FIELDS

8. Type in the **Filter Name**.
9. (Optional) Type in a **Description** of the SigTran filter.
10. Select a **Flavor** from the list.
11. Select a **Protocol**.
12. Select a **PC Type** and enter **Point Code**.
13. Click **Add** to List .
14. Select the appropriate **Logical Operator(s)**.
15. Click **Finish**.
    The *filter* is added.

Note: Sigtran filters can be combined using the Combination Filter operation.

Note: A choice can be made at this point to use "chunk forwarding" or to the forward whole IP packet (IP raw).

Note: To complete the filtering process the filter must be connected with a data flow, traffic classification and Dataflow process in IXP. See Routing PDUs to xDR Builders for SigTran or Routing PDUs to xDR Builders for more information.

Modifying a SigTran SS7 PC PDU Filter

Complete these steps to modify a SigTran SS7 PC Filter:

1. Select the **SigTran SS7 PC Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The changes are saved.

Deleting a SigTran SS7 PC PDU Filter

Complete these steps to delete a SigTran SS7 PC filter.

1. Select the **SigTran SS7 PC Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *filter* is deleted.

Adding a SigTran SS7-SIO PDU Filter

1. Select **Acquisition > PDU Filters**.
2. Click **Add** on the tool bar.
3. Select **SigTran - Protocol**.
4. Click **Next**.
5. Select **SS7 Protocol Filters**.
6. Click **Next**.
7. Select **SIO Filter**.
8. Click **Next**.
9. Select **NISI (Network Indicator + Service Indicator)**.

   Note: If only SI is selected, there is no need to select a Network Indicator.

10. Click **Next**.

    The table describes the fields on the SIO screen.

Field	Description
Filter Name	User-defined name for filter.
Description	Enables you to describe the characteristics of the filter
Protocol	Shows the protocols you can use: • M2PA • M3UA • M2UA
Network Indicator	Lists the network indicators available: • National • International
Service Indicator	Lists the service indicators available: • Signaling Network Management Messages • Signaling Network Testing and Maintenance Messages • Signaling Network Testing and Maintenance Special Messages • SCCP • Telephone User Part • ISDN User Part • Broadband User Part • Satellite ISDN User Part • AAL Type 2 Signaling • Bearer Independent Call Control • Gateway Control Protocol • Other
Value	Called
Add to List	Adds the Id information entered to the SIO List.
SIO List	Shows all SI + NI combinations added.

Field	Description
Select	Selects the highlighted SIO and places it in the Filter Expression Field
Filter Expression	Shows the expressions that have been created in the SIO list.
Logical Operators	Provides the following operators: • And = conjunction between two sub-filters • Or = disjunction between two sub-filters • Not = operator means negation of the sub-filter • ( ) = used to group sub-filters and modify the priority of operators
Select / Remove buttons	Clicking Select, adds a highlighted SIO to the Filter Expression Field. Clicking Remove removes the highlighted SIO from the list in the Filter Expression field.
Finish button (not shown)	Saves filter settings based on the information shown in the Filter Expression field.

TABLE 83: SIGTRAN SS7 SIO SCREEN FIELDS

11. Enter in the **Filter Name**.
12. (Optional) Enter a **Description**.
13. Select the **Protocol** for the filter.
14. Select a **Network Indicator** and **Service Indicator**.

    Note: Choose from either the pre-defined list or select **Other**. If Other is selected, the specific Service Indicator is manually entered.

15. Click **Add** to list.
16. Select the **SIO** from the *SIO* list.
17. Click **Select** to add the expression to the Filter Expression list.
    To remove an expression from the field, click **Remove** on the bottom right side of the screen.

    Note: To create a more complex expression, use the **Logical Operator(s)**. A name then can be assigned to the filter as well as a description of the filter.

    Note: More than one filter can be created.

    Note: This filter can be used in conjunction with other filters using the Combination filter option.

18. Click **Finish** to accept the values.

    Note: Sigtran filters can be combined using the Combination Filter operation.

    Note: A choice can be made at this point to use "chunk forwarding" or to the forward whole IP packet (IP raw.).

    Note: To complete the filtering process the filter must be connected with a data flow, traffic classification and dataflow process in IXP. See Routing PDUs to xDR Builders for SigTran or Routing PDUs to xDR Builders for more information.

Modifying a SigTran SS7-SIO PDU Filter

Complete these steps to modify a SigTran SS7-SIO PDU Filter:

1. Select the **SigTran SS7-SIO Filter** that needs modification.
2. Click **Modify** on the tool bar.
3. Modify the **appropriate information**.
4. Click **Modify**.
5. The *changes* are saved.

Deleting a SigTran SS7 SIO PDU Filter

Complete these steps to delete a SigTran SS7 SIO PDU Filter:

1. Select the **SigTran SS7 SIO PDU Filter** to be deleted.
2. Click **Delete** on the tool bar.
3. Click **OK** at the prompt.
4. The *filter* is deleted.

Adding a SigTran GT PDU Filter

1. Select **Acquisition > PDU Filters**.
2. Click **Add** on the tool bar.
3. Select **SigTran - Protocol**.
4. Click **Next**.
5. Select **SS7 Protocol Filters**.
6. Click **Next**.
7. Select **Global Title**.

   Note: If No Global Title is selected then complete steps 9-13 before clicking Finish.

   Note: In step 13 only Call Type is used for Non-Global Title SigTran filters.

8. Click **Next** to move to the Global Title filter screen.

   The table describes the fields on the Global Title screen.

Field	Description
Filter Name	User-defined name for filter.
Description	Enables you to describe the characteristics of the filter
Protocol	Shows the protocols you can use: • M2PA • M3UA • M2UA
SCCP Format	Lists the SCCP formats available: • ITU • ANSI
MTP3 Format	Lists the MTP3 formats available: • ITU • ANSI • Japan
Call Type	Lists the three different call types available: • Calling • Called • Both
Numbering Plan	Lists the different numbering plans available: • Unknown • ISDN/telephony numbering plan - E.164 • Generic • Data numbering plan - X.121 • Telex numbering plan - F.69 • Maritime mobile numbering plan - E.210/E.211 • Land mobile numbering plan - E.212 • ISDN/mobile numbering plan - E.214 • Private network or Network-specific numbering plan • Reserved
Nature of Address	• International • National
Global Title Value	A valid number.
Add to List	Adds the Id information entered to the GT List.
GT List	Show list of GT combinations created
Filter Expression	Shows the expressions and combinations that have been created from the use of the GT list and operators.
Logical Operators	Provides the following operators: • And = conjunction between two sub-filters • Or = disjunction between two sub-filters • Not = operator means negation of the sub-filter

Field	Description
	• ( ) = used to group sub-filters and modify the priority of operators
Select / Remove buttons	Clicking Select, adds a highlighted SIO to the Filter Expression Field. Clicking Remove removes the highlighted SIO from the list in the Filter Expression field.
Finish button (not shown)	Saves filter settings based on the information shown in the Filter Expression field.

TABLE 84: SIGTRAN SS7 GLOBAL TITLE (GT) SCREEN FIELDS

9. Enter in the **Filter Name**.
10. (Optional) Enter a **Description**.
11. Select the **Protocol** for the filter.
12. Select a **SCCP** and **MTP3 Format**.
13. Select a **Call Type, Numbering Plan, Nature of Address,** and **Global Title Value**
14. Click **Add** to list.
15. Select the **GT** from the *GT* list.
16. Click **Select** to add the expression to the Filter Expression list.
    To remove an expression from the field, click **Remove** on the bottom right side of the screen.

    Note: To create a more complex expression, use the **Logical Operator(s)**. A name then can be assigned to the Filter as well as a description of the filter.

    Note: More than one filter can be created.

    Note: This filter can be used in conjunction with other filters using the Combination Filter option.
17. Click **Finish** to accept the values.

    Note: Sigtran filters can be combined using the Combination Filter operation.

    Note: A choice can be made at this point to use "chunk forwarding" or to forward the whole IP packet (IP raw.).

    Note: To complete the filtering process the filter must be connected with a data flow, traffic classification and dataflow process in IXP. See Routing PDUs to xDR Builders for SigTran or Routing PDUs to xDR Builders for more information.

Modifying a SigTran GT PDU Filter

Complete these steps to modify a SigTran GT PDU Filter:

1. Select the **SigTran GT PDU Filter** that needs modification.
2. Click **Modify** on the tool bar.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a SigTran GT PDU Filter

Complete these steps to delete an SigTran GT Filter:

1. Select the **SigTran GT Filter** to be deleted.
2. Click **Delete** on the tool bar.
3. Click **OK** at the prompt.
   The *filter* is deleted.

Adding a SigTran SS7 SSN PDU Filter

Complete these steps to add a SigTran SS7 SSN Filter:

1. Select **Acquisition > PDU Filters** from the object menu.
   The *PDU Filters* list screen opens.
2. Click **Add** on the tool bar.
   PDU Filter Family screen opens.

3. Select **SigTran - Protocol**
4. Click **Next**.
   The *SigTran* screen opens.
5. Select **SS7 Protocol Filter**.
   The *SigTran SS7 Filters* screen opens.
6. Select **SS7 - Subsystem Number Filter**.
7. Click **Next**.
8. Select **Subsystem Number**.
9. Click **Next**.

   The table describes the fields on this screen.

Field	Description
Filter Name	User-defined name for filter.
Description	Enables you to describe the characteristics of the filter
Protocol	Lists the sigtran protocols to use: • M2PA • M3UA • M2UA
SCCP Format	Lists the types of sccp formats available: • ITU • ANSI
MTP3 Format	Lists the MTP3 formats available: • ITU • ANSI • Japan
Calling Type	Lists the call type to be used: • Calling • Called • Both
Subsystem Number Value	Enter the Subsystem Number Value to be used for the filter. (Range is integer 1-255)
Add to List	Adds the subsystem value to the SSN List.
Remove from List	Removes the subsystem value to the SSN List.
Logical Operators	Provides the following operators: • And = conjunction between two sub-filters • Or = disjunction between two sub-filters • Not = operator means negation of the sub-filter • ( ) = used to group sub-filters and modify the priority of operators
Select	Places a selected SSN and moves it to the filter expression list.
Filter Expression	Shows the finished expression to be used
Finish button	Saves filter settings based on the information shown in the Filter Expression field.

TABLE 85: SIGTRAN SS7 SSN FILTER SCREEN FIELDS

10. Type in the **Filter Name**.
11. (Optional) Type in a **Description** of the SigTran Filter.
12. Select a **Protocol** to be used.
13. Select a **SCCP Format** to be used.
14. Select a **MTP3 Format** to be used.
15. Select the **Call Type** to be used.
16. Enter the **Subsystem Number Value** to be used.
17. Click **Add** to List to place the SSN in the SSN List.
18. (Optional) Repeat steps 16 & 17 to place more SSN values in the SSN list field.
19. Select an **SSN** and click **Select** to place it in the Filter Expression field.
20. (Optional) **Select** the appropriate **Logical Operator(s)** to create more complex expressions.
21. Repeat steps 18 & 19 if more complex expressions are needed.

22. Click **Finish**.
    The *filter* is added.

    Note: Sigtran filters can be combined using the Combination Filter operation.

    Note: A choice can be made at this point to use "chunk forwarding" or to forward the whole IP packet (IP raw.)

    Note: To complete the filtering process the filter must be connected with a data flow, traffic classification and dataflow process in IXP. See Routing PDUs to xDR Builders for SigTran or Routing PDUs to xDR Builders for more information.

Adding a SigTran SS7 SSN PDU Filter-No Subsystem Number

Complete these steps to add a SigTran SS7 SSN Filter:

1. Select **Acquisition > PDU Filters** from the object menu.
   The *PDU Filters* list screen opens.
2. Click **Add** on the tool bar.
   PDU Filter Family screen opens.
3. Select **SigTran - Protocol**
4. Click **Next**.
   The *SigTran* screen opens.
5. Select **SS7 Protocol Filter**.
   The *SigTran SS7 Filters* screen opens.
6. Select **SS7 - Subsystem Number Filter**.
7. Click **Next**.
8. Select **No Subsystem Number**.
9. Click **Next**.

   The table describes the fields on this screen.

Field	Description
Filter Name	User-defined name for filter.
Description	Enables you to describe the characteristics of the filter
Protocol	Lists the sigtran protocols to use: • M2PA • M3UA • M2UA
SCCP Format	Lists the types of sccp formats available: • ITU • ANSI
MTP3 Format	Lists the MTP3 formats available: • ITU • ANSI • Japan
Calling Type	Lists the call type to be used: • Calling • Called • Both
Subsystem Number Value	Enter the Subsystem Number Value to be used for the filter. (Range is integer 1-255)
Add to List	Adds the subsystem value to the SSN List.
Remove from List	Removes the subsystem value to the SSN List.
Logical Operators	Provides the following operators: • And = conjunction between two sub-filters • Or = disjunction between two sub-filters • Not = operator means negation of the sub-filter • ( ) = used to group sub-filters and modify the priority of operators

Field	Description
Select	Places a selected SSN and moves it to the filter expression list.
Filter Expression	Shows the finished expression to be used
Finish button	Saves filter settings based on the information shown in the Filter Expression field.

TABLE 86: SIGTRAN SS7 SSN FILTER SCREEN FIELDS

10. Type in the **Filter Name**.
11. (Optional) Type in a **Description** of the SigTran Filter.
12. Select a **Protocol** to be used.
13. Select a **SCCP Format** to be used.
14. Select a **MTP3 Format** to be used.
15. Select the **Call Type** to be used.
16. Click **Finish**.
17. The *filter* is added.

Modifying a SigTran SS7 SSN PDU Filter

Complete these steps to modify a SigTran SS7 SSN Filter:

1. Select the **SigTran SS7 SSN Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a SigTran SS7 SSN PDU Filter

Complete these steps to delete a SigTran SS7 SSN Filter:

1. Select the **SigTran SS7 SSN Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *filter* is deleted.

About SigTran Combination Filter

SigTran Combination filters are literally combinations of the other three types of SigTran Filters. This type of filter provides greater flexibility in routing PDUs.

Adding a SigTran Combination PDU Filter

Complete these steps to add a SigTran Combination Filter:

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.

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. Click **Next**.
   The SigTran screen opens.
4. Select SigTran Combination Filter
   The *Combination Filters* screen opens.

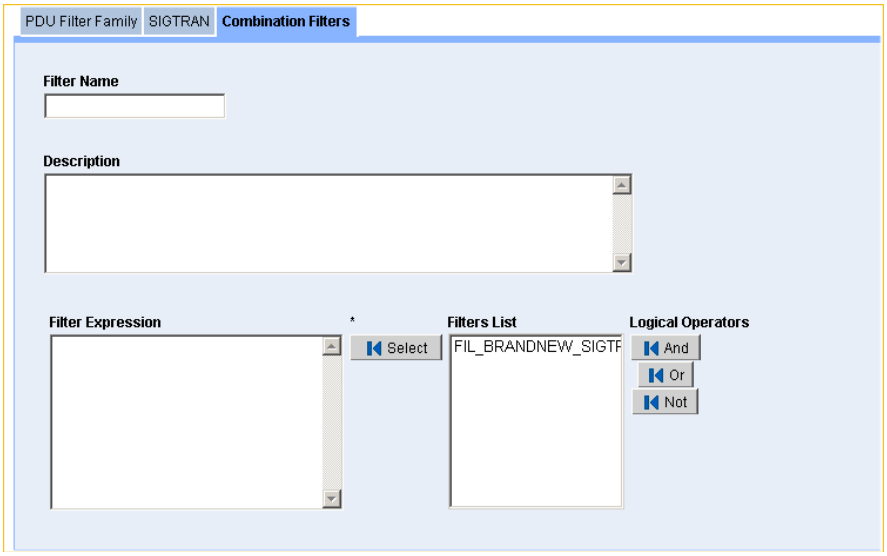


Figure 130: Combination Filters Screen

The table describes the fields on this screen.

Field	Description
Filter Name	User-defined name for filter.
Filter Description	Enter pertinent information for the combination filter.
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.
Finish button (not shown)	Saves the information to the system.

TABLE 87: COMBINATION FILTER SCREEN FIELDS

5. Type in the **Filter Name**.
6. (Optional) Type in a **Description** of the Filter.
7. Type in or select a **Filter Expression** in the *Filter Expression field*.
8. Click **Select**.
   The *expression* is added to the Filters List.
9. Select a **Logical Operator (And, Or, Not)**, by clicking the appropriate *Operator*.
   From the *pull-down* menu.
10. Click **Done**.
    The *Combination Filter* is added to the object tree in alphanumerical order.

Modifying a SigTran Combination PDU Filter

Complete these steps to modify a SigTran Combination Filter:

1. Select the **SigTran Combination Filter** that needs modification.
2. Select **Modify**.
3. Modify the **appropriate information**.
4. Click **Modify**.
   The changes are saved.

Deleting a SigTran Combination PDU Filter

Complete these steps to delete a SigTran Combination Filter:

1. Select the **SigTran Combination Filter** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The filter is deleted.

About PDU Dataflows

PDU Data Flows are used to group Linksets and/or Associations that are being captured on the IMF/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 xMF (IMF or 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.

The following PDU dataflows can be configured in a subsystem:

- GPRS dataflows (for PMF only)
- SS7 MSU dataflows (Including BICC monitoring over SigTran and L2 LSSU)
- IP dataflows
- Q.752 dataflows

Note: In an IMF subsystem there is a hard-coded limit of 20 input streams a dataflow can be routed per server.

Adding a GPRS Gb Dataflow

Complete these steps to add an GPRS data flow for a PMF subsytem.

1. Select **Acquisition > Sites > Subsystem >PDU Data Flows > GPRS > Add**.
2. Type in the **Name** of the *Gb dataflow*.
3. (Optional) Type in a **description** of the dataflow record.
4. Click **Next**.
5. Select a **Gb Filter** from the *drop-down* menu.
6. Enter the **Number** for packet truncation.
7. Click **Next**.
8. Click the **Gb Link** icon.
9. Enter the **Gb Link Name**.
10. Click **Apply Filter**.
11. Select **Gb Link Record** from the list.
12. Click **Select**.
13. Click **Close**.
14. Click **Add**.
    The *GPRS dataflow* 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.

Modifying a GPRS Gb Dataflow

Complete these steps to modify a GPRS Gb Dataflow:

1. Select the **GPRS Gb Dataflow Record** to be modified.
2. Click **Modify**.
   The Modify screen opens.
3. Make the **necessary modifications**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a GPRS Gb Dataflow

Complete these steps to delete an GPRS Gb Dataflow:

1. Select the **GPRS Gb Dataflow Record** to be deleted.
2. Click **Delete**.
3. Click **OK** at the prompt.
   The *record* is deleted.

Adding a SS7 Dataflow

Complete these steps to create a SS7 PDU dataflow.

1. Select **Acquisition > Site > Subsystem > PDU Data Flows > SS7**.
   The Add SS7 dataflow list screen opens.

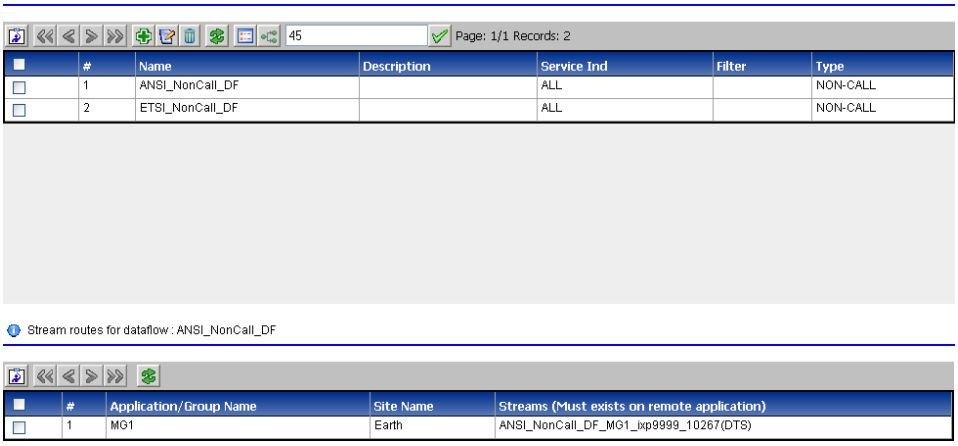


Figure 131: SS7 Dataflow List Screen

2. Click Add on the tool bar.
3. Type in the Name of the SS7 dataflow.
4. (Optional) Type in a Description of the dataflow record.
5. Click Next.

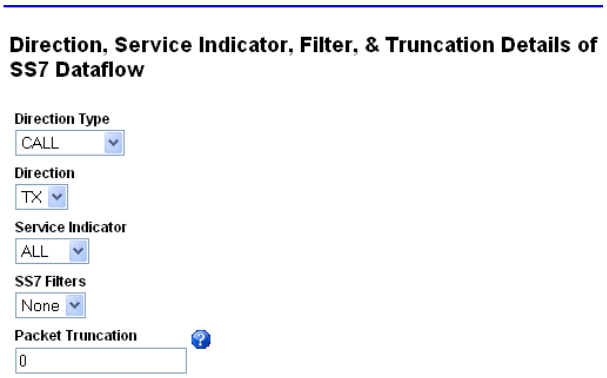


Figure 132: Direction, Service Indicator, Filter & Truncation Details Screen

The table describes the default fields on this screen.

Note: For LSSU support (selecting the Non-Call), the screen has only three fields with the following choices:

- Direction Type - Non-Call
- Direction - TX, RX or BOTH
- Service Indicator - ALL

Field	Description
Direction Type	Drop-down menu has the following options: • CALL or MSUCALL: For certain SCCP, TUP, or ISUP Service Indicator Message Types. Direction for this Direction Type can be only either RX or TX. • MSU: All other MSU data types including BICC over SigTran. Call direction can be RX, TX or Both • Non_Call: (For LSSU support.) The Direction for this message type can be RX, TX or Both. The service indicator will always be "ALL"
Direction	What is the source of the dataflow Either RX, TX, or Both (MSU and LSSU)
Service Indicator	• Drop-down menu of supported SS7 types **Note:** For LSSU support ALL is the only selection
SS7 Filters	Select the filters to be associated with the dataflow.
Packet Truncation	Enter an integer for the maximum length, in bytes, for each PDU. The range is between 0-4000.
Cancel / Previous /Next	Click on one of the following: • Cancel: Information is not saved. • Previous: Returns you to the SS7 Dataflow Information screen. • Next: The Monitored Linksets Details screen opens.

TABLE 88: DIRECTION, SERVICE INDICATOR, FILTER&TRUNCATION DETAILS OF SS7 DATAFLOW SCREEN FIELDS

6. Select the **Direction Type. (MSU, Call, or NON_CALL)**.
7. Select the **Direction. (Both, Rx, Tx)**
8. Select the **Service Indicator**. (For Non_Call only ALL is available).
9. Select a **SS7 Filter**.
10. Enter the **Length of the PDU** in the *Packet Truncation* field. (Integer between 0-4000)
11. Click **Next**.
    The Monitored Linkset Details screen opens.

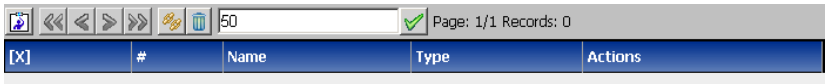


Figure 133: Monitored Linkset Details Screen

12. Click the **Linksets** icon to show the existing linksets.
    You can also create linksets if you need to.
13. Click **Add** to add the record to the database.
    SS7 Linkset Selector Filter opens.

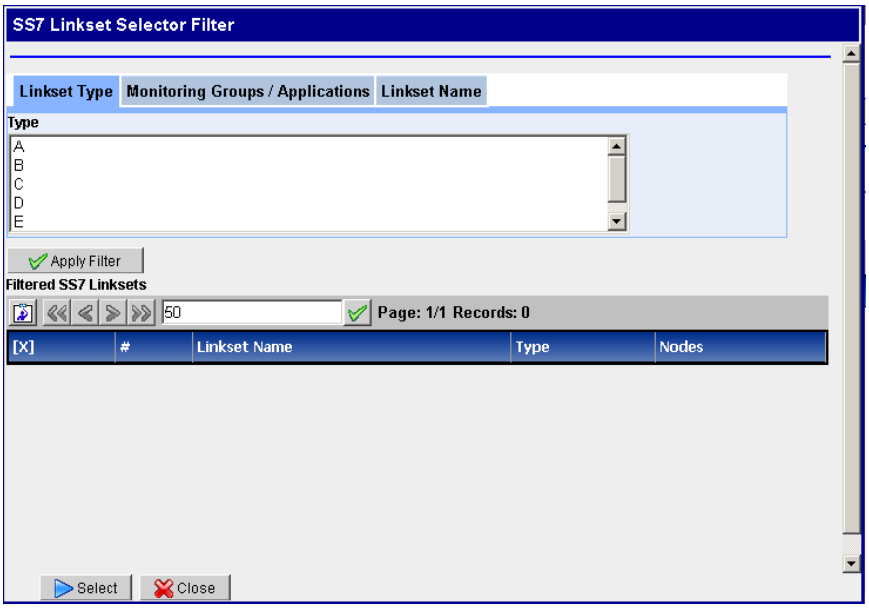


Figure 134: SS7 Linkset Selector Filter Screen

14. Select the **Linkset Type (A-F)** from the Linkset Type tab.
15. (Optional) Select an **option** from the Monitoring Group/Applications tab.
16. Select the **Linkset Name** tab and enter a **Linkset Name**.
17. Click **Apply Filter** to apply the filter you created.
18. Select a **Filtered Linkset** from the list at the bottom table.
19. Select the **Monitored Linkset**.
20. Click **Add**.

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

Managing MFP Streams to Third Party Applications

PDU Dataflows can be linked to ICP or third party applications. Complete these steps create a Stream from a PDU Dataflow:

1. Click **Manage MFP Routes** (to an ICP or third party application) to add the routes to a Dataflow.

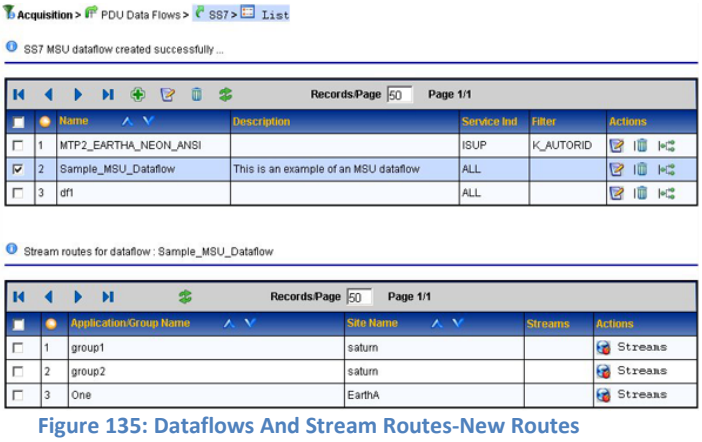


Figure 135: Dataflows And Stream Routes-New Routes

2. Click **Manage MFP Routes** (in Actions column of routes table) to add new streams. The add *Route* screen opens.

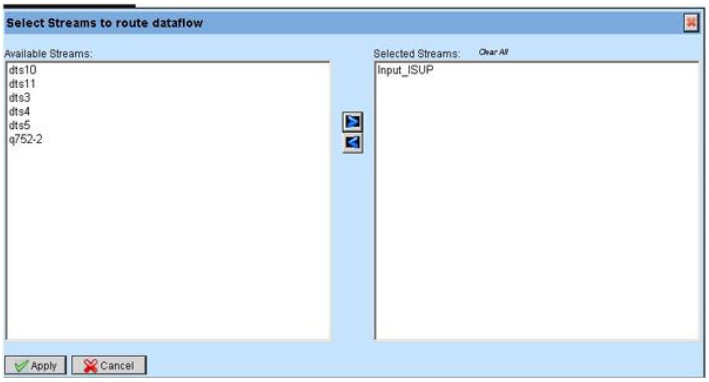


Figure 136: Dataflows And Stream Routes-Streams Screen

3. Select the **Available Routes** for the Dataflow.
4. Click the **Right Arrow**.
5. Click **Apply**.
   The *Stream* is added to the Dataflow.

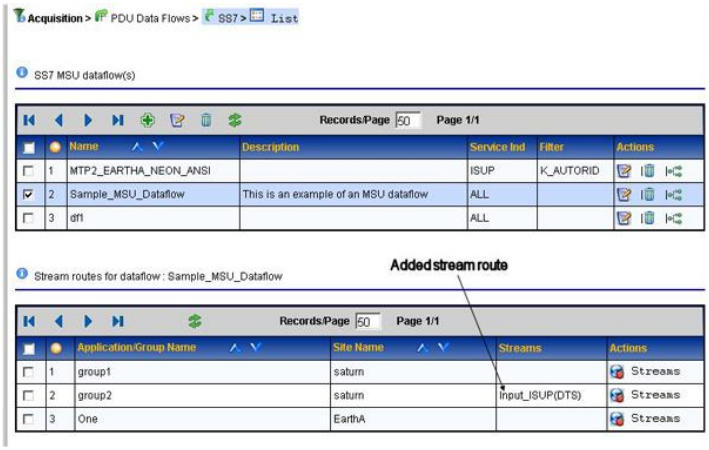


Figure 137: Dataflows and Routes Screen

Modifying a SS7 Dataflow

Complete these steps to modify an SS7 Dataflow:

1. Select the **SS7 Dataflow Record** to be modified.
2. Click **Modify**.
   The *Modify* screen opens.
3. Make the **necessary modifications**.
4. Click **Modify**.
   The *changes* are saved.

Deleting a SS7 Dataflow

Complete these steps to delete an SS7 dataflow

1. Select the **SS7 Dataflow Record** to be deleted.
2. Click **Delete**.
3. Click **OK** at the prompt.
   The *record* is deleted.

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.

IMF

When you create an IP dataflow in IMF, you can utilize fastcopy to select one or more Ethernet devices connected to a selected IMF 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.

You can use these options to send information about the direction of IP traffic to the IXP. To do this you must select the Way Management option and enter the specific network and/or host address(es) you want the directional information for. When this option is used, the data sent to the IXP will indicate whether the IP address is the source, Tx, or the destination, Rx, address in the IP packets.

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 Using PMF

Complete these steps to create an IP data flow:

1. Select **Acquisition >Site > PDU Data Flows > IP**.
   The IP Dataflow list screen opens.

Figure 138: IP Dataflow List Screen

2. Click **Add**.
   The *Add* screen opens.

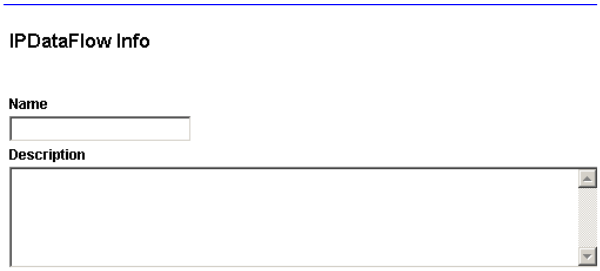


Figure 139: IP Data Flow Add Screen

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.

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) • 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. If this is not selected, IP address directional information is not be included in the information sent to the IXP. • 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		Click on one of the following: • Reset: Restores original settings. • Cancel: Information is not saved.

Section	Field	Description
		• Previous: Returns you to the Add IP Dataflows screen. • Next: The Add IP Dataflows Network View screen opens.

TABLE 89: ADD/MODIFY IP DATAFLOW SCREEN FIELDS

6. (Optional for Load Sharing) Select the **Number of Destinations** that will be used in load sharing (must be two or more).
7. (Optional) Select whether the system should utilize the **GTP User Plane** for loadsharing. action.
8. (Optional) Select (or not) whether the system should utilized the **GTP Control** Plane to all shared destinations.
9. Type in a valid **IP Address(es)**.
10. Click **Add**. The IP address is added to the IP Address list.
11. Click **Next** to move to the IP Data Flow Truncation Configuration scren.
12. Enter a **Packet Truncation Value** (integer).
13. (Optional) Select any **Annotations** you want to be associated with the dataflow.
14. Click **Next** to move to the IP Data Flow Stream Configuration screen.
    The *Traffic Classifications* screen opens.

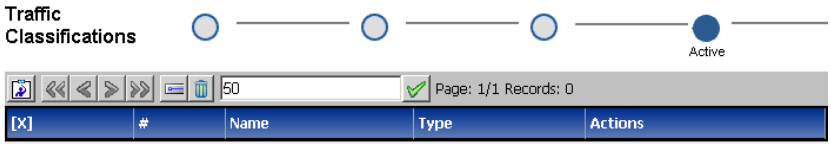


Figure 140: Traffic Classifications Screen

15. Click **Select Traffic Classifications** on the tool bar.
    The *Traffic Classification* Selector screen opens.

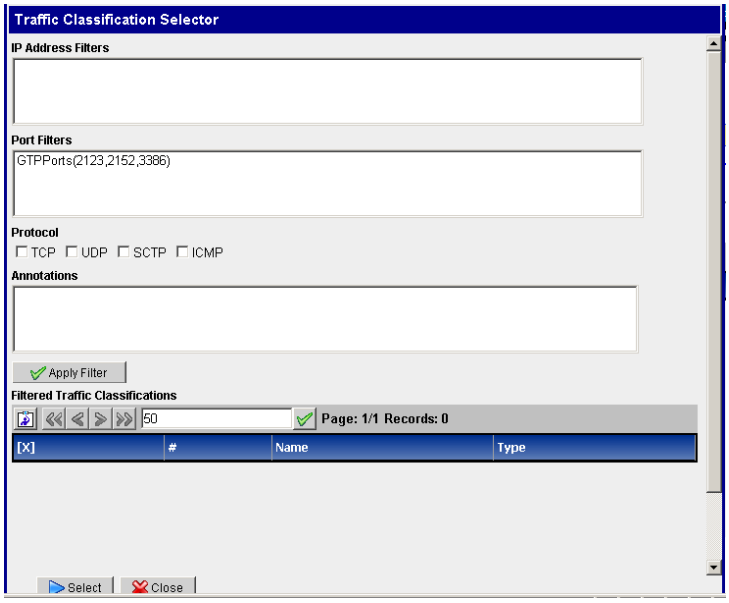


Figure 141: Traffic Classifications Selector Screen

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.

Adding an IP Dataflow Using IMF FastCopy

Complete these steps to create an IP dataflow using IMF FastCopy.

1. Select **Acquisition >IMF Site > PDU Data Flows > IP**.
   The *IP Dataflow* list screen opens.

Figure 142: IP Dataflow List Screen

2. Click **Add**.
   The *Add* screen opens.

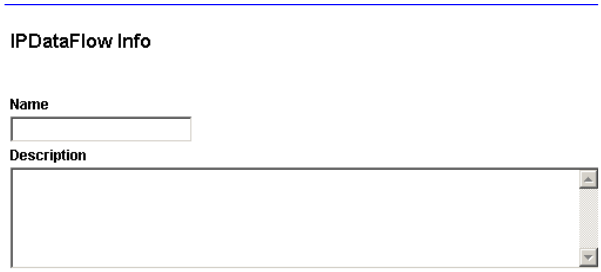


Figure 143: IP Data Flow Add Screen

3. Type in the **Name of the IP Dataflow**
4. (Optional) Type in a **Description** of the dataflow record.
5. Click **Next**.

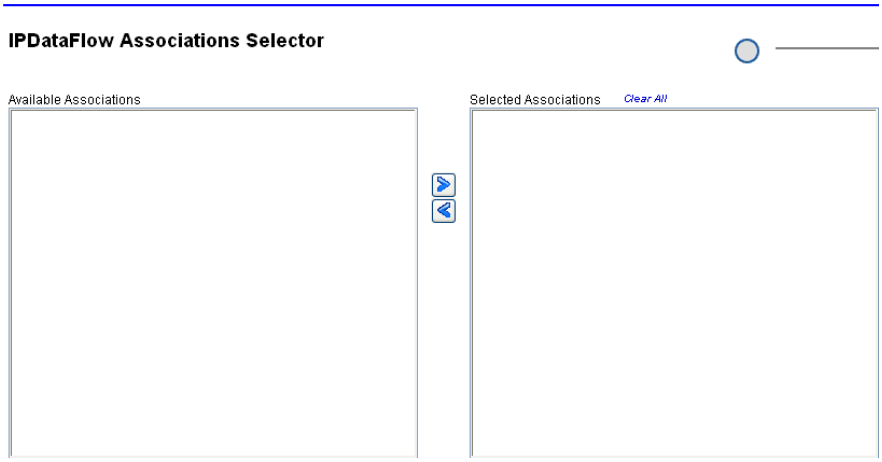


Figure 144: IP Dataflow Associations Selector Screen

6. Select one or more **Available Associations**.
7. Click the **Right Arrow** to place them into the *Selected Associations Field*.
8. Click **Add**.

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

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 SS7 Q.752 Dataflows

This dataflow is used to monitor Q.752 data, which can be sent to an IXP. A Q.752 dataflow definition consists of a dataflow name and a description.

Adding an SS7 Q.752 Dataflow

Complete these steps to create a Q.752 Dataflow:

1. Select **Acquisition > PDU Data Flows > Q.752 Dataflows**.
2. Right-Click and select **Add**.
   The *Add Q.752 Dataflow* screen opens.

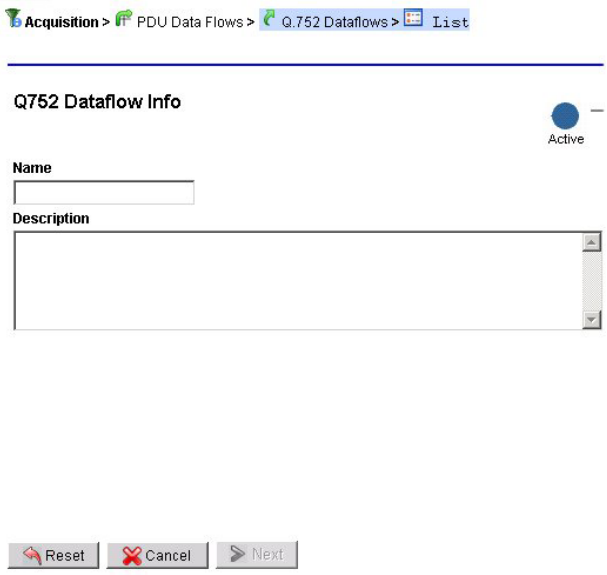


Figure 145: Add Q.752 Dataflow Screen

3. Type in the **Name of the MSU Dataflow**.
4. (Optional) Type in a **Description** of the dataflow record.

5. Click **Next**.
   The *Q.752 Dataflow View Details* screen opens.

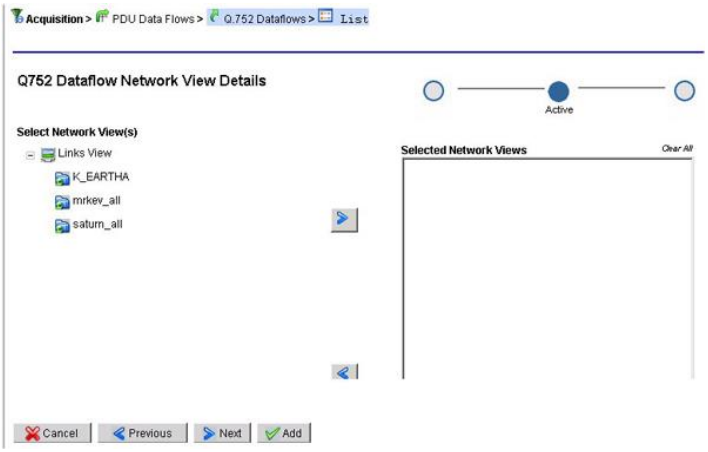


Figure 146: Network View Details Of Q.752 Record Screen

6. Expand the **Network Views Icon** to show the existing views.
7. Select the **View(s)** you want associated with the dataflow.
8. Click the **right arrow** to send the selected view to the selection field.
9. Click **Add** to add the record to the database.

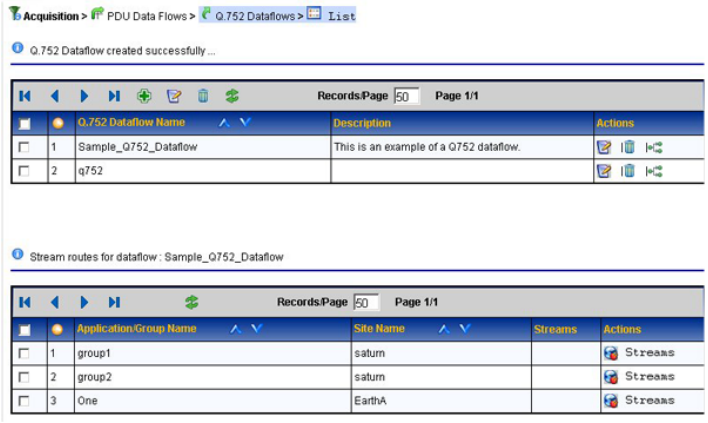


Figure 147: Dataflow Summary Screen

10. Select the **Dataflow** that was added.
11. Click **Routes** (far right icon in Actions column) to add the routes to the dataflow shown above.
12. Select the **Dataflow Route** (bottom table) that will have the streams.
13. Click **Route Streams** (in Actions column of routes table) to add new streams.
    The *Add Streams* screen opens.

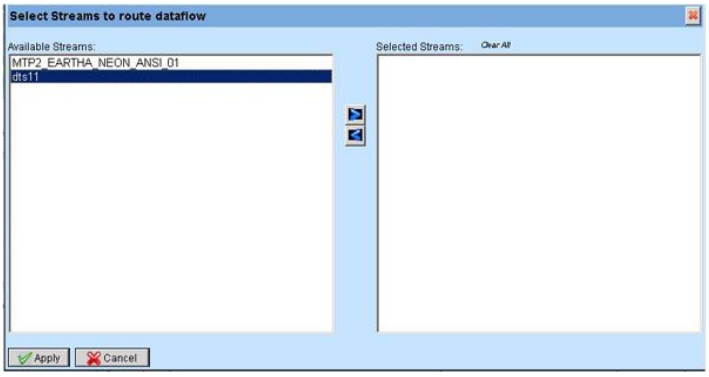


Figure 148: Dataflows And Stream Routes-Streams Screen

14. Select the **Available Streams** for the dataflow.
15. Click the **Right Arrow**.
16. Click **Apply**.
    The *stream* is added to the dataflow.

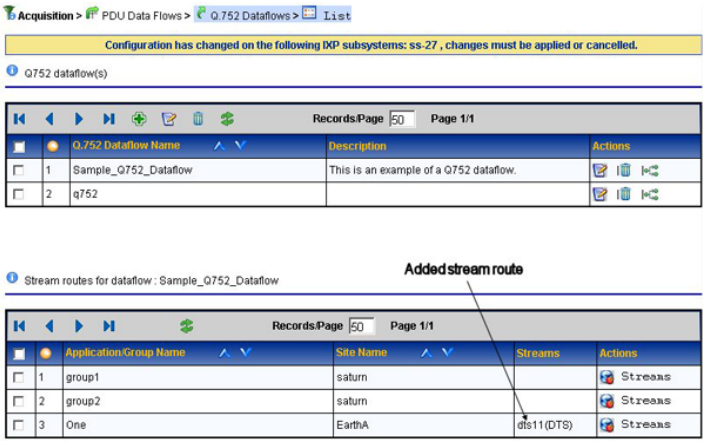


Figure 149: Dataflows And Stream Routes Streams Screen

17. You must now synchronize the subsystem.

Modifying an SS7 Q.752 Dataflow

Complete these steps to modify an SS7 Q.752 Dataflow:

1. Select the **SS7 Q.752 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. Click **OK** at the prompt.
   The *record* is deleted.
6. You must now **Synchronize** the subsystem.

Deleting an SS7 Q.752 Dataflow

Note: You must de-select any IP stream that is associated with an IP dataflow before deleting it.

1. Select the **Q.752 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 PIC 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 Next-Gen IMF or PMF subsystems. 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.

About SS7 OAM Alarms

This section describes how to use CCM to enable and disable Eagle OAM alarms. The Eagle STP reports alarms to an IMF subsystem. The IMF subsystem forwards these alarms to *ProAlarm* application. The user can enable or disable forwarding of such alarms globally. For a listing of OAM alarms, see *ProAlarm Configuration User Guide*.

Enabling and Disabling SS7 OAM Alarms

Complete these steps to enable or disable Eagle OAM alarms:

1. Select **Acquisition> Alarms > Eagle OAM > List**.
   The screen opens showing the list of Eagle OAM alarms shown below.

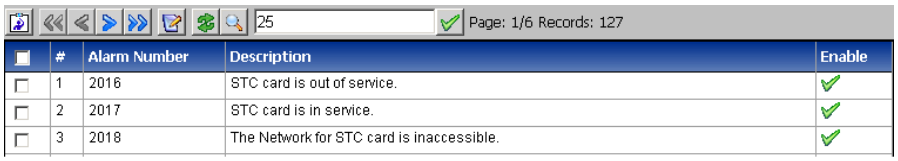


Figure 150: Alarms Configuration Screen

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

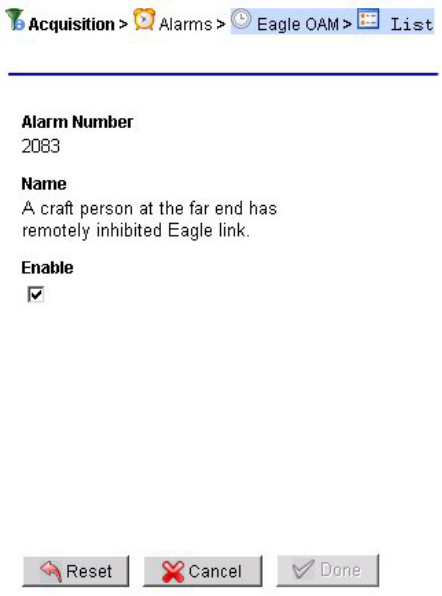


Figure 151: Modify Eagle OAM Alarm Configuration Screen

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.

Managing SLOR Thresholds

This section describes how the Q.752 alarms parameters are set by the CCM application. The IMF and PMF servers examine the received PDUs and count types of events. You can set threshold values for these counts. When the count exceeds or falls below the specified level, an alarm is generated.

There are three levels of SLOR alarms:

- High - Default threshold is 40 %
- Low - Default threshold is 20%
- Hold - Default threshold is 5%

Note: The thresholds are set for all IMF across subsystems. You cannot have different thresholds for different subsystems.

Note: It is recommended that a lower SLOR threshold should not be set above a higher threshold. For example, the threshold for a Low SLOR set at 50% while the High SLOR threshold being set to 40%.

Setting Signaling Link Occupancy Counter (SLOR) Thresholds

Complete these steps to modify a SLOR threshold:

1. Select **Acquisition > Alarms > SLOR Threshold> List**.
   The *SLOR threshold configuration* screen opens shown below.

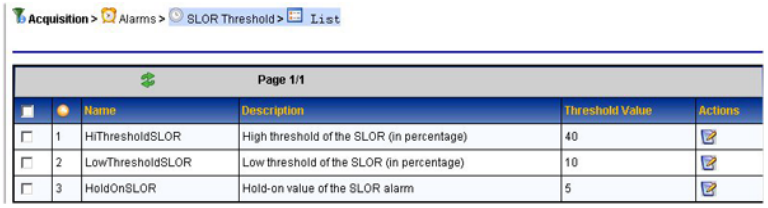


Figure 152: Slor Threshold List

2.Select the **Alarm** to be modified.
3.Click **Modify**.
The *Modify SLOR Threshold Configuration* screen opens with the alarm record details shown below.

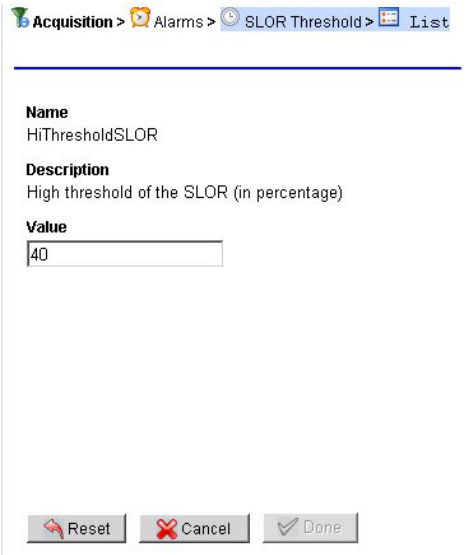


Figure 153: Modify SLOR Threshold Configuration Screen

4. Type in the new **Value** for the threshold.
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.

Managing Q.752 Alarms

This section describes how the Q.752 alarms are enabled or disabled by the CCM application. The IMF/PMF system can raise or clear alarms based on the counter thresholds. If an alarm condition is detected, it reports them to the IMF/PMF system. The IMF/PMF subsystem forwards these alarms to *ProAlarm* application. You can enable or disable forwarding of such alarms globally. For a listing of Q.752 alarms, see *ProAlarm Configuration User Guide*.

Enabling and Disabling Q.752 Alarms

Complete these steps to enable or disable a Q.752 alarm:

1. Select **Acquisition > Alarms >Q.752/SS7> List**.
   The *Q.752/SS7 Alarms Configuration* screen opens.

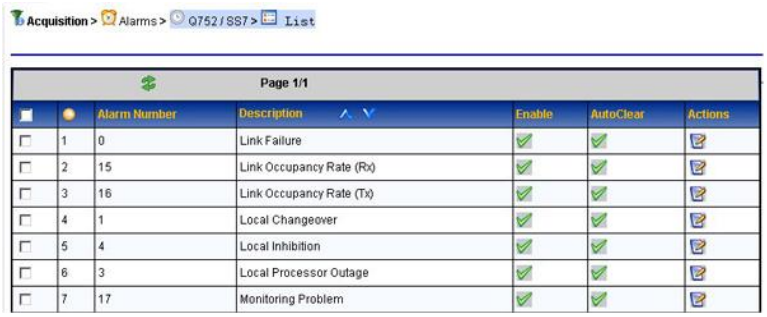


Figure 154: Q752/SS7 Alarms Configuration Screen

2.Select the **Alarm** to be enabled or disabled.
3.Click **Actions Icon** (modify) the Modify Platform Alarm Configuration screen opens with the alarm record details.

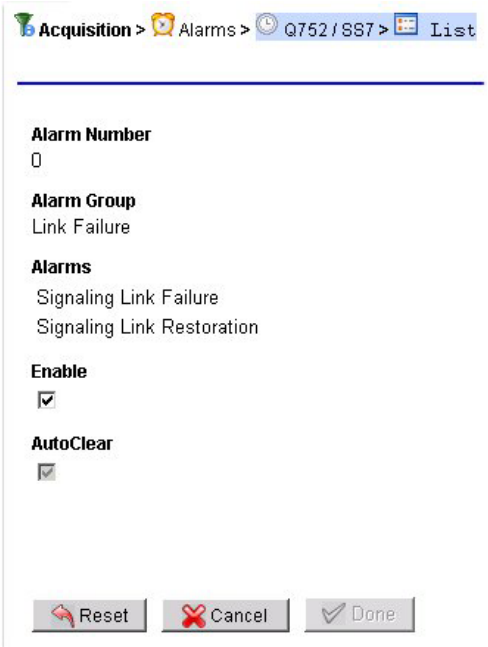


Figure 155: Modify Platform Alarm Configuration Screen

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.**Select** or **de-select** AutoClear function.
6.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.

About Resource ID Groups (RID)

Resource ID Groups (RID Groups) are used to create SS7 and Sigtran linksets. You manage Resource ID Groups using the Acquisition perspective.

About Auto RID

Auto RID provides two automatically configured RID groups: one for 'AUTO RID' with a value of 65535 and another for 'AUTO RID REVERSE' with a value of 65534. The figure below shows the default settings in the Resource ID group list screen. See About Auto RID for more information.

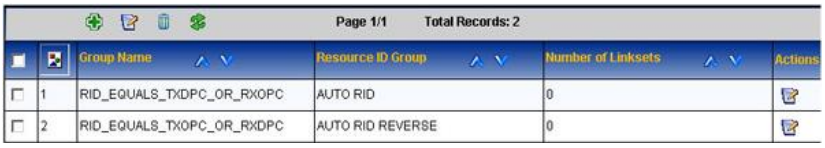


Figure 156: Modify Resource ID Group List Screen (Default)

Creating a Resource ID Group

Complete these steps to create a Resource ID Group:

1. Select **Acquisition > Resource ID Groups**.
   The *Resource ID* group list screen opens.

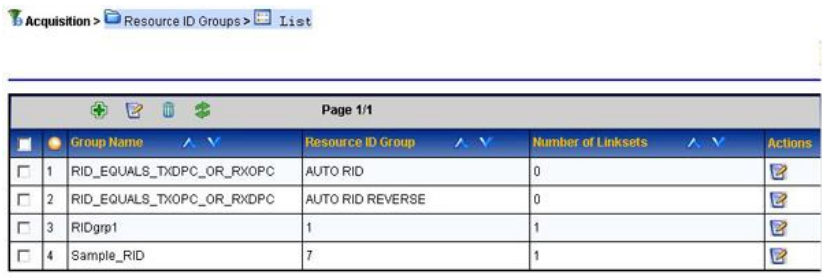


Figure 157: Resource ID Group List Screen

2. Click **Add**.
   The *Add* screen opens.

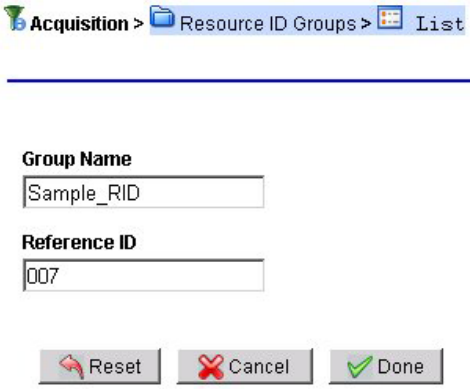


Figure 158: Resource ID Group List Screen

3. Type in the **Group Name**.
4. Type in the **Reference Group** (this must be a number)

   Note: The Referenced ID must be a number. No symbols or letters are allowed.

5. Click **Done**.
   The *Resource ID Group* is added to the Settings list.

Modifying a Resource ID Group

Complete these steps to modify a Resource ID Group:

1. Select the **Resource ID Group** that needs modification from the Object Tree.
2. Select **Modify**.
3. Modify the **appropriate information**.

   Note: You can only modify the Group Name. To change any other information, you must either add a new group, or delete the existing group and add it again with the new information.

4. Click **Modify**.
   The *changes* are saved.

Deleting a Resource ID Group

Complete these steps to delete a Resource ID Group:

Note: You cannot delete an RID group is it has linksets assigned to it or if the RID group is pre-defined.

1. Select the **Resource ID Group** to be deleted.
2. Select **Delete** from the menu.
3. Click **OK** at the prompt.
   The *group* is deleted.

About Q.752 Counters

Listing Q.752 Counters

Complete these steps to list a Q.752 counter:

1. Select **Acquisition > Q.752 counters > List**.
   The Q.752 Counters List screen opens shown below.

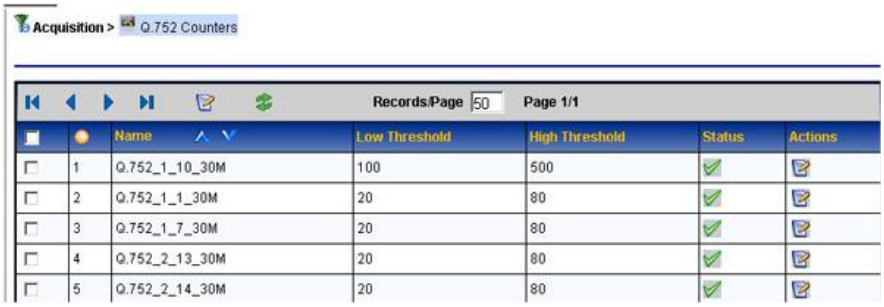


Figure 159: Q752 Counters List Screen

2. From the list you can **modify** a record(s).

Modifying a Q.752 counter Record

Complete these steps to modify a Q.752 counter record:

1. Select **Acquisition > Q.752 counters > List to open the Q.752 Counters List** screen.
2. Select the **Counter** to be modified.
3. Click **Modify** on the right-hand column.
   The *Q.752 Counter Modify Information* screen opens.

   Note: You can also select the record to be modified by clicking in the left-hand column then click the Modify button on the tool bar.

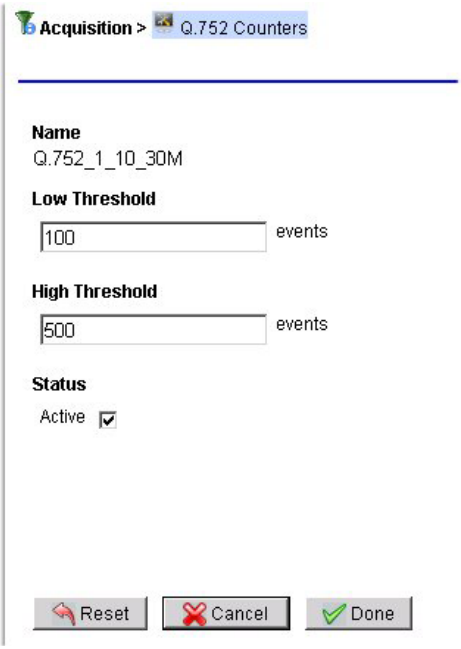


Figure 160: Q752 Counter Modify Information Screen

4. The only **Fields** you can modify are:

a) **Low Threshold** (number)
b) **High Threshold** (number)
c) **Active** (to activate or de-activate the counter)

5. Click **Done** to send the changes to the database.
   You are returned to the List screen.
6. Click **Refresh** to view changes.

   Note: It takes approximately 10 seconds for the changes to be registered by the xMF system.

Chapter 9: IXP Mediation

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 Subsytem in the *Mediation Perspective* to view a platform overview of the system.

DWH Server Name	IP Address	State
ixp7500-1a_DWH	10.240.23.202	ACTIVE

Server	Dataflow Processing	Type	Active	Input Stream(s)	Output
ixp7500-1a	Test_Build	Building	✓	Test	Test_BuildIS41DataBrokerTDRreconstitution
	Deepak_S	Building	✓	Test	B_Deepak_5
	Test_Dataflow_Assistant	Building	✓	Test	B_Test_Session_6
	Test_DA1	Building	✓	Test	B_Test_GP_7
	ReTest_DB_Build	Building	✓	Test	ReTest_DB_BuildMAPDataBrokerTDRreconsti
	DFP_Using_Assitant	Building	✓	Test	B_test_session1_11
	StoreDFP	Building	✓	Test	B_session001_12
	ixp7500PoolMonitor_1	Operation	✓	ixp7500PoolMonitor	O_ixp7500PoolMonitor_2 K_ixp7500AggSessionMonitor_3
	DB_Operate	Operation	✓	Test_BuildIS41DataBrokerTDRreconstitution	DB_Operate_operate
	Non_DB_Operate	Operation	✓	B_Deepak_5	Non_DB_Operate_operate
	Test_GP_8	Operation	✓	B_Test_GP_7	K_T_Stats_9
	StreamMonitor	Storage	✓	ixp7500StreamMonitor	ixp7500StreamMonitor
	BuildMonitor	Storage	✓	ixp7500BuildMonitor	ixp7500BuildMonitor
	OperateMonitor	Storage	✓	ixp7500OperateMonitor	ixp7500OperateMonitor
	PoolMonitor	Storage	✓	O_ixp7500PoolMonitor_2	ixp7500PoolMonitor
	BuildThreadMonitor	Storage	✓	ixp7500BuildThreadMonitor	ixp7500BuildThreadMonitor
	S_ixp7500AggSessionMonitor_4	Storage	✓	K_ixp7500AggSessionMonitor_3	ixp7500AggSessionMonitor
	S_Deepak	Storage	✓	B_Deepak_5	Deepak
	S_Test_GP	Storage	✓	B_Test_GP_7	Test_GP
	S_T_Stats_10	Storage	✓	K_T_Stats_9	T_Stats
	Test_RKS_CSV_Modify	Storage	✓	ReTest_DB_BuildMAPDataBrokerTDRreconstitution	CSV Feed: /opt/abc

Figure 161: 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.

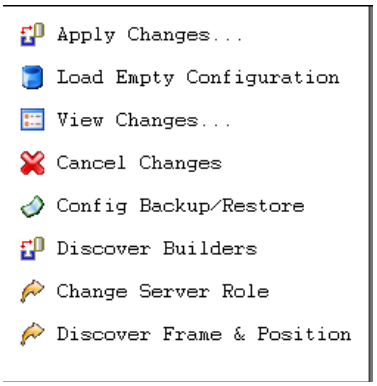


Figure 162: Subsystem Pop-Up Menu

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 synchronize the subsystem after you have modified the frame and position of a host in the IXP subsystem.

TABLE 90: IXP SUBSYSTEM POP-UP MENU OPTIONS

About applying changes to a subsystem (Synchronizing)

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 PIC system. CCM has an 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: Select the **Subsystem** that has been modified:

1. 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.
2. 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.

3. 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 effect, 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 Dataflow at the associated xMF subsystem. (For more information, see Avoiding Lost PDU Routes Due to Cancel Changes on an xMF 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 xMF Subsystem removes the existing configuration (any changes that have occurred) of that subsystem and restores the latest applied (active) configuration which includes Monitoring Groups in the case of IMF or Card/Port/Link Mapping and Traffic Classifications (TCs) in the case of PMF. Feeder Thresholds, xMF subsystem parameters and PDU Dataflow are preserved (but the PDU routes are not preserved). This action also enables the "Apply Changes" banner for that xMF subsystem. PDU dataflow routing can be restored either by modifying the Build DFPs on the IXP subsystem in order to re-associate the Dataflow 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.

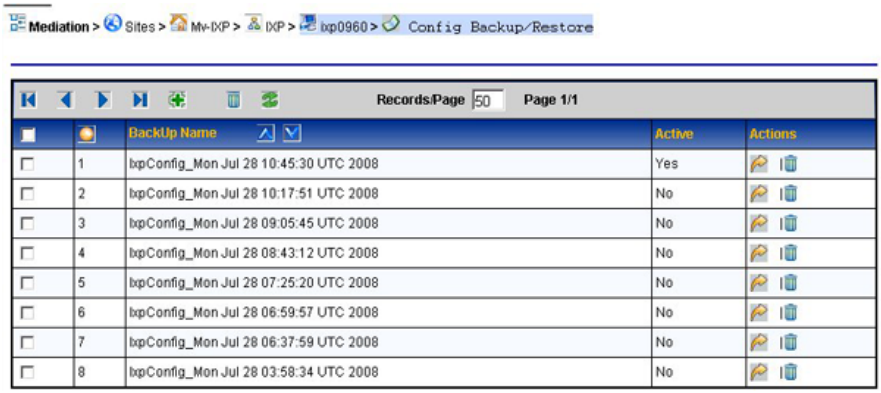


Figure 163: Archived List Of Configurations

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.

Figure 164: Discovery Results Screen

3. 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:

1. Select and right-click on the **IXP Subsystem** that needs the discovery process.
2. 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 server 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:

1. Select and right-click on the **IXP Subsystem** for the role change.
2. Select **Modify Server Roles** option.
   The *role change* screen opens for changing the primary and secondary server roles shown below.

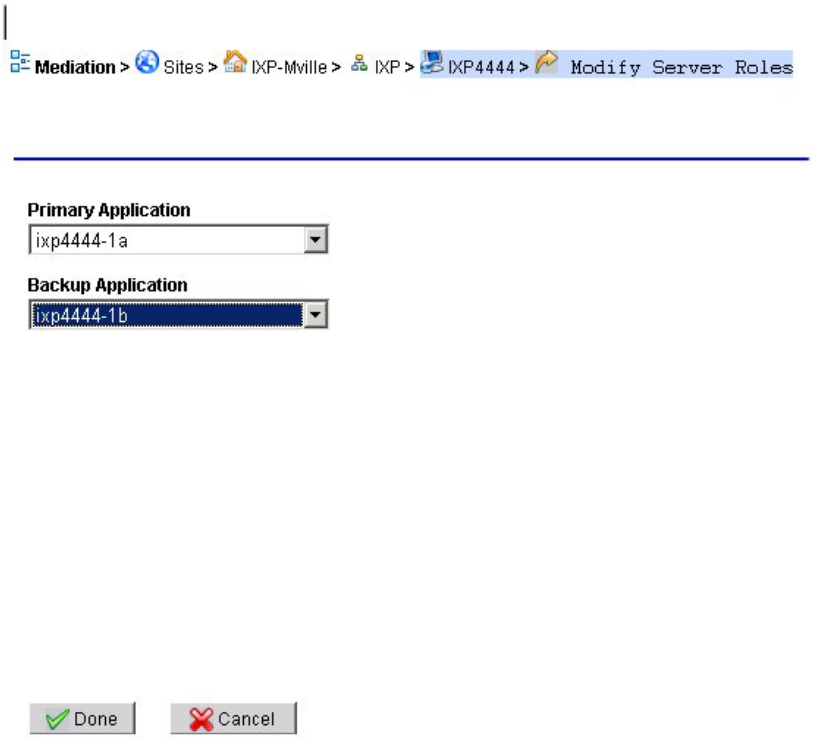


Figure 165: Server Role Change Screen

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.

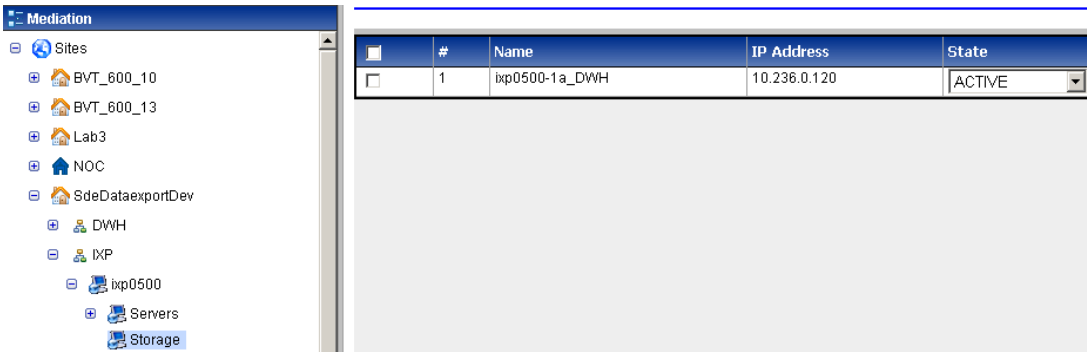


Figure 166: Storage Server Object and List Table

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*.

Figure 167: 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.

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.

TABLE 91: STORAGE POOL SERVER STATES

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, "Unable to execute query: ORA-00942: table or view does not exist." will appear.

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 92: VALUES ASSOCIATED WITH 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

TABLE 93: NSP APPLICATIONS EFFECTED BY EACH STATE

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 Dataflow
- xDR - that originate from external IXP Subsystems, legacy or current, and are connected to an XDR input stream.

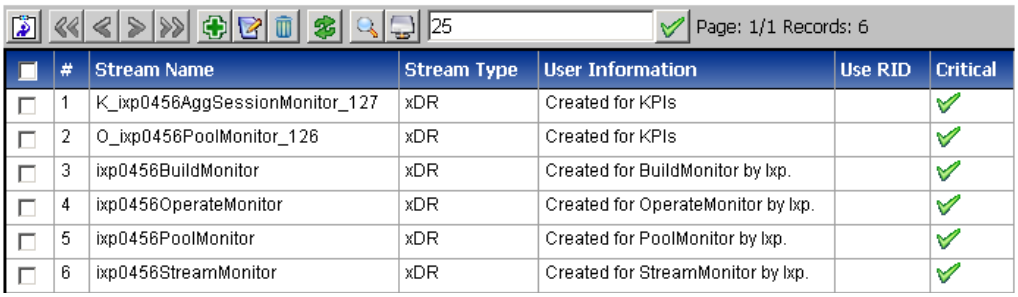
  Note: The XDR input stream name needs to match the stream name of the legacy subsystem.

  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 within 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.



25 Page: 1/1 Records: 6

#	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 Ixp.		✓
4	ixp0456OperateMonitor	xDR	Created for OperateMonitor by Ixp.		✓
5	ixp0456PoolMonitor	xDR	Created for PoolMonitor by Ixp.		✓
6	ixp0456StreamMonitor	xDR	Created for StreamMonitor by Ixp.		✓

Figure 168: 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.

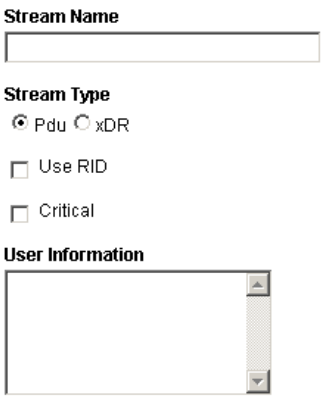


Figure 169: Add Streams Screen

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.

   Note: Click **Apply Changes** for the IXP subsystem for the changes to take effect.

Modifying a Stream

1. Select **Streams > List**.
   The *streams* list screen opens.
2. Select the **Stream** to be modified.
3. Click **Modify**.
   The screen for that *stream* opens shown below.

Figure 170: 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.

Adding an External PDU Stream

The primary purpose of the external PDU stream function is to configure IXP to accept PDUs from third party sources such as Neptune, Ocean or Cisco PMP.

Complete these steps to configure an external PDU Stream:

1. Select **Mediation > Site > IXP > Subsystem > External PDU Streams**.
   The External PDU Stream List screen opens.
2. Click **Add** on the tool bar or in the contextual menu.
   The *Add* screen opens.

Configuring an External PDU Stream for Neptune

Listed are the steps to configure external PDU stream for Neptune:

1. Select **Mediation > Site > IXP > Subsystem > External PDU Streams**.
   The *External PDU Stream List* screen opens.
2. Click **Add** or select external PDU stream and click **Modify** on the tool bar.

The external PDU stream edition screen opens.

3. Select **NEPTUNE** for **Type**. (Available only at creation. Disable during modification)
4. Enter **Name** to identify the name of the stream in the subsystem. (Available only at creation. Disable during modification)
5. Enter any **User information**.
6. Enter Neptune process flow **IP address** or select already registered Neptune probe.
   In case of probe selection, IP address, Login and Password fields are automatically completed and disabled.
7. Enter capture output **Port**.
   Port is 56000 for UP captures and 56001 for CP capture, xDR and Others.
8. Select whether the stream is **Active** or not.
9. Select if the stream is **Critical** or not.
10. Select the **Server** that will run the external stream interface process.
11. In case of no registered probe was selected, enter probe **Login** and **Password**.
12. Add **Additional parameters** ProbePortId to specify the output port ID on the probe.

Capture	Port:ID
User Plane 1	56000:0 to 56000:9
User Plane 2	56000:10 to 56000:19
User Plane 3	56000:20 to 56000:29
Control Plane	56001:0
RADIUS/DIAMETER	56001:8
DNS	56001:9
Traffic counter	56001:10
TCPDR	56001:11

TABLE 94: NEPTUNE OUTPUT CAPTURE PORT AND ID

13. Click **Create** or **Modify**.
14. **Synchronize** the IXP Subsystem to consolidate changes into the system.

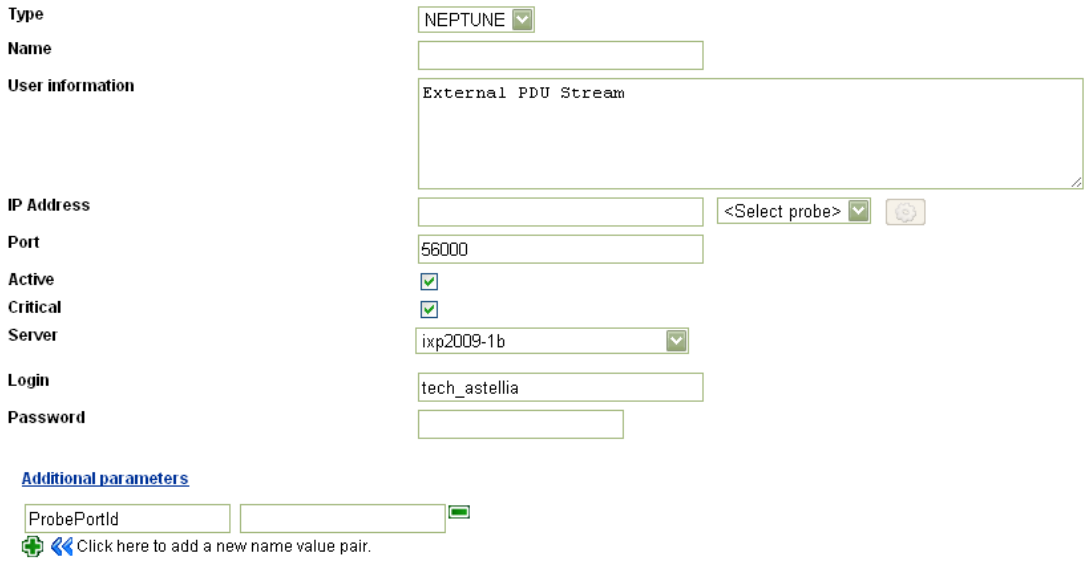


Figure 171: External PDU Stream for Neptune

Configuring way management feature

This feature should be used on Gb and IU-PS external PDU streams to configure the direction of each PDU received by the Neptune probe.

Listed are the steps to configure direction of received PDU:

1. Copy *Neptune loadbalancing files* on IXP primary server in directory /var/TKLC/ixp/NeptuneFiles

The *Neptune loadbalancing file* names must contain at least the type of IP addresses (SGSN, RNC or BSC).
Example:

- *Neptune loadbalancing file* name: *BSC_Gb_Topology1.txt*
- *Neptune loadbalancing file* contains:

Gb topology1 BSC for loadbalancing

NEPIPADDR
10.24.143.106
10.24.143.102
10.24.143.99

2. Run the script *UploadNeptuneFiles.sh* and check the log (/var/TKLC/log/ixp/UploadNeptuneFiles.log) on the IXP primary server in cfguser to update the table *GlobalParam* with the IP addresses held in the *Neptune loadbalancing files*,
3. In CCM, select **Mediation > Site > IXP > Subsystem > External PDU Streams**.

   The *External PDU Stream List* screen opens.
4. Select external PDU stream and click **Modify** on the tool bar.
5. Declare a new entry in the **Additional parameters**, call it **NeptuneFile** and give it the name(s) of the *Neptune loadbalancing file(s)*. The IP addresses provided in these files will be used by the *External PDU Stream* to define the direction of each PDU.
6. Click **Modify.**
7. **Synchronize** the IXP Subsystem to consolidate changes into the system.

Configuring loadsharing feature on IXP

This feature might be used on Gb and IU-PS external PDU streams to loadshare PDU to several DataFlow Processings. This feature is based on *Neptune loadbalancing files* like the way management feature.

1. In CCM, select **Mediation > Site > IXP > Subsystem > External PDU Streams**.

   The *External PDU Stream List* screen opens.
2. Select external PDU stream and click **Modify** on the tool bar.
3. Select a value for the **Loadbalancing** (between 2 and 8)
4. Declare a new entry in the **Additional parameters** call it **NeptuneFile** and give it the name(s) of the *Neptune loadbalancing file(s).* The IP addresses provided in these files will be used by the *External PDU Stream* to define the direction of each PDU and each *Neptune loadbalancing file* is used to feed one DataFlow Processing input stream.
   Example:
   - *Neptune loadbalancing file* names: GbBSCTopology1.*txt* and GbBScTopology2.*txt*
   - Name of *External PDU Stream*: NEP_1_Gb
   - **Loadbalancing**: 2
   - **Additional parameters** NeptuneFile: "GbBSCTopology1/GbBScTopology2"

   The streams NEP_1_Gb_1 and NEP_1_Gb_2 are automatically created.

Remark: If *External PDU Stream* is already used by a DataFlow Processing, then changing the **loadsharing** parameter generates the following error: "*Error while modifying External PDU Stream : 'NEP_1_Gb' under IXP subsystem 'ixp2009' This Stream is input for some dataflow processing(s) and hence can't be deleted*". It is necessary to modify Build DataFlow Processing in order to not use the stream *NEP_1_Gb* because loadsharing will create the stream *NEP_1_Gb_1*, *NEP_1_Gb_2*…

5. Click **Modify.**
6. **Synchronize** the IXP Subsystem to consolidate changes into the system.

Configuring filtering of FLOW CONTROL PDUs feature on IXP

This feature might be used on Gb external PDU streams to filter the FLOW CONTROL PDU in IxpInterface process.

The FLOW CONTROL PDU filter will be applied on:

- IPv4/UDP packets on port 20000,
- NS Unit Data type,
- BSSGP filtered types are 0x26, 0x27, 0x28 and 0x29 and all other kind of PDU will pass the filter,

1. In CCM, select **Mediation > Site > IXP > Subsystem > External PDU Streams**.

   The *External PDU Stream List* screen opens.
2. Select external PDU stream and click **Modify** on the tool bar.
3. Declare a new entry in the **Additional parameters** call it **EnableGbFlowControlFilter** and give it a value of 1 (0 is used to disable the feature)
4. Click Modify.
5. Synchronize the IXP Subsystem to consolidate changes into the system.

Configuring an External PDU Stream for OCEAN

Listed are the steps to configure external PDU stream for Neptune:

1. Select **Mediation > Site > IXP > Subsystem > External PDU Streams**.
   The *External PDU Stream List* screen opens.
2. Click **Add** or select external PDU stream and click **Modify** on the tool bar.
   The external PDU stream edition screen opens.
3. Select **OCEAN** for **Type**. (Available only at creation. Disable during modification)
4. Enter **Name** to identify the name of the stream in the subsystem. (Available only at creation. Disable during modification)
5. Enter any **User information**.
6. Enter **IP address** of the OCEAN probe.
7. Enter connexion **Port**.
   Default is 2030.
8. Select whether the stream is **Active** or not.
9. Select if the stream is **Critical** or not.
10. Select the **Server** that will run the external stream interface process.
11. Enter probe **Login** and **Password**.
12. Enter the type of **Service**.
    Capture is the default service type.
13. Enter the **Transmission timeout** value (in ms units).
    Default value is 4000.
14. Enter the **Connection timeout** value (in ms units).
    Default value is 4000
15. Enter the **Max number of connection attempts**.
    Default is 50000.
    Note: If neither probe nor simulator is ready when trying to connect to the interface, an attempt is performed about each second (the real delay depends of Astellia API timeout). When the max

number is reached (50,000) an alarm is raised and no more connection attempt will be performed until the process is restarted. To have the system attempt to connect until it is successful, set Max number of connection attempts to "0" (unlimited attempts at connection).

16. Enter the **Interface buffer size** value (in octets).
    Default is 49512.
17. Enter the **Socket buffer size** value (in octets).
    Default is 262144.

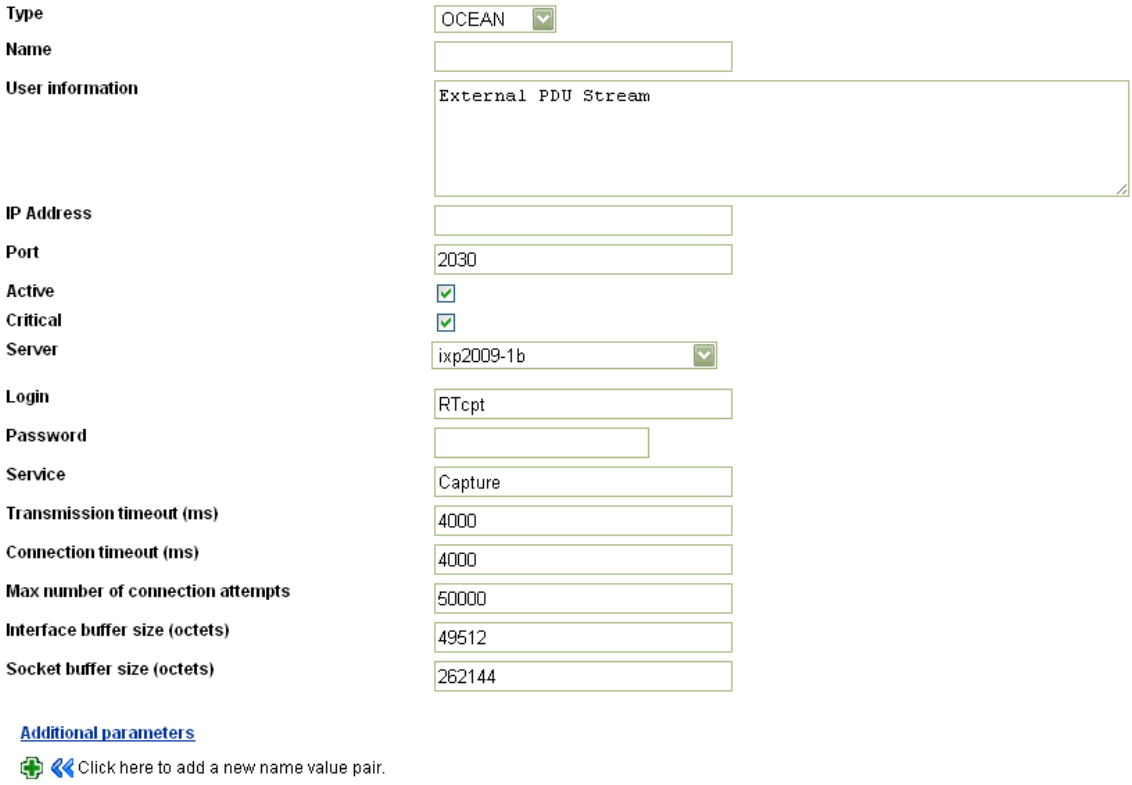


Figure 172: External PDU Stream for OCEAN

Configuring an External PDU Stream for Cisco PMP

Listed are the steps to configure external PDU stream for CISCO PMP:

1. Select **Mediation > Site > IXP > Subsystem > External PDU Streams**.
   The *External PDU Stream List* screen opens.
2. Click **Add** or select external PDU stream and click **Modify** on the tool bar.
   The external PDU stream edition screen opens.
3. Select the **PMP** for **Type** (Available only at creation. Disable during modification).
   Note: PMP option is subjected to license agreement.
4. Enter **Name** to identify the name of the stream in the subsystem (Available only at creation. Disable during modification).
5. Enter any **User information**.
6. Enter **IP Address** of the Cisco switch.
7. Select the **Server** that will run the external stream interface process.
8. Enter connexion **Port** (listening UDP port).
9. Select whether the stream is A**ctive** or not.
10. Select if the stream is a **Critical** one or not.
11. Click **Create** or **Modify**.
12. **Synchronize** the IXP Subsystem to consolidate changes into the system.

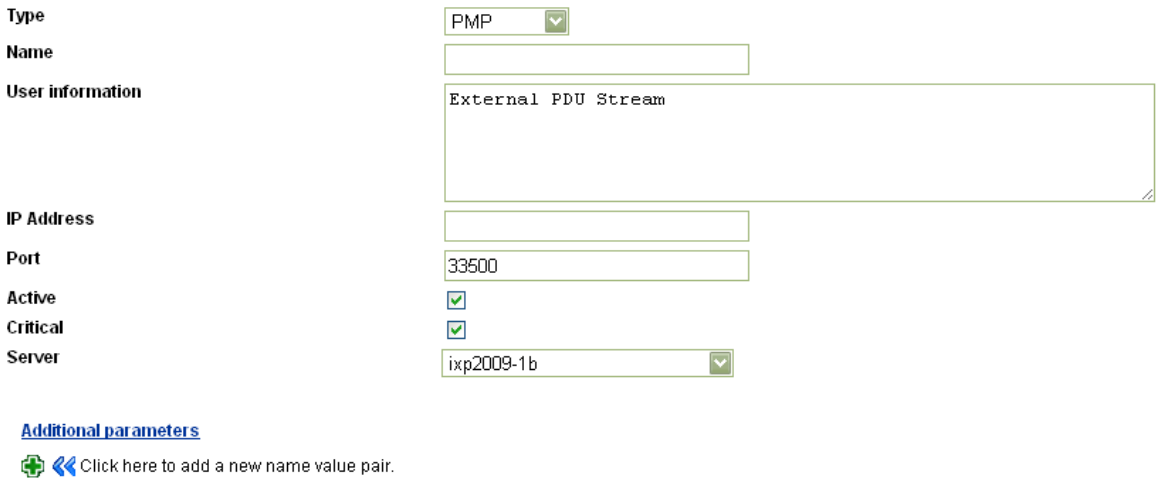


Figure 173: External PDU Stream for PMP

Configuring Additional Parameters for an External PDU Stream

Additional parameters allows to add extra name-value pairs to external PDU stream configuration. Complete these steps to configure the additional parameters of an external PDU Stream:

1. Select **Mediation > Site > IXP> Subsystem > External PDU Streams**.
   The External *PDU Stream List* screen opens.
2. Click **Add** or select external PDU stream and click **Modify** on the tool bar.
   The external PDU stream edition screen opens.
3. Section **Additional Parameters** is at the bottom.

Figure 174: Additional Parameters Screen

4. Click the plus button to add new entry
5. Enter **Name** in the first field (for example SganNb)
6. Enter **Numerical Value** in the second field
7. Repeat steps 4-6 to add additional value pairs.
8. Click **Create** or **Modify**
9. **Synchronize** the IXP Subsystem to consolidate changes into the system.

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. For the Storage Type DFP, user can create one of three types of Store DFPs
   a. Datawarehouse (Storage in Session)
   b. DataBroker (Storage in Files on NFS mounted directories for DataBroker (Syniverse) builders

c. CSV (Storage in CSV Files with Formatting capabilities)

4.

About Dataflow Processings

Dataflow Processing is the receiving end from a PDU Stream or PDU Dataflow as configured on the IMF/PMF. The Dataflow Processing configuration is used to build an 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 IMF/PMF over the input stream that was created for the IMF/PDU 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 precess has an additional turning parameter called a flush timeout. The flush timeout is the fequency 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.

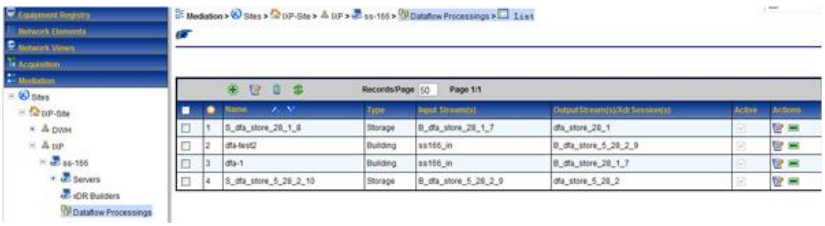


Figure 175: Dataflow Processings List

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.

TABLE 95: DATAFLOW PROCESSINGS LIST TABLE

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.

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>

TABLE 96: DATAFLOW PROCESSING NAMING CONVENTIONS

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.

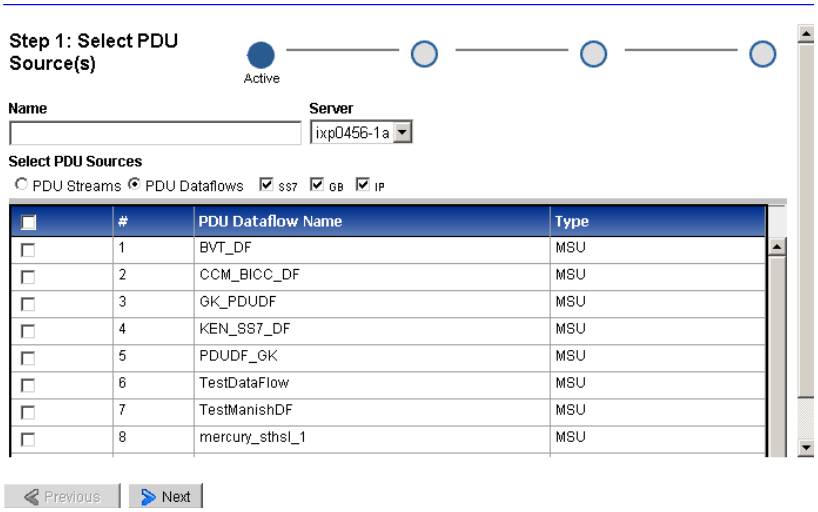


Figure 176: xDR Dataflow Assistant Inital Screen-PDU Sources

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 recommenced 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 it is a Stream or Dataflow and what category (SS7, Gb, IP)
8. Click **Next** to choose an xDR Builder shown below.

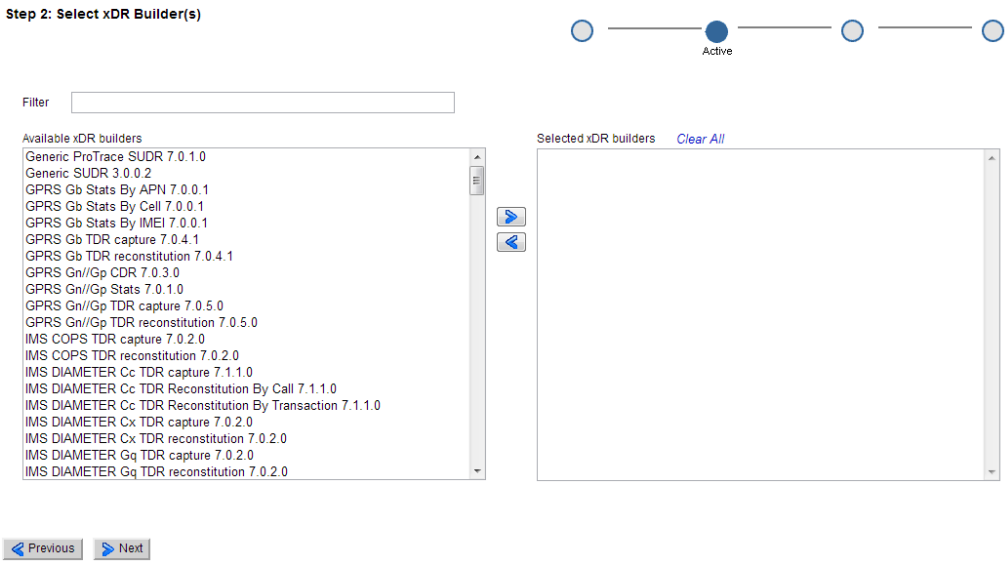


Figure 177: Dataflow Assistant Xdr Builder Selection

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.

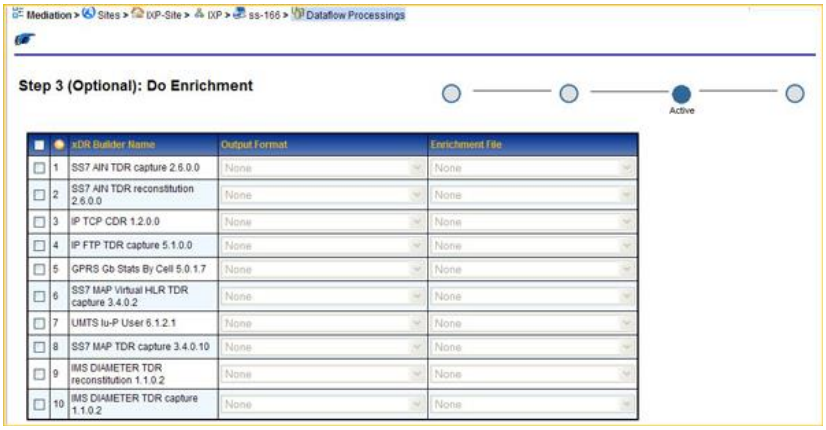


Figure 178: Xdr Assistant - Enrichment Selection

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.

    Note: IF session point code feature is enabled then to configure flavor of session refer ***Appendix D: Defining and Modifying Flavor (PC Format) of Session at CCM***

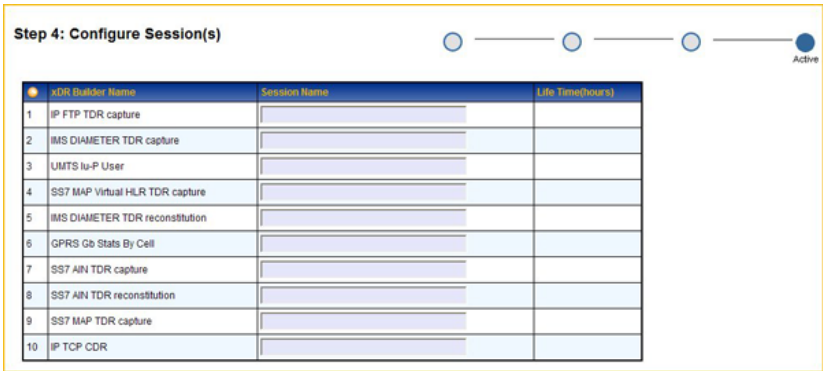


Figure 179: xDR Assistant - Configuring Sessions Screen

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 Neptune Assistant

The Neptune Assistant option provides a wizard to help you quickly create all required IXP configuration elements to connect a Neptune probe:

- External PDU streams
- Build and store dataflow processings
- Sessions

About Naming Conventions

The name of all created element from Neptune Assistant will include the Neptune probe name and will use same convention as ***xDR Dataflow Assistant***.

Acces to Neptune Assistant

1. Select **Mediation > Site > IXP > Subsystem**.
2. Right-click on the **Subsystem**.
   The *pop-up* menu opens.

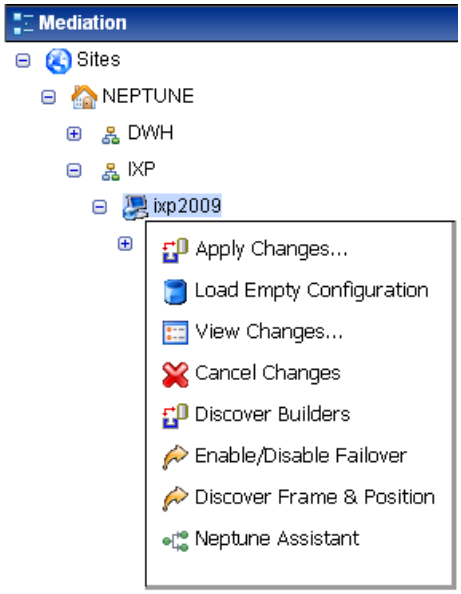


Figure 180: Neptune Assistant access

3. Click on **Neptune Assistant**.
   The Neptune probe list associated with the selected IXP subsystem opens.

Creating configuration using Neptune Assistant

1. Click **Add** on Neptune Assistant list tool bar.
   The Neptune assistant screen opens.

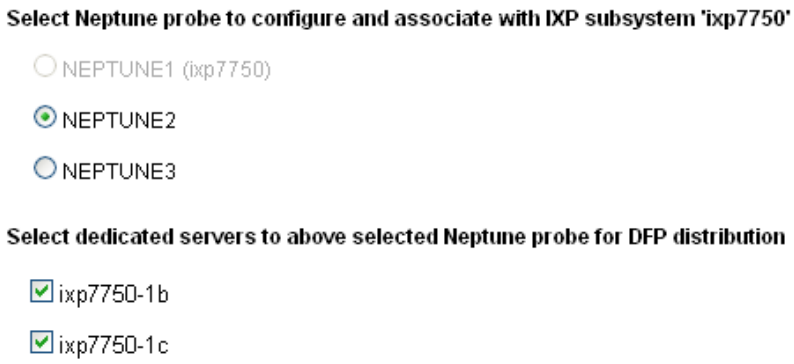


Figure 181: Neptune Assistant screen

2. Select Neptune probe to configure and associate with selected IXP subsystem
3. Select dedicated servers to selected Neptune probe for DFP distribution
4. Click **Create**
   All required IXP configuration elements to connect Neptune probe will be created.

IXP configuration elements creating by Neptune Assistant

Neptune assistant will create configuration for CP and UP captures and also for traffic counters and TCPDR.

One external PDU stream will be created for each output on Neptune:

- 1 CP capture
- 1 traffic counters
- 1 TCPDR
- N_1 UP APN
- N_2 UP IMSI

Each external PDU stream will be created with type "NEPTUNE" and use probe capture IP, login and password.

The number of UP streams will be determine according to the number of selected IXP servers in Neptune Assistant. By default, the number of UP streams will be:

Nb selected IXP servers	1	2	3	4	5	6	7	8	9	…
Nb UP APN streams	1	1	2	3	5	6	8	9	10	10
Nb UP IMSI streams	1	1	2	4	5	7	8	10	10	10

TABLE 97: NEPTUNE ASSISTANT UP STREAMS ALLOCATION

The port and name will be assigned according to above Neptune capture configuration (see §3.2.1):

Outputs	***Port:ID***	***Name***
CP capture	56001:0	<Probe name>_CP
UP APN captures	56000:0 to 56000:9	<Probe name>_APN_<0-9>
UP IMSI captures	56000:10 to 56000:19	<Probe name>_IMSI_<10-19>
Traffic counter	56001:10	<Probe name>_UP_STAT
TCPDR	56001:11	<Probe name>_IPS<1-4>

TABLE 98: NEPTUNE ASSISTANT EXTERNAL PDU STREAMS

Each ouput will be connected to one build DFP (except IPS capture which is loadbalanced to 4 build DFPs by default).

Following final builders will be activated for build DFPs with output stream name set according to probe, input stream and final builder:

Build DFP name	***Final builders***	***Output stream name***
B_<Probe name>_APN_<0-9>	GPRS Gn//Gp TDR reconstitution	O_<Probe name>_APN_<0-9>_GTP_TDR
	IP DNS TDR	O_<Probe name>_APN_<0-9>_IP_DNS_TDR
	IP FTP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_FTP_TDR
	IP HTTP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_HTTP_TDR
	IP IMAP4 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_IMAP4_TDR
	IP MMS TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_MMS_TDR
	IP MMS on WAPv2 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_MMS_WAPv2_TDR
	IP POP3 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_POP3_TDR
	IP RTSP TDR	O_<Probe name>_APN_<0-9>_IP_RTSP_TDR
	IP SMTP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_SMTP_TDR
	IP WAP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_WAP_TDR
	IP WAP2 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_WAP2_TDR
B_<Probe name>_IMSI_<10-29>	GPRS Gn//Gp TDR reconstitution	O_<Probe name>_IMSI_<10-19>_GTP_TDR
	IP DNS TDR	O_<Probe name>_IMSI_<10-19>_IP_DNS_TDR
	IP FTP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_FTP_TDR
	IP HTTP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_HTTP_TDR
	IP IMAP4 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_IMAP4_TDR
	IP MMS TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_MMS_TDR
	IP MMS on WAPv2 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_MMS_WAPv2_TDR
	IP POP3 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_POP3_TDR
	IP RTSP TDR	O_<Probe name>_IMSI_<10-19>_IP_RTSP_TDR
	IP SMTP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_SMTP_TDR
	IP WAP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_WAP_TDR
	IP WAP2 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_WAP2_TDR
B_<Probe name>_UP_STAT	UP Transport TDR reconstitution	O_<Probe name>_TRANPORT_STAT
	UP Usage TDR reconstitution	O_<Probe name>_USAGE_STAT
B_<Probe name>_CP	GPRS Gn//Gp TDR reconstitution	O_<Probe name>_CP_GTP_TDR
B_<Probe name>_IPS<1-4>	IP Sessions Summary TDR	O_<Probe name>_IPS<1-4>

For each probe, following sessions will be created:

<Probe name>_APN_GTP_TDR
<Probe name>_APN_IP_DNS_TDR
<Probe name>_APN_IP_FTP_TDR
<Probe name>_APN_IP_HTTP_TDR
<Probe name>_APN_IP_IMAP4_TDR
<Probe name>_APN_IP_MMS_TDR
<Probe name>_APN_IP_MMS_WAPv2_TDR
<Probe name>_APN_IP_POP3_TDR
<Probe name>_APN_IP_RTSP_TDR
<Probe name>_APN_IP_SMTP_TDR
<Probe name>_APN_IP_WAP_TDR
<Probe name>_APN_IP_WAP2_TDR
<Probe name>_IMSI_GTP_TDR
<Probe name>_IMSI_IP_DNS_TDR
<Probe name>_IMSI_IP_FTP_TDR
<Probe name>_IMSI_IP_HTTP_TDR
<Probe name>_IMSI_IP_IMAP4_TDR
<Probe name>_IMSI_IP_MMS_TDR
<Probe name>_IMSI_IP_MMS_WAPv2_TDR
<Probe name>_IMSI_IP_POP3_TDR
<Probe name>_IMSI_IP_RTSP_TDR
<Probe name>_IMSI_IP_SMTP_TDR
<Probe name>_IMSI_IP_WAP_TDR
<Probe name>_IMSI_IP_WAP2_TDR
<Probe name>_TRANPORT_STAT
<Probe name>_USAGE_STAT

<Probe name>_CP_GTP_TDR
<Probe name>_IPS<1-4>

One store DFP will be created for each session with as input stream the subset of output streams corresponding to associated final builder:

Input streams	***Session output***	***Store DFP name***
O_<Probe name>_APN_<0-9>_GTP_TDR	<Probe name>_APN_GTP_TDR	S_<Probe name>_APN_GTP_TDR
O_<Probe name>_APN_<0-9>_IP_DNS_TDR	<Probe name>_APN_IP_DNS_TDR	S_<Probe name>_APN_IP_DNS_TDR
O_<Probe name>_APN_<0-9>_IP_FTP_TDR	<Probe name>_APN_IP_FTP_TDR	S_<Probe name>_APN_IP_FTP_TDR
O_<Probe name>_APN_<0-9>_IP_HTTP_TDR	<Probe name>_APN_IP_HTTP_TDR	S_<Probe name>_APN_IP_HTTP_TDR
O_<Probe name>_APN_<0-9>_IP_IMAP4_TDR	<Probe name>_APN_IP_IMAP4_TDR	S_<Probe name>_APN_IP_IMAP4_TDR
O_<Probe name>_APN_<0-9>_IP_MMS_TDR	<Probe name>_APN_IP_MMS_TDR	S_<Probe name>_APN_IP_MMS_TDR
O_<Probe name>_APN_<0-9>_IP_MMS_WAPv2_TDR	<Probe name>_APN_IP_MMS_WAPv2_TDR	S_<Probe name>_APN_IP_MMS_WAPv2_TDR
O_<Probe name>_APN_<0-9>_IP_POP3_TDR	<Probe name>_APN_IP_POP3_TDR	S_<Probe name>_APN_IP_POP3_TDR
O_<Probe name>_APN_<0-9>_IP_RTSP_TDR	<Probe name>_APN_IP_RTSP_TDR	S_<Probe name>_APN_IP_RTSP_TDR
O_<Probe name>_APN_<0-9>_IP_SMTP_TDR	<Probe name>_APN_IP_SMTP_TDR	S_<Probe name>_APN_IP_SMTP_TDR
O_<Probe name>_APN_<0-9>_IP_WAP_TDR	<Probe name>_APN_IP_WAP_TDR	S_<Probe name>_APN_IP_WAP_TDR
O_<Probe name>_APN_<0-9>_IP_WAP2_TDR	<Probe name>_APN_IP_WAP2_TDR	S_<Probe name>_APN_IP_WAP2_TDR
O_<Probe name>_IMSI_<10-19>_GTP_TDR	<Probe name>_IMSI_GTP_TDR	S_<Probe name>_IMSI_GTP_TDR
O_<Probe name>_IMSI_<10-19>_IP_DNS_TDR	<Probe name>_IMSI_IP_DNS_TDR	S_<Probe name>_IMSI_IP_DNS_TDR
O_<Probe name>_IMSI_<10-19>_IP_FTP_TDR	<Probe name>_IMSI_IP_FTP_TDR	S_<Probe name>_IMSI_IP_FTP_TDR
O_<Probe name>_IMSI_<10-19>_IP_HTTP_TDR	<Probe name>_IMSI_IP_HTTP_TDR	S_<Probe name>_IMSI_IP_HTTP_TDR
O_<Probe name>_IMSI_<10-19>_IP_IMAP4_TDR	<Probe name>_IMSI_IP_IMAP4_TDR	S_<Probe name>_IMSI_IP_IMAP4_TDR
O_<Probe name>_IMSI_<10-19>_IP_MMS_TDR	<Probe name>_IMSI_IP_MMS_TDR	S_<Probe name>_IMSI_IP_MMS_TDR
O_<Probe name>_IMSI_<10-19>_IP_MMS_WAPv2_TDR	<Probe name>_IMSI_IP_MMS_WAPv2_TDR	S_<Probe name>_IMSI_IP_MMS_WAPv2_TDR
O_<Probe name>_IMSI_<10-19>_IP_POP3_TDR	<Probe name>_IMSI_IP_POP3_TDR	S_<Probe name>_IMSI_IP_POP3_TDR
O_<Probe name>_IMSI_<10-19>_IP_RTSP_TDR	<Probe name>_IMSI_IP_RTSP_TDR	S_<Probe name>_IMSI_IP_RTSP_TDR
O_<Probe name>_IMSI_<10-19>_IP_SMTP_TDR	<Probe name>_IMSI_IP_SMTP_TDR	S_<Probe name>_IMSI_IP_SMTP_TDR
O_<Probe name>_IMSI_<10-19>_IP_WAP_TDR	<Probe name>_IMSI_IP_WAP_TDR	S_<Probe name>_IMSI_IP_WAP_TDR
O_<Probe name>_IMSI_<10-19>_IP_WAP2_TDR	<Probe name>_IMSI_IP_WAP2_TDR	S_<Probe name>_IMSI_IP_WAP2_TDR
O_<Probe name>_TRANPORT_STAT	<Probe name>_TRANPORT_STAT	S_<Probe name>_TRANPORT_STAT
O_<Probe name>_USAGE_STAT	<Probe name>_USAGE_STAT	S_<Probe name>_USAGE_STAT
O_<Probe name>_CP_GTP_TDR	<Probe name>_CP_GTP_TDR	S_<Probe name>_CP_GTP_TDR
O_<Probe name>_IPS<1-4>	<Probe name>_ IPS<1-4>	S_<Probe name>_ IPS<1-4>

The distribution will be done evenly on all selected IXP servers.
External PDU streams and corresponding build DFPs will be distributed identically.

Here is the distribution preview of build DFPs and corresponding external DPU streams on IXP servers:

Nb servers	*Server 1*	*Server 2*	*Server 3*	*Server 4*	*Server 5*	*Server 6*	*Server 7*	*Server 8*	*Server 9*
1	4 IPS 1 CP 1 UP_STAT 1 APN 1 IMSI								
2	4 IPS	1 CP 1 UP_STAT 1 APN 1 IMSI							
3	4 IPS	1 CP 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI						
4	4 IPS	1 MA 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI	1 APN 2 IMSI					
5	4 IPS	1 MA 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI	2 APN 1 IMSI	1 APN 2 IMSI				
6	4 IPS	1 MA 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI	2 APN 1 IMSI	1 APN 2 IMSI	1 APN 2 IMSI			

7	4 IPS	1 MA 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI	2 APN 1 IMSI	2 APN 1 IMSI	1 APN 2 IMSI	1 APN 2 IMSI		
8	4 IPS	1 MA 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI	2 APN 1 IMSI	2 APN 1 IMSI	1 APN 2 IMSI	1 APN 2 IMSI	1 APN 2 IMSI	
9	4 IPS	1 MA 1 APN 1 IMSI	1 UP_STAT 1 APN 1 IMSI	2 APN 1 IMSI	2 APN 1 IMSI	2 APN 1 IMSI	1 APN 2 IMSI	1 APN 2 IMSI	1 APN 2 IMSI

Store DFPs are evenly distributed on all servers.

Overview of all IXP elements created:

Input stream	***Build DFP***	***xDR builder***	***Output stream***	***Store DFP***	***Session***
<Probe name>_APN_<0-9>	B_<Probe name>_APN_<0-9>	GPRS Gn//Gp TDR reconstitution	O_<Probe name>_APN_<0-9>_GTP_TDR	S_<Probe name>_APN_GTP_TDR	<Probe name>_APN_GTP_TDR
		IP DNS TDR	O_<Probe name>_APN_<0-9>_IP_DNS_TDR	S_<Probe name>_APN_IP_DNS_TDR	<Probe name>_APN_IP_DNS_TDR
		IP FTP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_FTP_TDR	S_<Probe name>_APN_IP_FTP_TDR	<Probe name>_APN_IP_FTP_TDR
		IP HTTP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_HTTP_TDR	S_<Probe name>_APN_IP_HTTP_TDR	<Probe name>_APN_IP_HTTP_TDR
		IP IMAP4 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_IMAP4_TDR	S_<Probe name>_APN_IP_IMAP4_TDR	<Probe name>_APN_IP_IMAP4_TDR
		IP MMS TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_MMS_TDR	S_<Probe name>_APN_IP_MMS_TDR	<Probe name>_APN_IP_MMS_TDR
		IP MMS on WAPv2 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_MMS_WAPv2_TDR	S_<Probe name>_APN_IP_MMS_WAPv2_TDR	<Probe name>_APN_IP_MMS_WAPv2_TDR
		IP POP3 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_POP3_TDR	S_<Probe name>_APN_IP_POP3_TDR	<Probe name>_APN_IP_POP3_TDR
		IP RTSP TDR	O_<Probe name>_APN_<0-9>_IP_RTSP_TDR	S_<Probe name>_APN_IP_RTSP_TDR	<Probe name>_APN_IP_RTSP_TDR
		IP SMTP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_SMTP_TDR	S_<Probe name>_APN_IP_SMTP_TDR	<Probe name>_APN_IP_SMTP_TDR
		IP WAP TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_WAP_TDR	S_<Probe name>_APN_IP_WAP_TDR	<Probe name>_APN_IP_WAP_TDR
		IP WAP2 TDR reconstitution	O_<Probe name>_APN_<0-9>_IP_WAP2_TDR	S_<Probe name>_APN_IP_WAP2_TDR	<Probe name>_APN_IP_WAP2_TDR
<Probe name>_IMSI_<10-19>	B_<Probe name>_IMSI_<10-19>	GPRS Gn//Gp TDR reconstitution	O_<Probe name>_IMSI_<10-19>_GTP_TDR	S_<Probe name>_IMSI_GTP_TDR	<Probe name>_IMSI_GTP_TDR
		IP DNS TDR	O_<Probe name>_IMSI_<10-19>_IP_DNS_TDR	S_<Probe name>_IMSI_IP_DNS_TDR	<Probe name>_IMSI_IP_DNS_TDR
		IP FTP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_FTP_TDR	S_<Probe name>_IMSI_IP_FTP_TDR	<Probe name>_IMSI_IP_FTP_TDR
		IP HTTP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_HTTP_TDR	S_<Probe name>_IMSI_IP_HTTP_TDR	<Probe name>_IMSI_IP_HTTP_TDR
		IP IMAP4 TDR reconstitution	O_<Probe name>_IMSI_<1019>_IP_IMAP4_TDR	S_<Probe name>_IMSI_IP_IMAP4_TDR	<Probe name>_IMSI_IP_IMAP4_TDR
		IP MMS TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_MMS_TDR	S_<Probe name>_IMSI_IP_MMS_TDR	<Probe name>_IMSI_IP_MMS_TDR
		IP MMS on WAPv2 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_MMS_WAPv2_TDR	S_<Probe name>_IMSI_IP_MMS_WAPv2_TDR	<Probe name>_IMSI_IP_MMS_WAPv2_TDR
		IP POP3 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_POP3_TDR	S_<Probe name>_IMSI_IP_POP3_TDR	<Probe name>_IMSI_IP_POP3_TDR
		IP RTSP TDR	O_<Probe name>_IMSI_<10-19>_IP_RTSP_TDR	S_<Probe name>_IMSI_IP_RTSP_TDR	<Probe name>_IMSI_IP_RTSP_TDR

		IP SMTP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_SMTP_TDR	S_<Probe name>_IMSI_IP_SMTP_TDR	<Probe name>_IMSI_IP_SMTP_TDR
		IP WAP TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_WAP_TDR	S_<Probe name>_IMSI_IP_WAP_TDR	<Probe name>_IMSI_IP_WAP_TDR
		IP WAP2 TDR reconstitution	O_<Probe name>_IMSI_<10-19>_IP_WAP2_TDR	S_<Probe name>_IMSI_IP_WAP2_TDR	<Probe name>_IMSI_IP_WAP2_TDR
<Probe name>_UP_STAT	B_<Probe name>_UP_STAT	UP Transport stat	O_<Probe name>_TRANSPORT_STAT	S_<Probe name>_TRANPSORT_STAT	<Probe name>_TRANPORT_STAT
		UP Usage stat	O_<Probe name>_USAGE_STAT	S_<Probe name>_USAGE_STAT	<Probe name>_USAGE_STAT
<Probe name>_CP	B_<Probe name>_CP	GPRS Gn//Gp TDR reconstitution	O_<Probe name>_CP_GTP_TDR	S_<Probe name>_CP_GTP_TDR	<Probe name>_CP_GTP_TDR
<Probe name>_IPS<1-4>	B_<Probe name>_IPS<1-4>	IP Sessions Summary TDR	O_<Probe name>_ IPS<1-4>	S_<Probe name>_ IPS<1-4>	<Probe name>_ IPS<1-4>

Neptune Assistant Advanced parameters

It is possible to change default number of UP captures for APN and IMSI, and the default number of IPS loadbalancing.

Figure 182: Neptune Assistant Advanced parameters

Deleting IXP configuration elements created by Neptune Assistant

1. Select Neptune probe in Neptune Asistant list
2. Click **Delete** in the tool bar.

All IXP configuration elements created by Neptune assistant will be deleted except sessions.

Neptune Assistant list tool bar

Neptune assistant list provides also in the tool bar:

the possibility to directly open Neptune probe administration portal

the possibility to reset Neptune probe configuration

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.

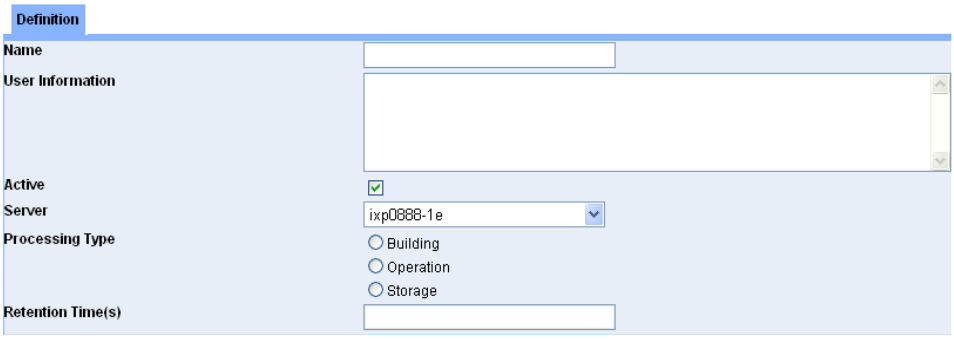


Figure 183: Add Screen

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.)

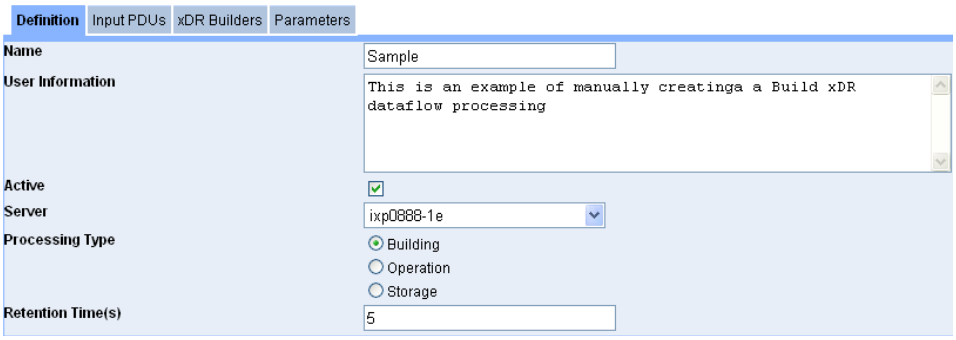


Figure 184: Dataflow Building Screen

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.

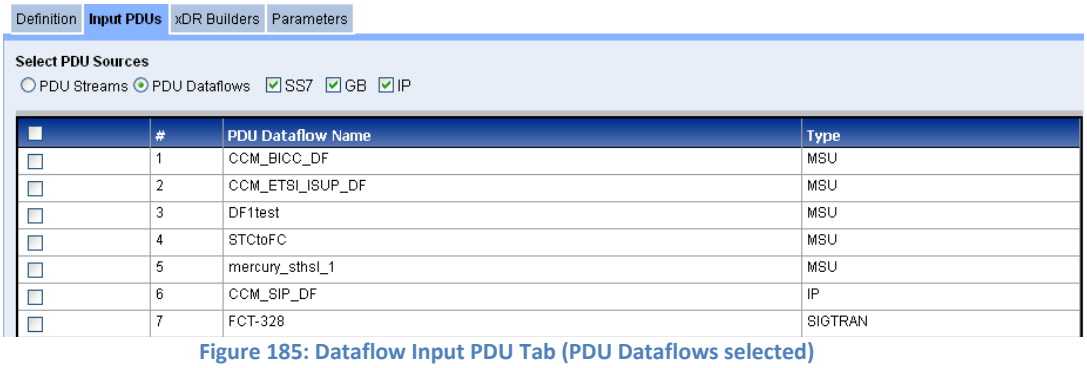


Figure 185: Dataflow Input PDU Tab (PDU Dataflows selected)

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.

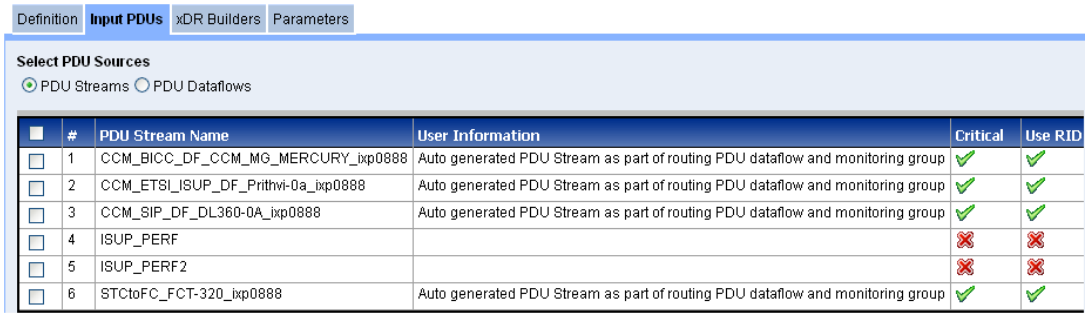


Figure 186: Dataflow Input PDU Tab (PDU Dataflows selected)

14. Select the **PDU Stream Name(s)** to be used.
15. Click **Next** to open the xDR Builders tab.

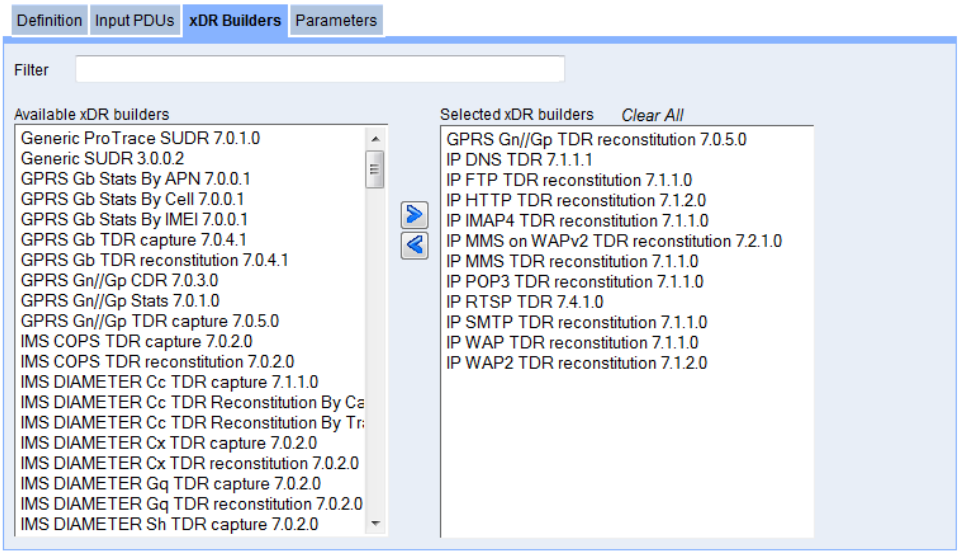


Figure 187: Xdr Builders Tab

16. Select one or more **xDR Builders** from Available list.
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,"

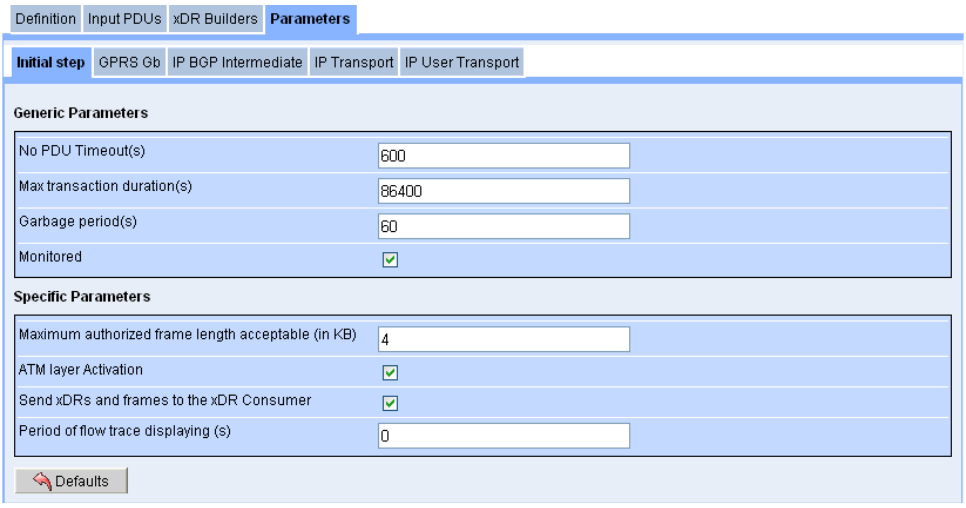


Figure 188: Parameters Tab (with SS7, GPRS, IP and Misc xDR Builders selected)

18. You can **modify** the default values of any parameter.
19. Click **Create**.
    You must now **Apply 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 a dSIP-T/SIP xDRs manually using the build process.

Note: In addition, in configuring partial ANSI ISUP a 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.

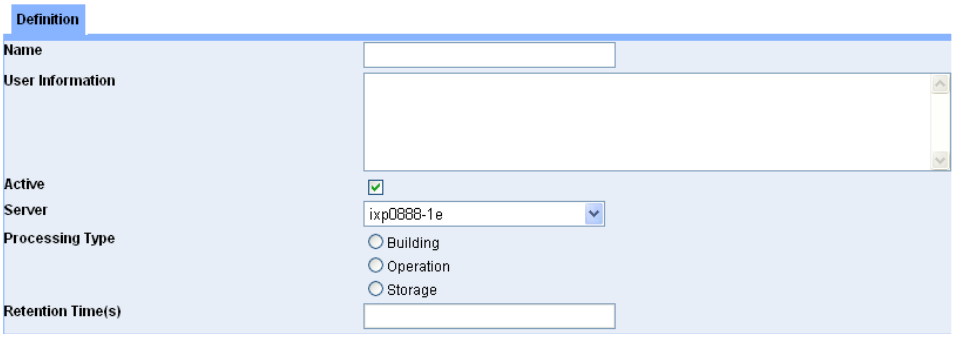


Figure 189: Add Screen

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.)

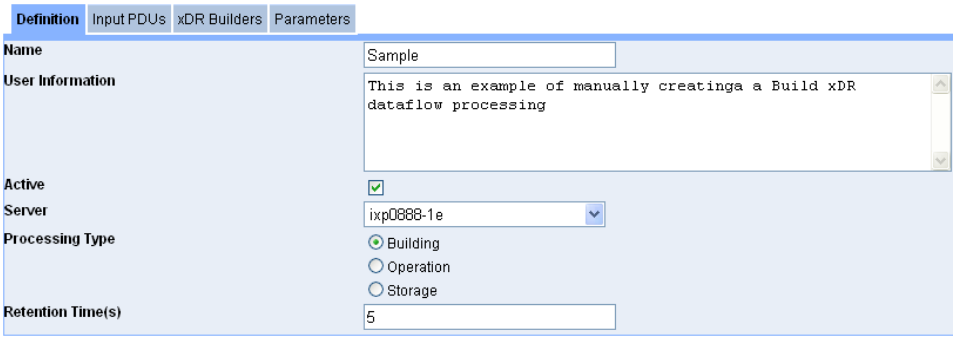


Figure 190: Dataflow Building Screen

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.

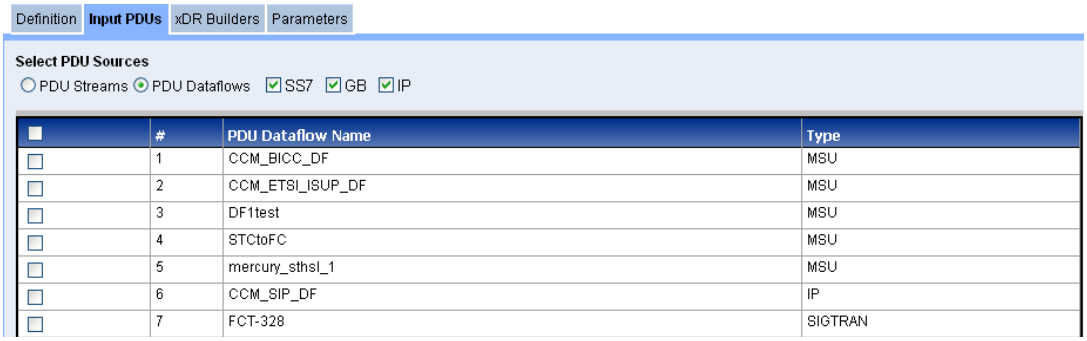


Figure 191: Dataflow Input PDU Tab (PDU Dataflows selected)

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.

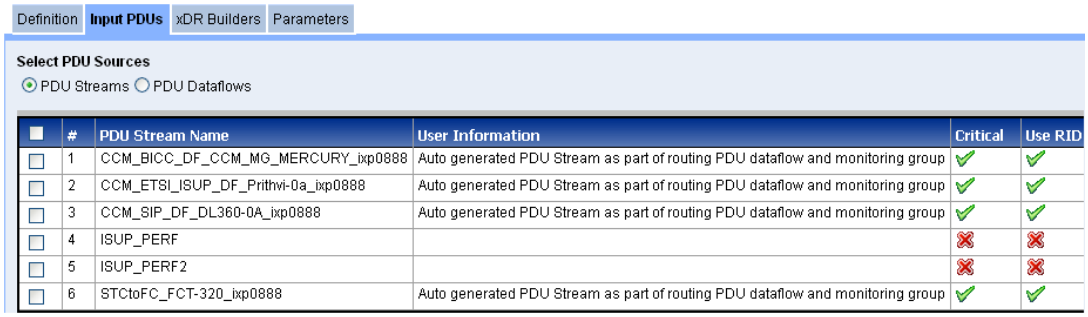


Figure 192: Input PDU Tab (PDU Streams selected if working with external PDU streams)

13. Select the **PDU Stream Name(s)** to be used.
14. Click **Next** to open the xDR Builders tab.

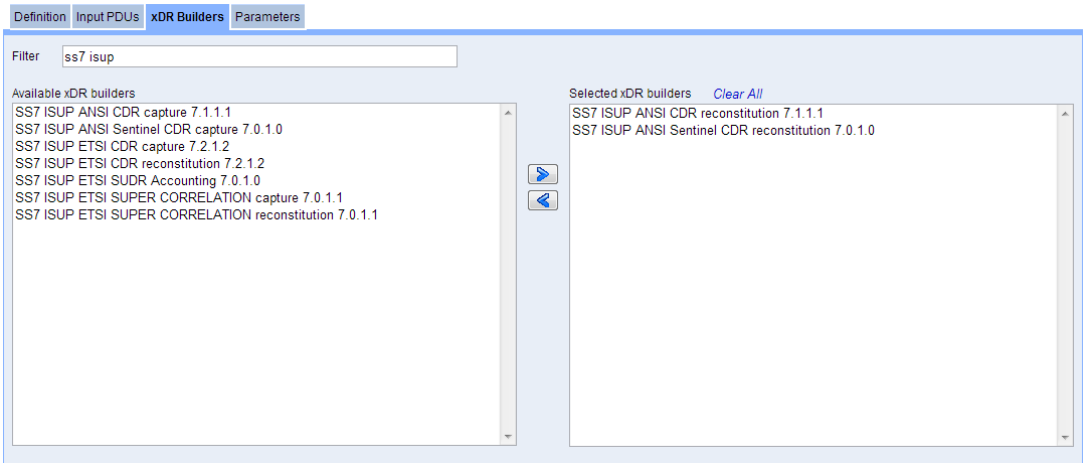


Figure 193: xDR Builders Tab

15. Select one or more **SS7 ISUP ANSI CDR Reconstruction** from Available list.
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,"

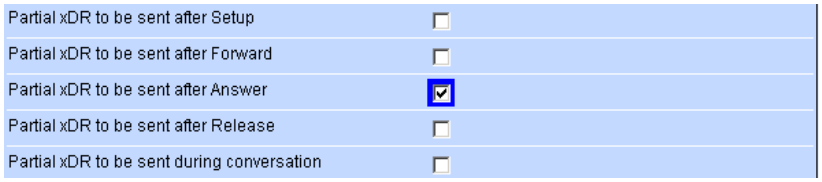


Figure 194: Parameters Tab Showing SS7 ISUP ANSI CDR Tab

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.

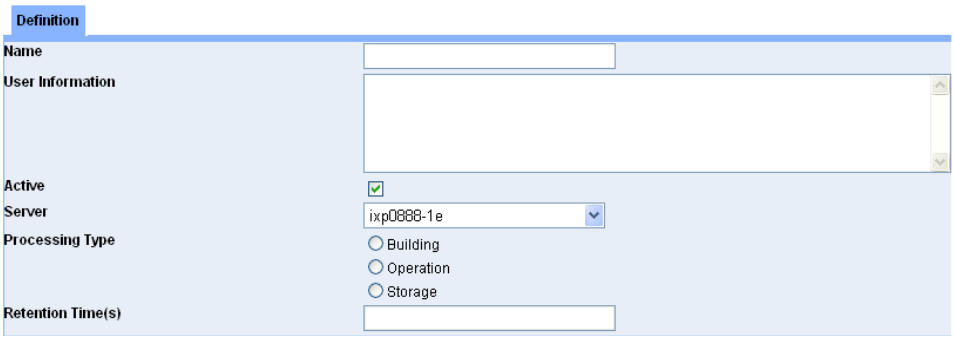


Figure 195: Add Screen

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.)

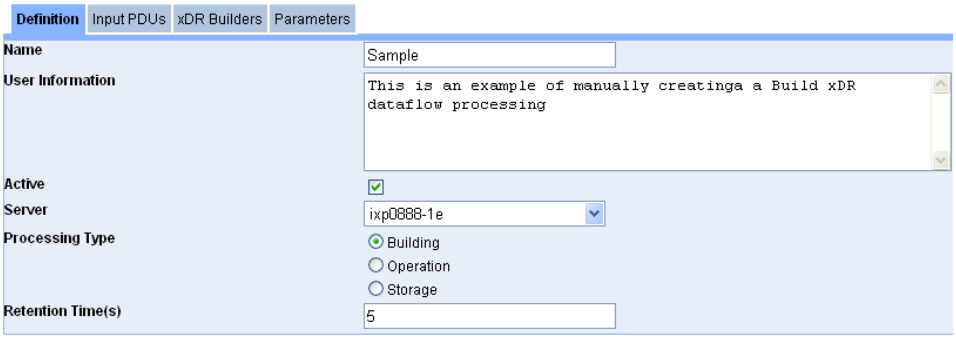
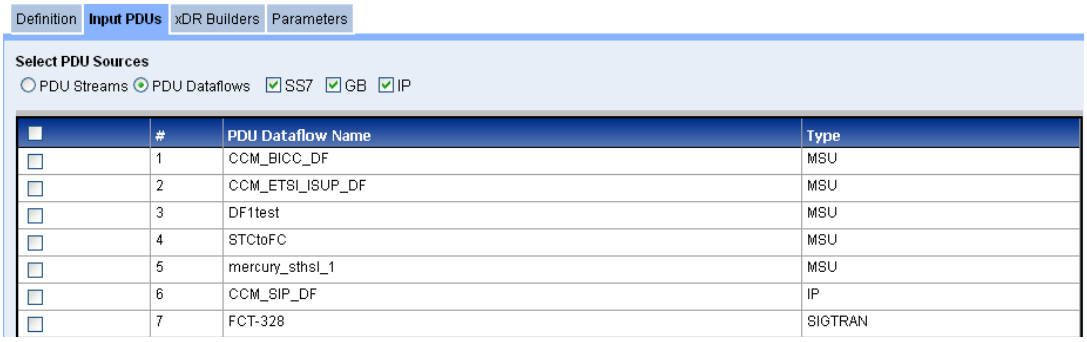


Figure 196: Dataflow Building Screen

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.



#	PDU Dataflow Name	Type
1	CCM_BICC_DF	MSU
2	CCM_ETSI_ISUP_DF	MSU
3	DF1test	MSU
4	STCtoFC	MSU
5	mercury_sthsl_1	MSU
6	CCM_SIP_DF	IP
7	FCT-328	SIGTRAN

Figure 197: 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 198: 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,"

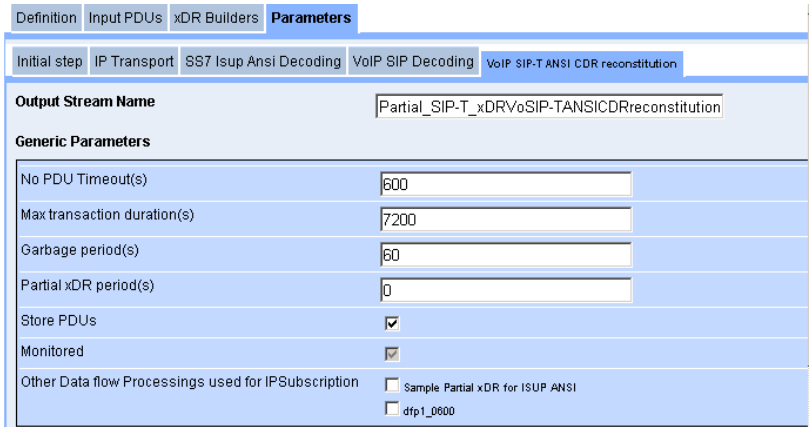


Figure 199: Parameters Tab with VoIP SIP-T ANSI CDR Tab

16. Select **Answer** (move to selected options field) from the CDR Partial section.

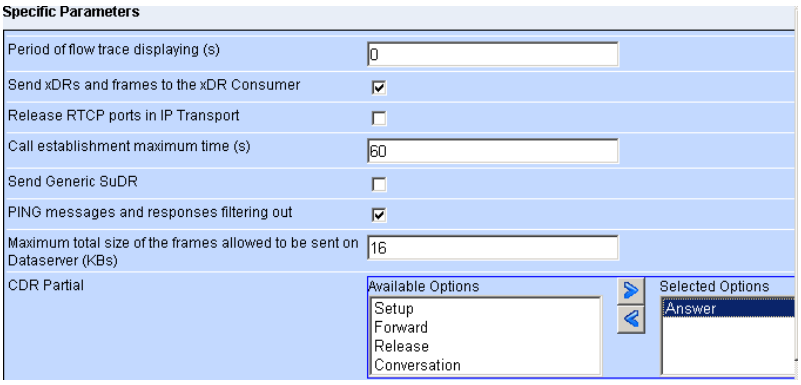


Figure 200: VoIP SIP with Answer selected

17. Click **Create**.
    You must now **Apply 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.

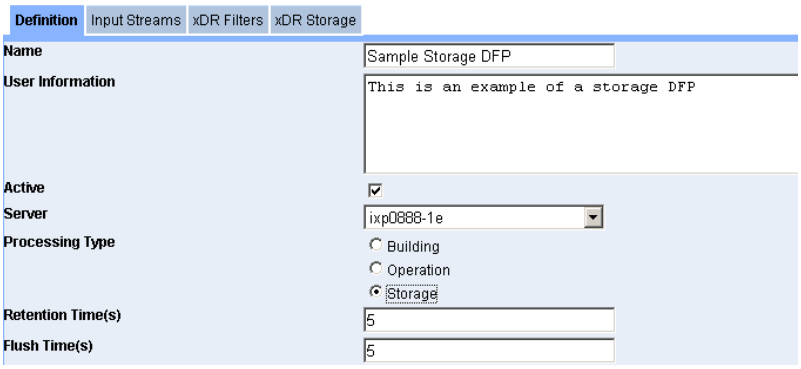


Figure 201: Add Screen

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.

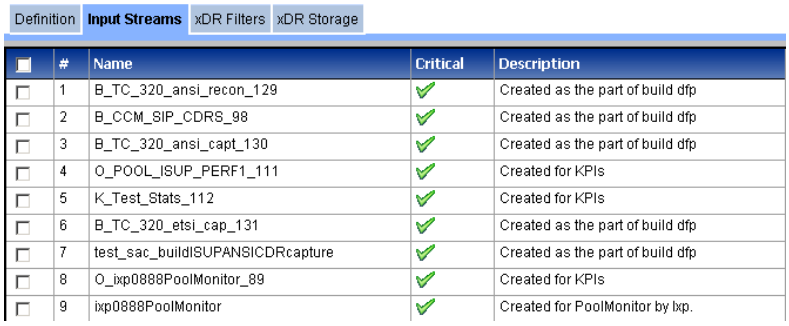


Figure 202: Input Streams Screen

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.

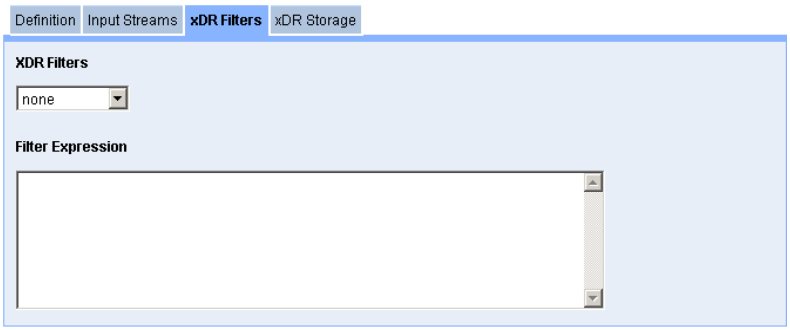


Figure 203: xDR Filter Screen

14. Select **Create Filter** from the drop-down menu.
    The *Create New xDR Filter* opens.

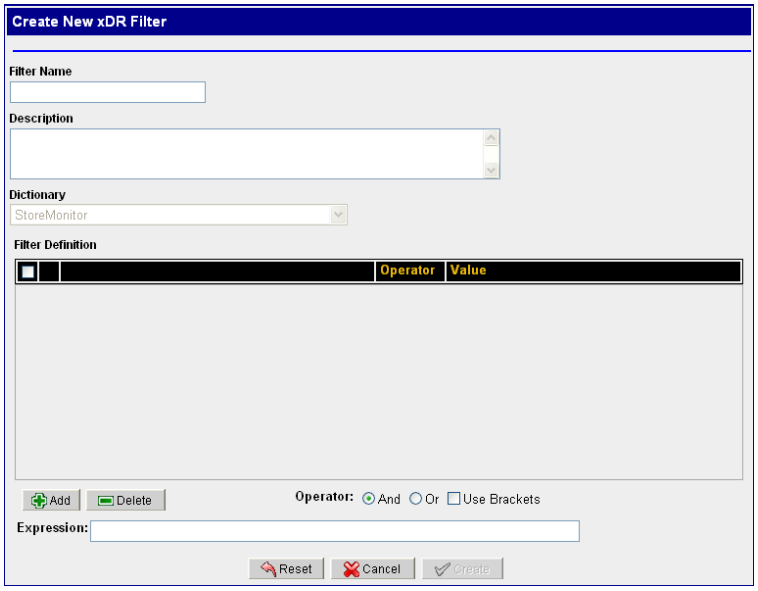


Figure 204: xDR Filter Screen

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.

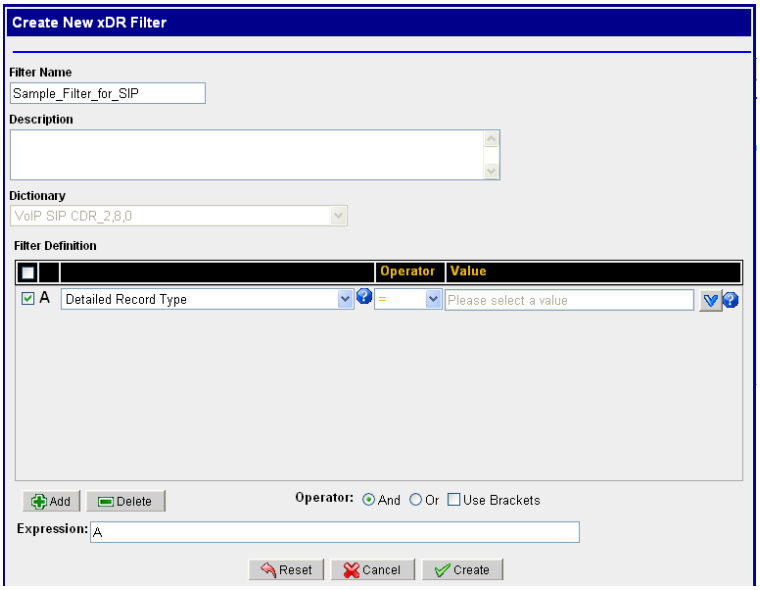


Figure 205: xDR Filter Screen with condition

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.

    Note: To configure flavor of session refer ***Appendix D: Defining and Modifying Flavor (PC Format) of Session at CCM***

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 an 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.

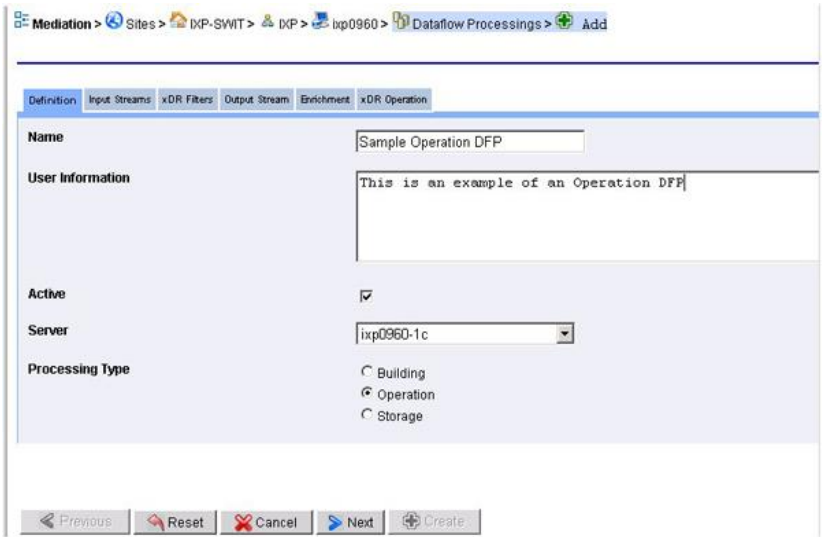


Figure 206: Add Dataflow Processing Screen

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.

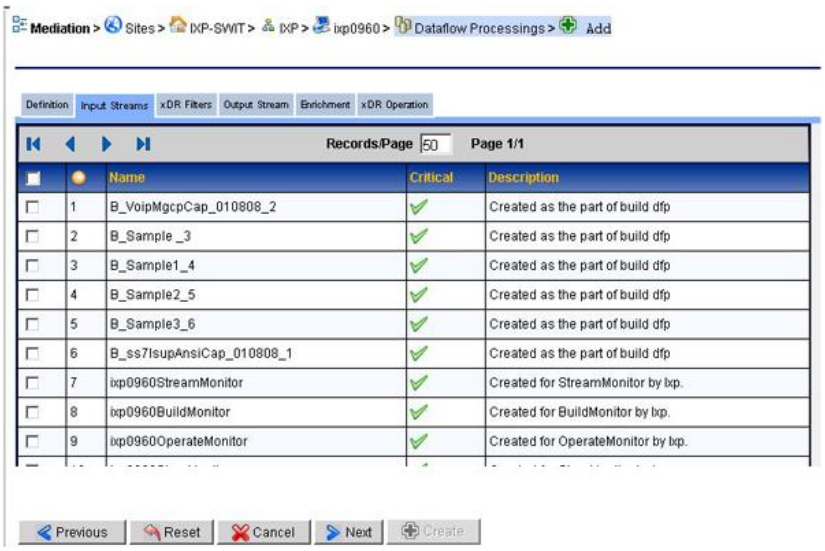


Figure 207: IP Streams Screen

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**.

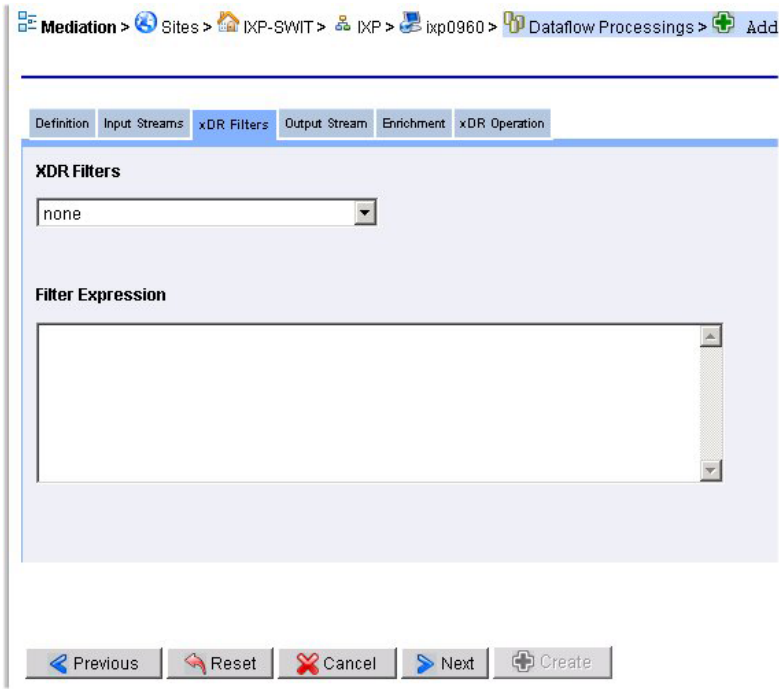


Figure 208: Xdr Filters Screen

12. Select an **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.

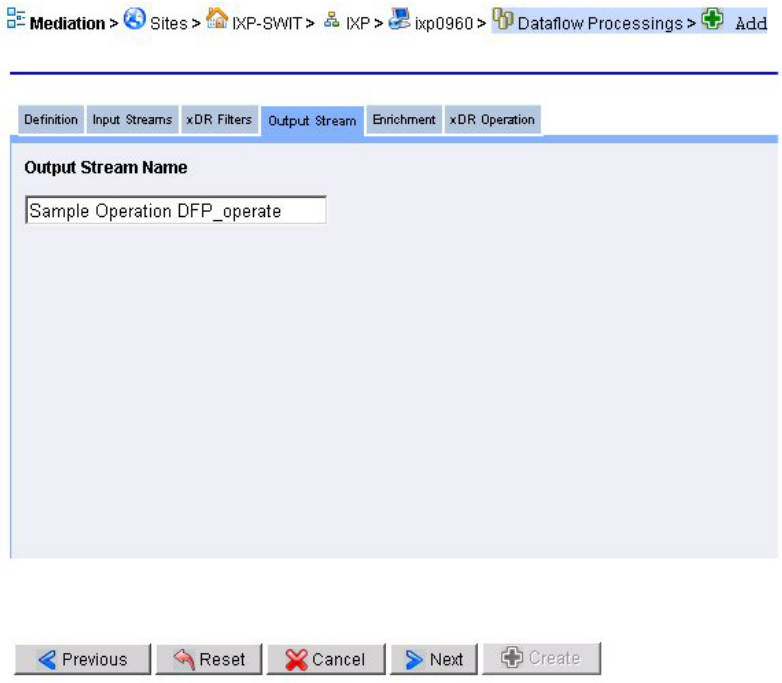


Figure 209: Output Steams Screen

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.

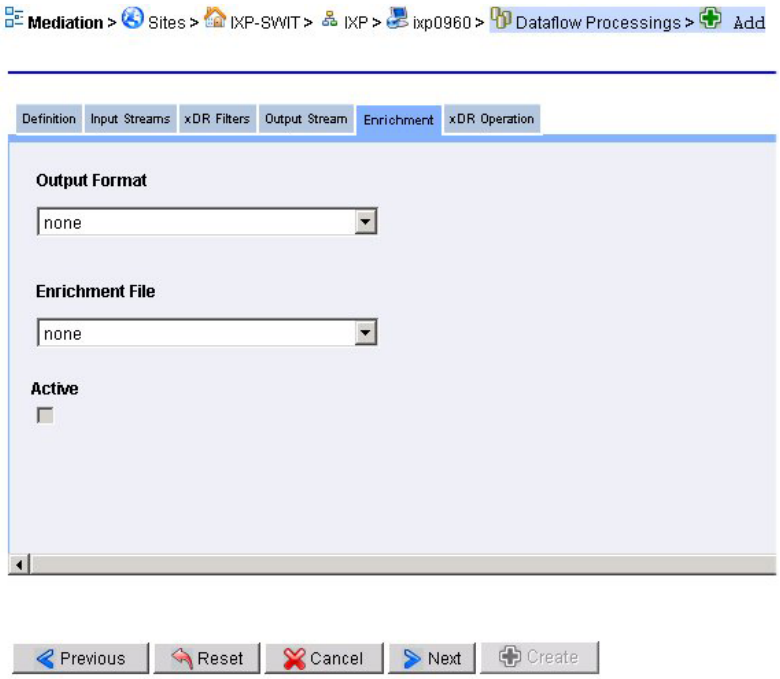


Figure 210: Enrichment Screen

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.

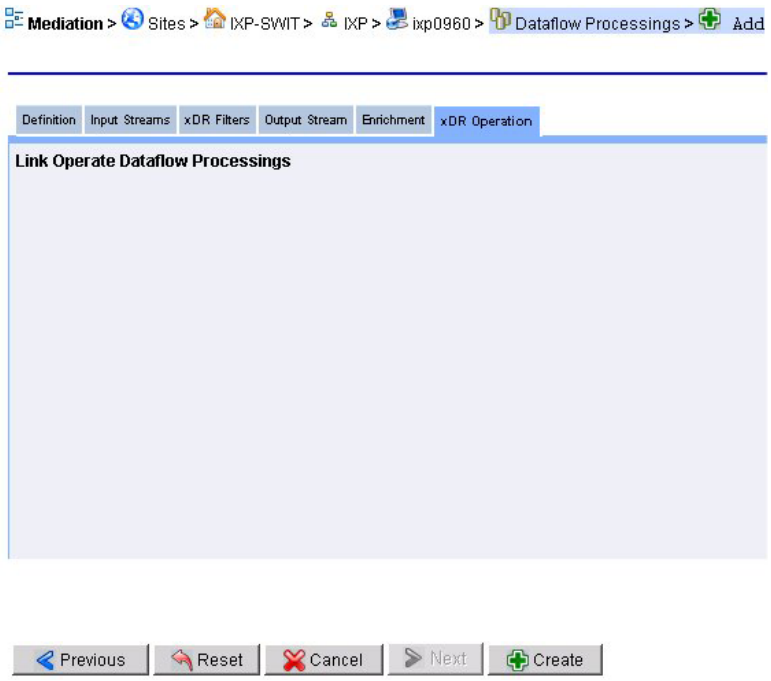


Figure 211: Xdr Operation Screen

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.

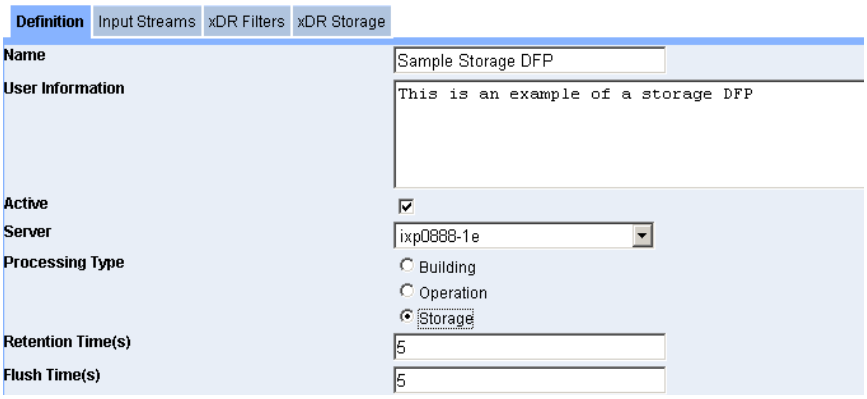


Figure 212: Xdr Operation Screen

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* (Defalt is 5 sec).
11. Click **Next**.
    The list of *Input Steams* appears.

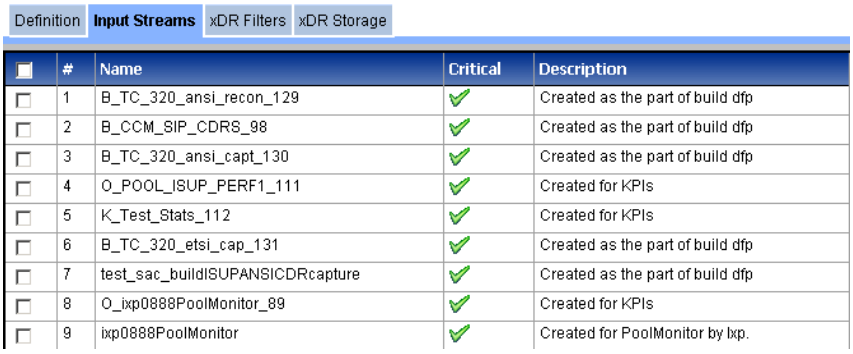


Figure 213: Input Streams Screen

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.

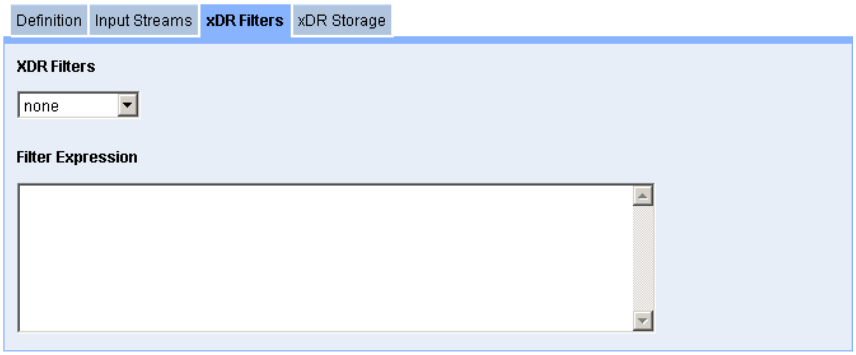


Figure 214: xDR Filter Screen

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.

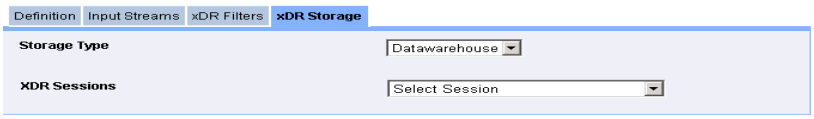


Figure 215: xDR Storage Screen

16. **Select** Storage Type
    Select Storage Type as Datawarehouse in the Storage Type drop down list box.

17. **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.

Note: If Session Point Code Feature is enabled then to configure flavor of session refer ***Appendix D: Defining and Modifying Flavor (PC Format) of Session at CCM***

18. Click **Create**.
    The *Storage Dataflow Processing* is created. You are now prompted to **Synchronize** the subsystem to save the changes.

Adding an xDR Dataflow Processing Feed Manually – Storage (DataBroker)

You can manually add a storage xDR dataflow procession session (DataBroker) 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.

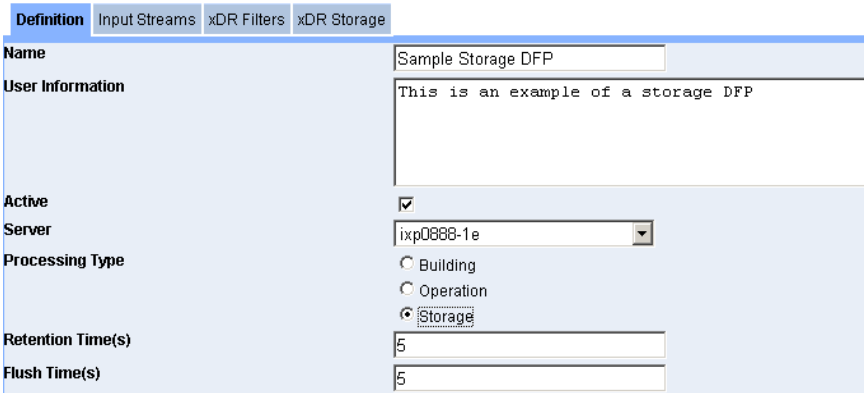


Figure 216: Xdr Definition Screen

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* (Defalt is 5 sec).
11. Click **Next**.
    The list of *Input Steams* appears.

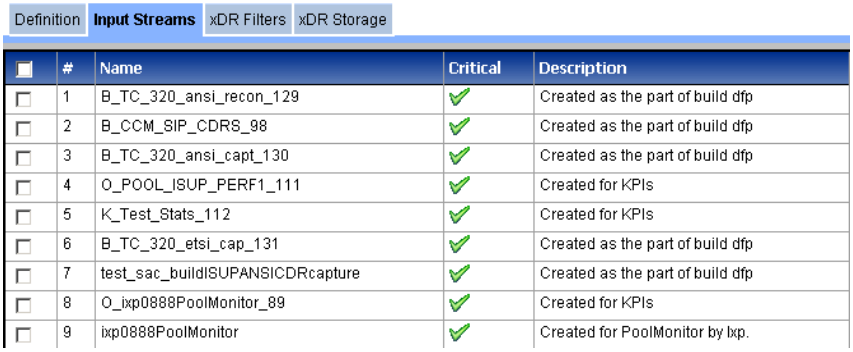


Figure 217:Input Stream Screen

12. Select the **Input Steams** to be used in the *Dataflow Processing*.

    Note: Input Stream must be selected for the DataBroker Builder. If the input stream selected is not from DataBroker Builder then this (DataBroker Storage Feed) Store DFP will not be available under XdrStorage Tab and hence it can't be created.

13. Click **Next**.
    The *xDR Filter* screen appears.

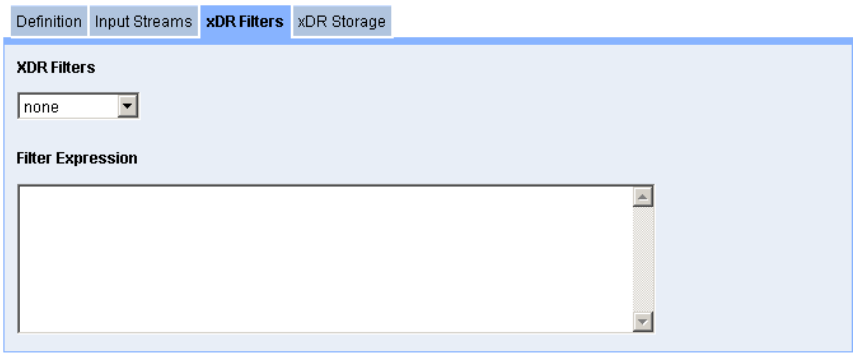


Figure 218: Xdr Filter Screen

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.

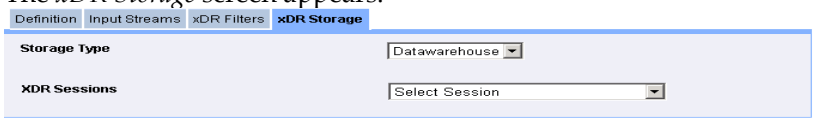


Figure 219: xDR Storage Screen

16. **Select** The Storage Type
    Select *DataBroker* As the Storage Type in the Storage Type Drop Down. The Default Parameters for DataBroker Storage Feed are loaded.

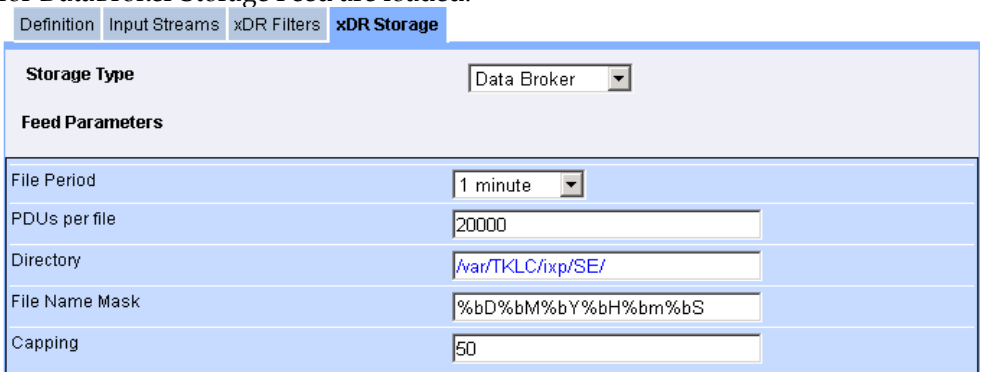


Figure 220: xDR Storage Screen

17. Enter **DataBroker** Parameters

File Period: Select File Period value from the List Box. Possible Values are 20 Seconds, 30 seconds, 1 Minute, 5 Minutes, 10 Minutes, 15 Minutes, 1 hour

PDUs Per File: This parameter denotes maximum number of PDUs per DataBroker File if File Period is not reached. Deafult Value is 20000. Possible Values are in Range 1000 – 1000000

Directory: This parameter denotes the relative directory on IXP from the Customer mounted NFS Directory where the files will be generated. Possible values are any valid path String starting with /.

File Name Mask: This parameter denotes the file Name Pattern of the DataBroker output file. Default pattern for DataBroker Type Feed is "%bD%bM%bY%bH%bm%bS". Enter valid file pattern or use the Default File Name Pattern

A file name mask is a text string made of figures, letters, "_" and "-"; except "%", no other character is allowed. If a "%" character is encountered, it must be followed by any of:

- LT": can only be at the first place; means that the date fields have to be converted to local time zone (as defined in the operating system)
- "bD": day in the month (2 digits, 01 to 31) of the beginning of the file period
- "bM": month (2 digits, 01 to 12) of the beginning of the file period
- "bY": year (4 digits) of the beginning of the file period
- "bH": hours (2 digits, 00 to 23) of the beginning of the file period
- "bh": hours (2 digits, 01 to 12) of the beginning of the file period
- "bA": "AM" or "PM" of the hour of the beginning of the file period
- "bm": minutes (2 digits, 00 to 59) of the beginning of the file period
- "bS": seconds (2 digits, 00 to 59) of the beginning of the file period
- "eD": day in the month (2 digits, 01 to 31) of the end of the file period
- "eM": month (2 digits, 01 to 12) of the end of the file period
- "eY": year (4 digits) of the end of the file period
- "eH": hours (2 digits, 00 to 23) of the end of the file period
- "eh": hours (2 digits, 01 to 12) of the end of the file period
- "eA": "AM" or "PM" of the hour of the end of the file period
- "em": minutes (2 digits, 00 to 59) of the end of the file period
- "eS": seconds (2 digits, 00 to 59) of the end of the file period

E.g.- With Default File Name Mask (%bD%bM%bY%bH%bm%bS), the file generated on 05th Octorber 2012 (11:15 am) at could be 05102012111500

Capping: This parameter denotes the Output Capping in Mbps. Default Values is 50 and possible Values are in the range 1-999. (This Field could be left empty)

18. Click **Create**.

The *Storage Dataflow Processing* is created. You are now prompted to **Synchronize** the subsystem to save the changes

Adding an xDR Dataflow Processing Feed Manually – Storage (CSV Streaming)

Note: To Create This Type of Storage Dataflow Processing CSV license must be enabled otherwise the option to choose this type of Store DFP will not be available in the wizard.

You can manually add a storage xDR dataflow processing (CSV) 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.

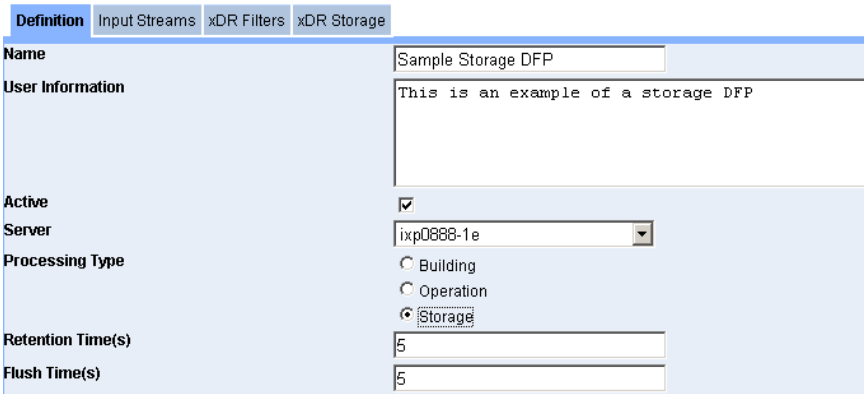


Figure 221: xDR Operation Screen

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* (Defalt is 5 sec).
11. Click **Next**.
    The list of *Input Steams* appears.

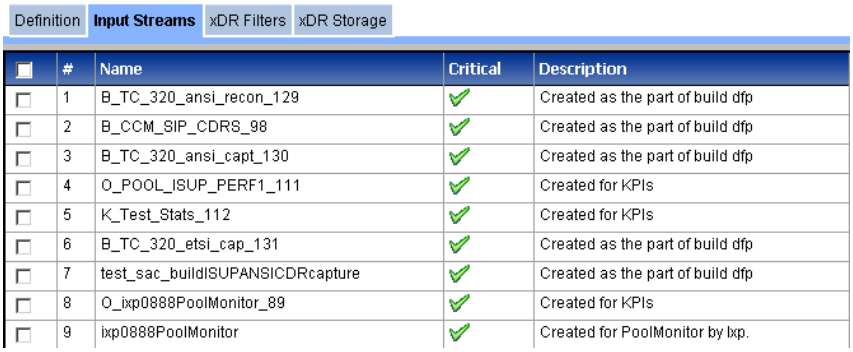


Figure 222: Input Streams Screen

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.

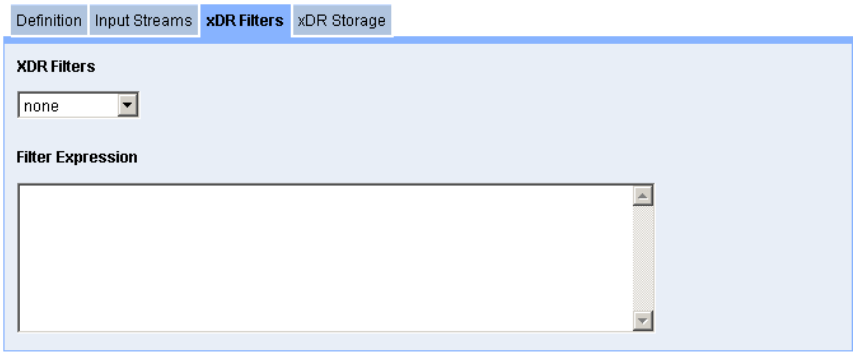


Figure 223; xDR Filter Screen

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.

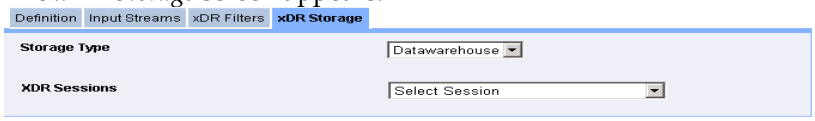


Figure 224: xDR Storage Screen

16. **Select** The Storage Type
Select *CSV* As the Storage Type in the Storage Type Drop Down. Then the parameters for this type of Storage DFP are loaded with default values.

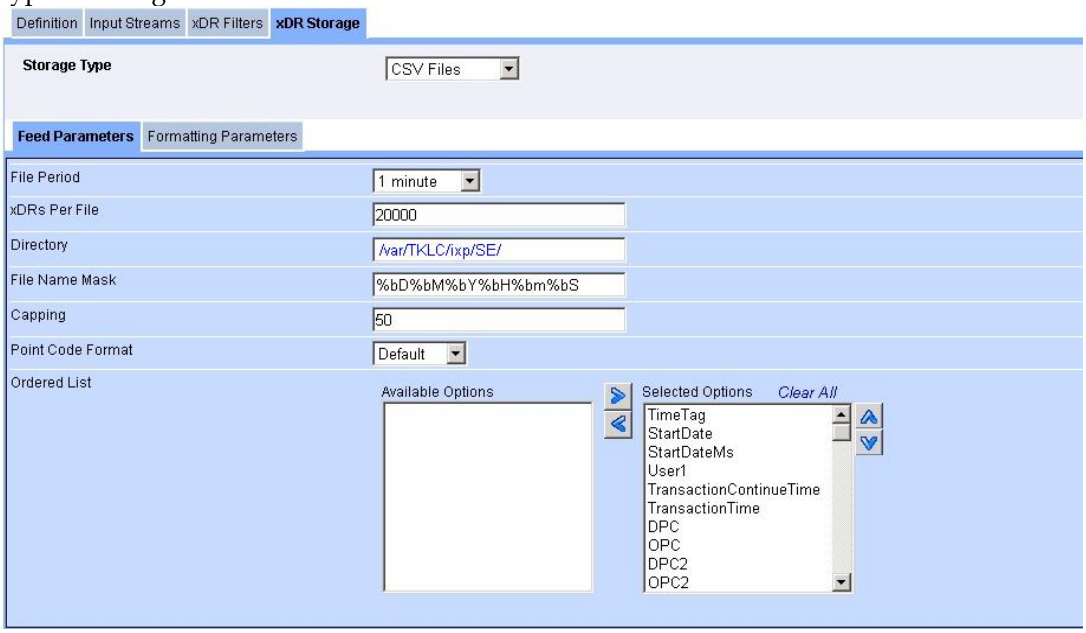


Figure 225: xDR Storage Screen

17. **Enter the Parameters**
    a. **Enter Feed Parameters**

File Period: Select File Period value from the List Box. Possible Values are *20 Seconds, 30 seconds, 1 Minute, 5 Minutes, 10 Minutes, 15 Minutes, 1 hour*
XDRs Per File: This parameter denotes maximum number of xDRs per CSV File if File Period is not reached. Deafult Value is *20000*. Possible Values are in Range *1000 – 1000000*

Directory: This parameter denotes the directory relatively to /var/TKLC/ixp/StoreExport on IXP from the Customer mounted NFS Directory where the files will be generated. Possible values are any valid path String starting with /.

File Name Mask: This parameter denotes the file Name Pattern of the CSV output file. Default pattern for CSV Type Feed is "*%bD%bM%bY%bH%bm%bS-%eD%eM%eY%eH%em%eS*". Enter valid file pattern or use the Default File Name Pattern

A file name mask is a text string made of figures, letters, "_" and "-"; except "%", no other character is allowed. If a "%" character is encountered, it must be followed by any of:

- LT": can only be at the first place; means that the date fields have to be converted to local time zone (as defined in the operating system)
- "bD": day in the month (2 digits, 01 to 31) of the beginning of the file period
- "bM": month (2 digits, 01 to 12) of the beginning of the file period
- "bY": year (4 digits) of the beginning of the file period
- "bH": hours (2 digits, 00 to 23) of the beginning of the file period
- "bh": hours (2 digits, 01 to 12) of the beginning of the file period
- "bA": "AM" or "PM" of the hour of the beginning of the file period
- "bm": minutes (2 digits, 00 to 59) of the beginning of the file period
- "bS": seconds (2 digits, 00 to 59) of the beginning of the file period
- "eD": day in the month (2 digits, 01 to 31) of the end of the file period
- "eM": month (2 digits, 01 to 12) of the end of the file period
- "eY": year (4 digits) of the end of the file period
- "eH": hours (2 digits, 00 to 23) of the end of the file period
- "eh": hours (2 digits, 01 to 12) of the end of the file period
- "eA": "AM" or "PM" of the hour of the end of the file period
- "em": minutes (2 digits, 00 to 59) of the end of the file period
- "eS": seconds (2 digits, 00 to 59) of the end of the file period

E.g.- With Default File Name Mask (%bD%bM%bY%bH%bm%bS-%eD%eM%eY%eH%em%eS), the file generation started at 05th Octorber 2012 (11:15 am) and ended on 05th Octorber 2012 (11:30 am) at could be 05102012111500-05102012113000

Capping: This parameter denotes the Output Capping in Mbps. Default Values is 50 and possible Values are in the range *1-999.* (This Field could be left empty)

Point Code Format: This parameter denotes the point code flavor. You can select one of following values *Default, ANSI, ETSI_I, ETSI_N, Chinese, Japanese*

Ordered List: You can define the ordering of the fields from dictionary. Then the output CSV Files should maintain the order specified in this parameter. Some Dictionary Fields could be deselected while creating Storage DFP. Select and Move the fields using Left Arrow Button from *Selected Options* to *Available Options* if you don't want to keep the fields in output CSV Files.

b. Formatting Parameters

Select This Tab to Specify User Preferences.

Following Screen appears

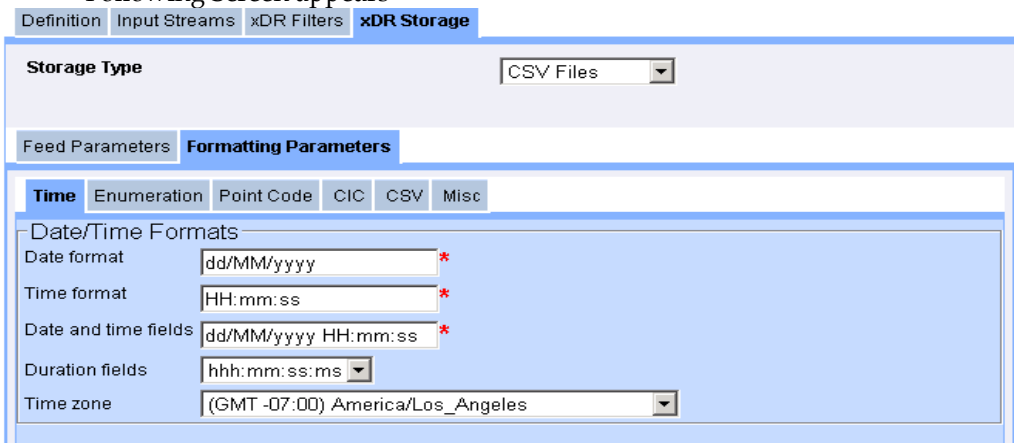


Figure 226: xDR Storage Screen

Specific preferences will be applied while creating the Storage DFP as selected by user in this screen.

Note: - All the preferences screen are same as global user preferences and as in previous release except for CSV preference. CSV Preference is provided for CSV type Storage DFP formatting.

Select Time Tab for Time Related preferences. E.g. you can change Date and Time formats, TimeZone etc.

Select Enumeration Tab for providing Mapping. Following mapping are provided

- Translate ENUM values
- Point Code to Node Name
- Link Short Name to Long Name

Select point Code Tab for Point Code related preferences. You can select whether point code format is displayed in Hexadecimal or Decimal Format.

Select CIC tab for CIC Related Preferences. You can select whether this field is displayed in Hexadecimal or Decimal Format.

Select CSV tab for specifying CSV File Related preferences. This TAB look like as below

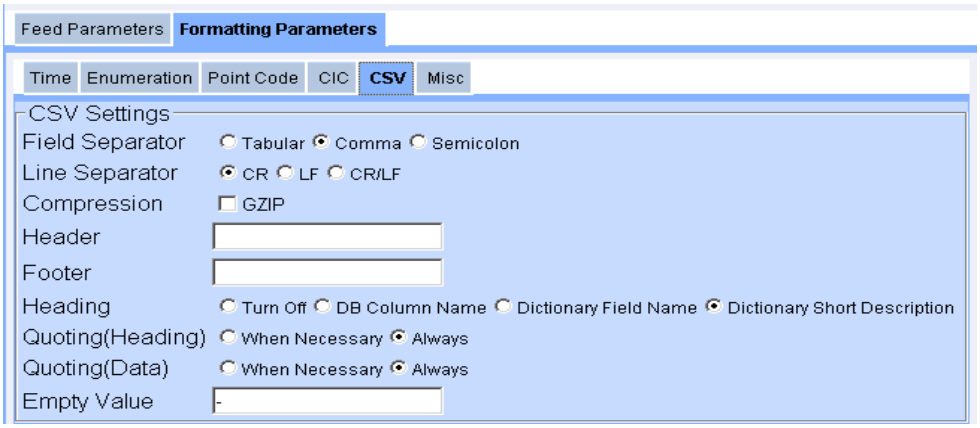


Figure 227: Formatting Parameters(CSV) screen

Field Separator :- Select whether the fields in CSV File generated from this DFP are separated by *Tabular* or *Comma* or *Semicolon* Field.
Line Separator :- Select whether the record lines in CSV File should be separated by *CR, LF* or *CR/LF*
Compression :- Click CheckBox if CSV Files Need to be compressed in *GZIP* format.
Header :- Input header text that should appear as header in the CSV File Generated.
Footer :- Input Footer text that should appear as footer in the CSV File Generated.
Heading :- Select one of Radio Button to provide any one of Heading in the CSV File.
Quoting (Heading) :- Select Either "When Necessary" or "Always" to specify quoting on heading field.
Quoting (Data) : - Select Either "When Necessary" or "Always" to specify quoting on Data field.
Empty Value :- Provide the String for Empty Value in CSV Text File.

18. 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.

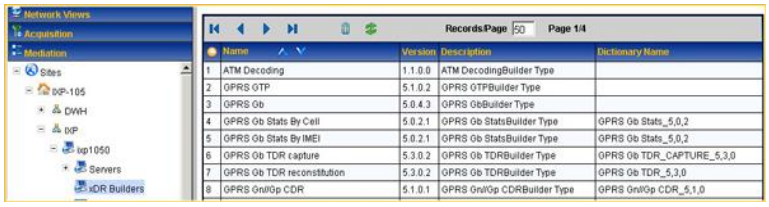


Figure 228: Xdr Builder List Screen

The following information is provided:

Column	Description
Name	xDR Builder Name

Column	Description
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

TABLE 99: XDR BUILDER LIST DESCRIPTIONS

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 Subsytems.

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.

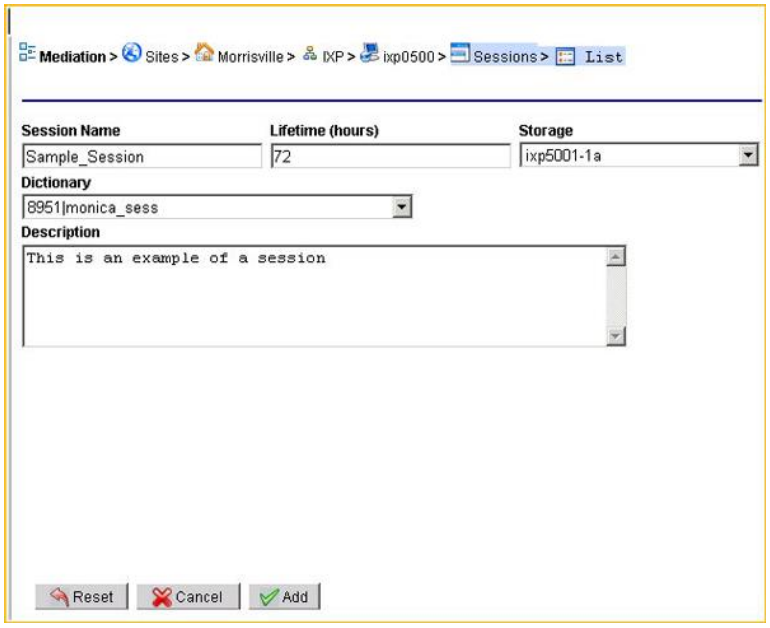


Figure 229: Add Sessions Screen

3. Type a **Session Name**.

   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 Subsytems*.

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.

Figure 230: 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.

Figure 231: Selected Session For Modification

3. Click **Modify** on the toolbar.
   The *Session Record* opens.
4. Make the **needed modifications**.

Note: IF session point code feature is enabled then to modify flavor of session refer ***Appendix D: Defining and Modifying Flavor (PC Format) of Session at CCM***

Note: You cannot 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 cannot 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 a dSIP-T/SIP xDRs manually using the build process.

Note: In addition, in configuring partial ANSI ISUP a 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 *xDR Storage* screen is shown below.

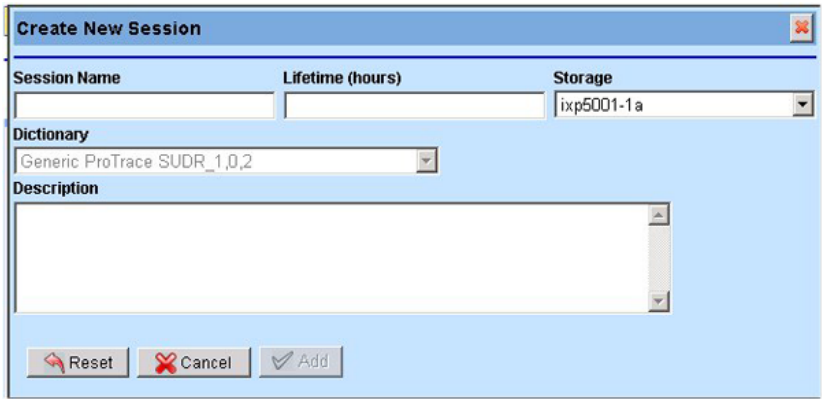


Figure 232: Create Session Screen

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.

   Note: IF session point code feature is enabled then to configure flavor of session refer ***Appendix D: Defining and Modifying Flavor (PC Format) of Session at CCM***

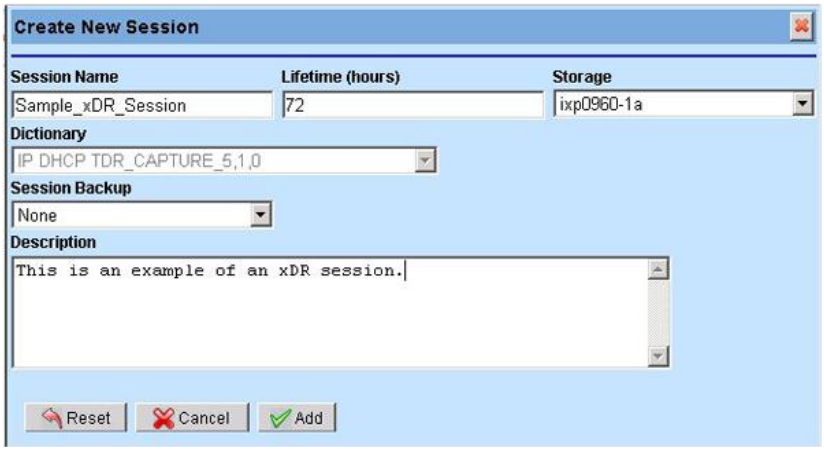


Figure 233: Completed Xdr Session Screen

7. Click Add.

The *Session* is created and the *Session Name* shows up in the *Session* field shown below.

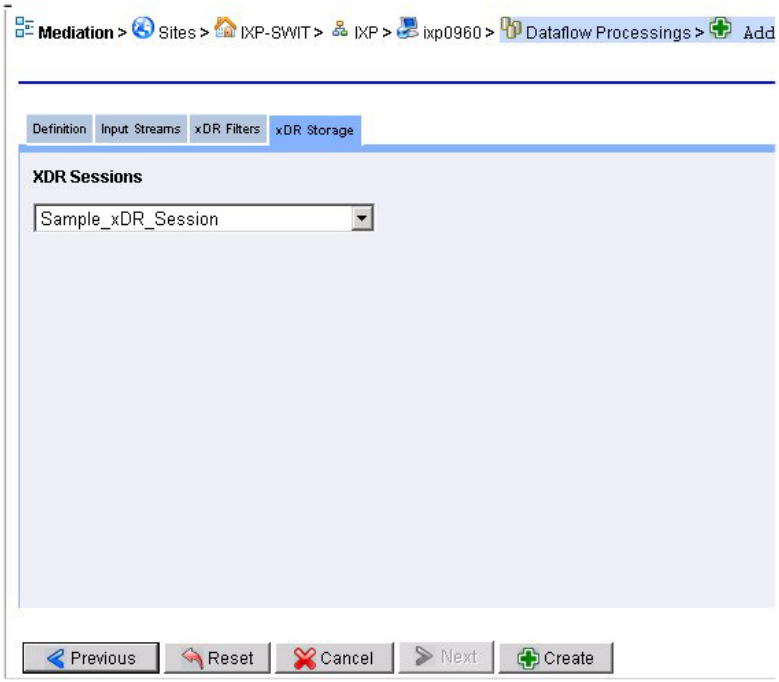


Figure 234: Added Session in Xdr Storage Screen

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 See About Applying Changes to a Subsystem (Synchronizing).

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.

4. Click **Delete**.
5. Click **OK** at the prompt.
   The *Dataflow Processing* is deleted. You must now **Synchronize** the subsystem. See About Applying Changes to a Subsystem (Synchronizing).

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 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

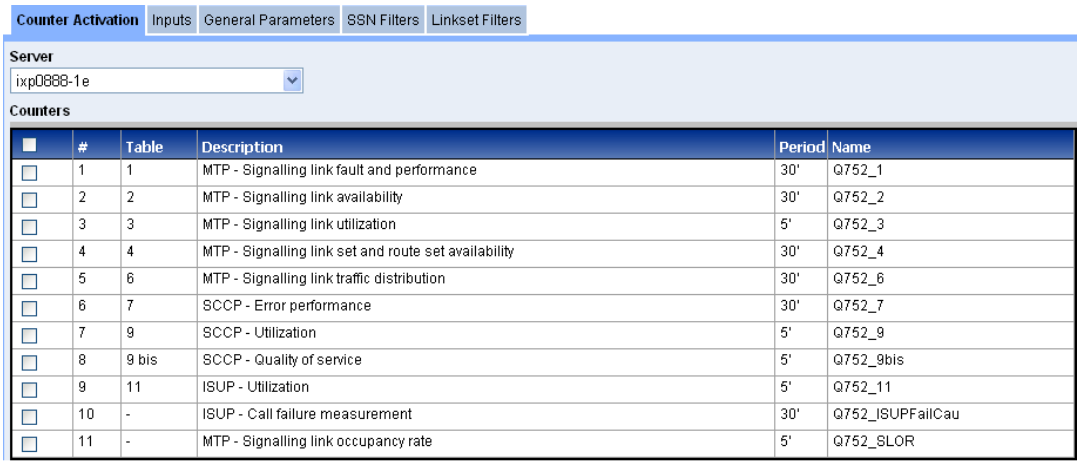
The Q.752 Dataflow Assistant option provides a wizard to help you quickly create a Q.752 processing. The process follows five stages:

- 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



	#	Table	Description	Period	Name
☐	1	1	MTP - Signalling link fault and performance	30'	Q752_1
☐	2	2	MTP - Signalling link availability	30'	Q752_2
☐	3	3	MTP - Signalling link utilization	5'	Q752_3
☐	4	4	MTP - Signalling link set and route set availability	30'	Q752_4
☐	5	6	MTP - Signalling link traffic distribution	30'	Q752_6
☐	6	7	SCCP - Error performance	30'	Q752_7
☐	7	9	SCCP - Utilization	5'	Q752_9
☐	8	9 bis	SCCP - Quality of service	5'	Q752_9bis
☐	9	11	ISUP - Utilization	5'	Q752_11
☐	10	-	ISUP - Call failure measurement	30'	Q752_ISUPFailCau
☐	11	-	MTP - Signalling link occupancy rate	5'	Q752_SLOR

Figure 235: 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.

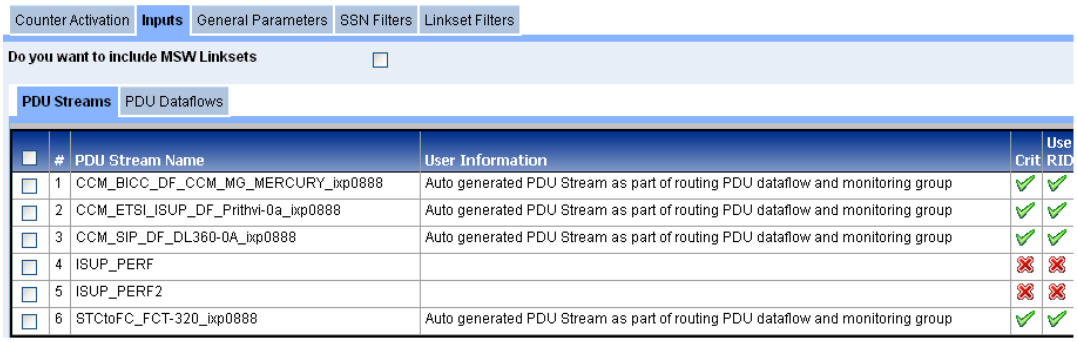


Figure 236: Inputs Screen (PDU Streams Tab)

4. Select one or more **PDU Streams** from the list.
   If you want to add Dataflows, complete steps 7 thru 9
5. (Optional) If you want *Message Switch* linksets included, click **MSW** field where it asks you if you want *MSW* linksets.
6. Select the **PDU Dataflows** tab.

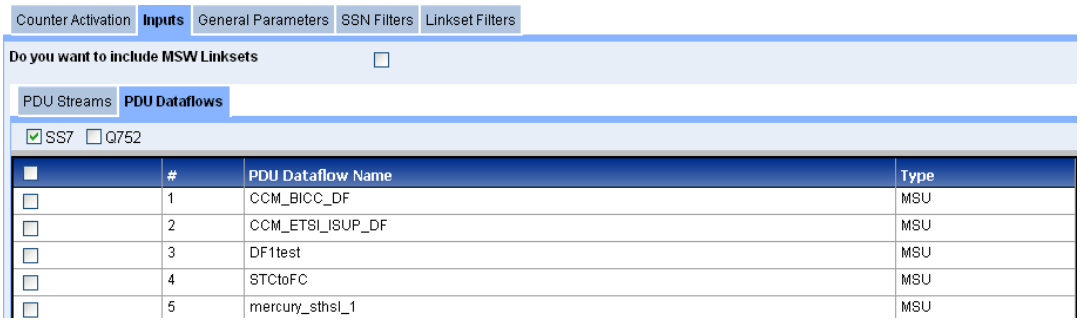


Figure 237: Inputs Screen (PDU Dataflows Tab)

7. Select what type of **Dataflow** (SS7 / Q.752).

   Note: You can select both types of input streams.

8. Select one or more **PDU Dataflows** from the list.
9. Click **Next**.
   The *General Parameters* screen appears.

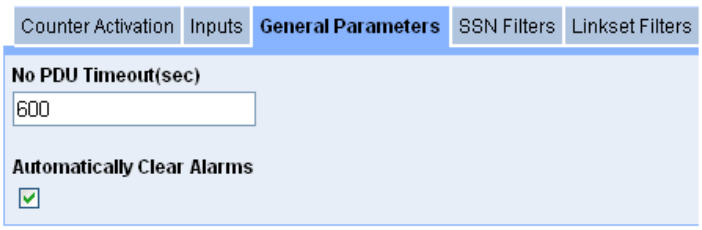


Figure 238: General Parameters Screen

10. Enter the number of sec in the **No PDU Timeout** field (default is 600).
11. (Optional) Select to **automatically clear alarms** after the process has run.
12. Click **Next**.
    The *SSN Filter* screen appears.

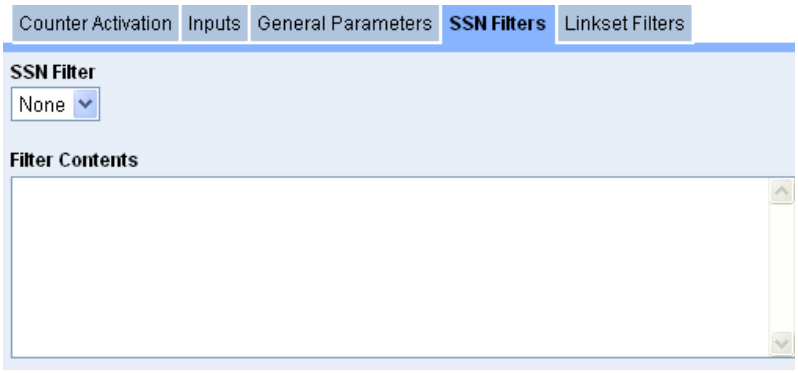


Figure 239: Linkset Filters Tab

13. Select the **SSN Filter** type from the pull-down menu.
    The content of the *Filter* appears in the Filter Contents field.
14. Click **Next**
    The *Linkset Filters* screen appears.

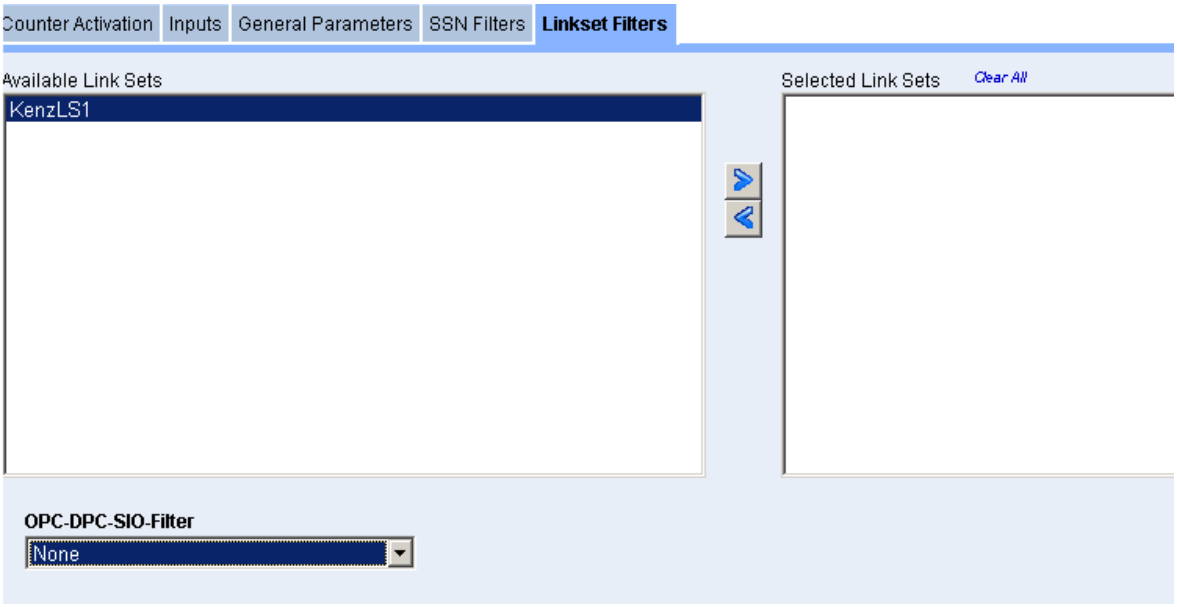


Figure 240: Linkset Filters Tab

1. Select one or more **Available Linksets**.
2. Click right arrow to place them into the **Selected Linksets** field.
3. (Optional-according to the linksets used) Select an **OPC-DPC-SIO Filter**.
4. Click **Finish**.
   The configured *Q.752 Processing* is saved.

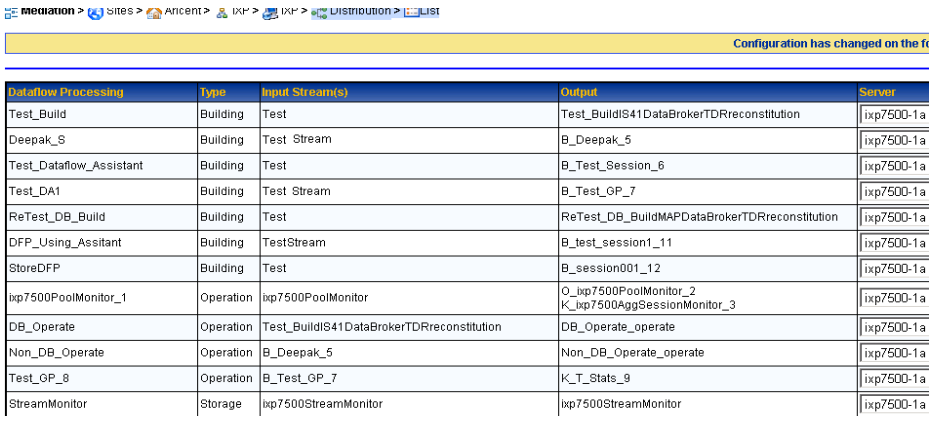
   Note: Make sure you **Apply Changes** for the changes to be reflected in the IXP Subsystem.

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	Server
Test_Build	Building	Test	Test_BuildIS41DataBrokerTDRreconstitution	ixp7500-1a
Deepak_S	Building	Test Stream	B_Deepak_5	ixp7500-1a
Test_Dataflow_Assistant	Building	Test	B_Test_Session_6	ixp7500-1a
Test_DA1	Building	Test Stream	B_Test_GP_7	ixp7500-1a
ReTest_DB_Build	Building	Test	ReTest_DB_BuildMAPDataBrokerTDRreconstitution	ixp7500-1a
DFP_Using_Assitant	Building	TestStream	B_test_session1_11	ixp7500-1a
StoreDFP	Building	Test	B_session001_12	ixp7500-1a
ixp7500PoolMonitor_1	Operation	ixp7500PoolMonitor	O_ixp7500PoolMonitor_2 K_ixp7500AggSessionMonitor_3	ixp7500-1a
DB_Operate	Operation	Test_BuildIS41DataBrokerTDRreconstitution	DB_Operate_operate	ixp7500-1a
Non_DB_Operate	Operation	B_Deepak_5	Non_DB_Operate_operate	ixp7500-1a
Test_GP_8	Operation	B_Test_GP_7	K_T_Stats_9	ixp7500-1a
StreamMonitor	Storage	ixp7500StreamMonitor	ixp7500StreamMonitor	ixp7500-1a

Figure 241: 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:

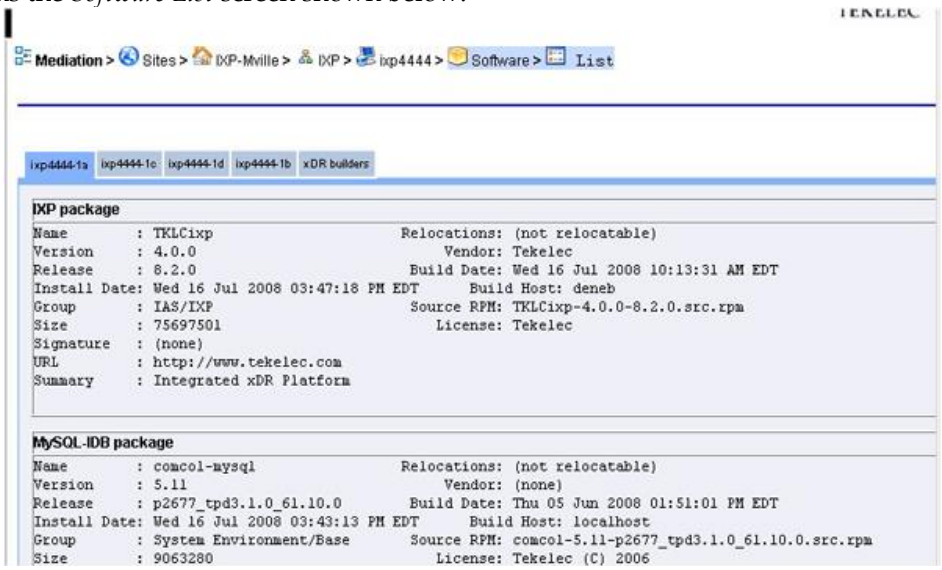


Figure 242: Software List Screen

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

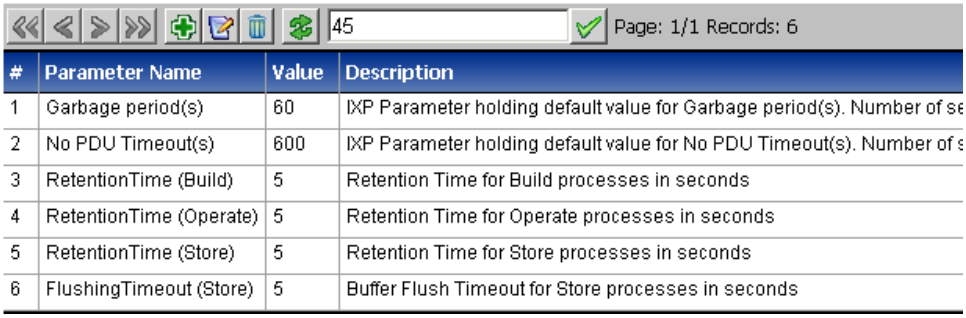
Subsystem references enable you to create preferences with values for the Subsystem.

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.



45 Page: 1/1 Records: 6

#	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 s
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 243: Subsystem Preferences List Screen

2. Click **Add**.
   The *Subsystem Preferences Add* screen opens shown below.

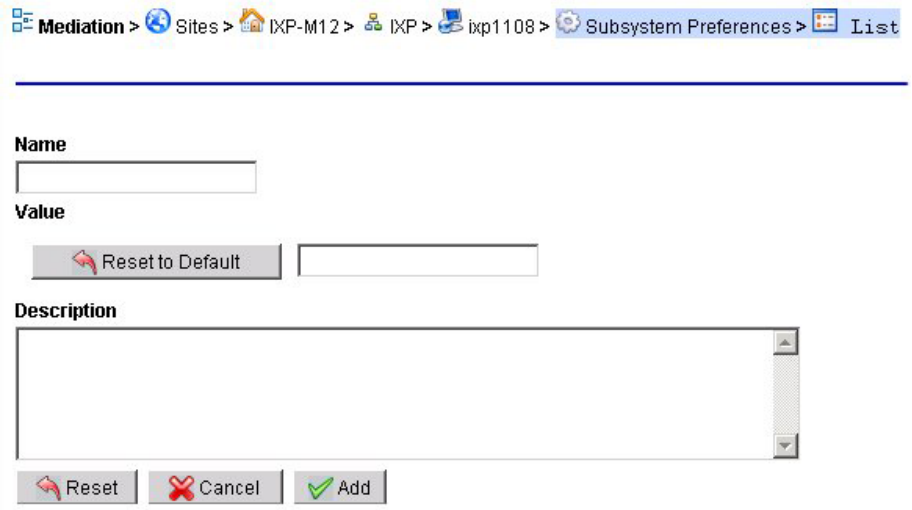


Figure 244: Subsystem Preferences List Screen

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.

- Q.752 filters - see About Q.752 Filters.
- xDR filters - see About xDR Filters.
- Dictionaries - see About Dictionaries.
- Sessions - see About Sessions.

About Q.752 Filters

Each IXP subsystem has the capability to generate Q.752 statistics based on incoming PDU streams. IXP supports filtering the PDUs using SSN and DPC-OPC-SIO filters. These filters are defined globally. The filters are referenced when configuring Q.752 for any IXP Subsystem.

Selecting *Q.752 Filters* in the object tree opens its two options:

- SSN Filters
- DPC-OPC-SIO filters.

Figure 245: SSN Filters List Screen

Creating SSN Filters

Complete these steps to add an SSN Filter:

1. Select **Q.752 Filters > SSN Filters > List**.
   The *List* screen opens.
2. Click **Add**.
   The *Add* screen opens shown below.

Field	Description
Filter Name	Alphanumeric field for creating an SSN filter name. The name cannot contain spaces.
Enter SSN	Numeric field where an integer is entered between 1-255.
Add filter button	Clicking this button, adds the SSN to the list, you must have a minimum of 1 and a maximum of 10 SSN's.
SSN List	Lists all the SSNs that you created.
Remove from List button	Removes the highlighted SSN from the list.

Field	Description
Reset button	Resets all the fields to their defaults (blank).
Cancel button	Cancels the procedure and returns you to a blank screen.
Create button	Saves the filter to the system and creates a record in the SSN list screen.

TABLE 100: ADD SSN FILTER SCREEN

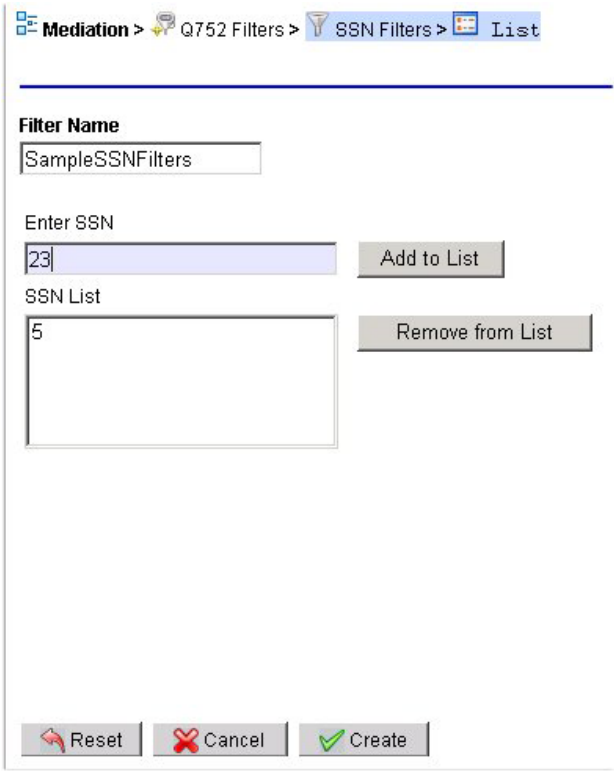


Figure 246: SSN Filter Add Screen

3. Enter a **Filter Name**.
4. Enter a **SSN** (integer 1-255).
5. Click **Add** to List.
   The *SSN* is added to the list.
6. Repeat steps 4 & 5 to add more SSNs.
7. Click **Create**.
   The *Filter* is added to the SSN List screen shown below.

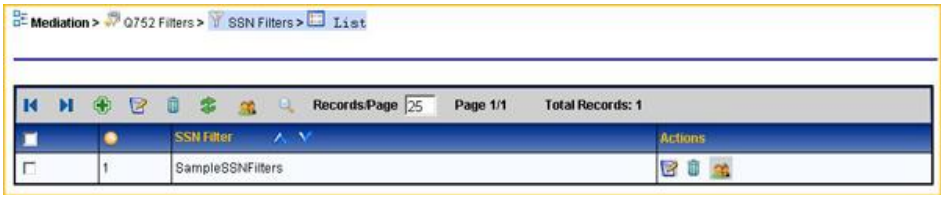


Figure 247: SSN Filter Add Completed

Modifying an SSN Filter

Complete these steps to modify an SSN from a Filter:

Note: If the SSN filter is associated with a Q.752 configuration and the filter is modified, it results in the modification of the Q.752 configuration internally.

1. Select **Q.752 Filters > SSN filters > List**.
   The *List* screen opens.
2. Select the **SSN Filter** to be modified.

3. Click **Modify**.
   The *Modify* screen opens.
4. Make the **needed modifications**.
5. Click **Modify**.
   The *Record* is modified.

Using remove from list Operation

Complete these steps to remove an SSN from a Filter using the remove from list operation:

1. When the filter record is open, (either in the add mode or modify mode), **highlight** the **SSN** to be removed.
2. Click the **Remove from List** button.
3. Click either **Create** or **Modify** (depending on which mode you are in).
   The *SSN* is removed from the list.

Deleting an SSN Filter

Complete these steps to delete an SSN from a filter:

Note: If the SSN filter is associated with a Q.752 configuration you cannot delete the filter in this location. You have to manually remove the filter by navigating to the Q.752 configuration and setting the SSN Filter to none. You will then have to return to this location to delete the filter.

1. Select **Mediation > Q.752 Filters > SSN Filters > List**.
   The *List* screen opens.
2. Select the **SSN Filter** to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.
   The *Filter* is deleted.

Listing OPC-DPC-SIO Filters

Select **Mediation >Q.752 filters > OPC-DPC-SIO Filters**.
The *List* screen opens shown below.

Figure 248: OPC-DPC-SIO Filters List Screen

From this screen you can add new OPC-DPC-SIO filters or manage existing ones.

Field	Description
Filter Name	Alphanumeric field for creating an SSN filter name. The name cannot contain spaces.
Select Flavor	Pull-down list that has the different protocol/flavors. You can have multiple flavors in one filter.
OPC	Originating Point Code is entered here in the appropriate format/flavor
DPC	Destination Point Code is entered here in the appropriate format/flavor
SIO	Service Indicator is entered as an integer between 1-1million
Add to list button	Clicking this button, adds the OPC-DPC-SIO combination to the list, you must have a minimum of 1 and a maximum of 5 OPC-DPC-SIO's.
OPC-DPC-SIO List	Lists all the SSNs that you created.
Remove from List button	Removes the highlighted SSN from the list.
Reset button	Resets all the fields to their defaults (blank).
Cancel button	Cancels the procedure and returns you to a blank screen.
Create button	Saves the filter to the system and creates a record in the OPC-DPC-SIO list screen.

TABLE 101: ADD OPC-DPC-SIO FILTERS SCREEN

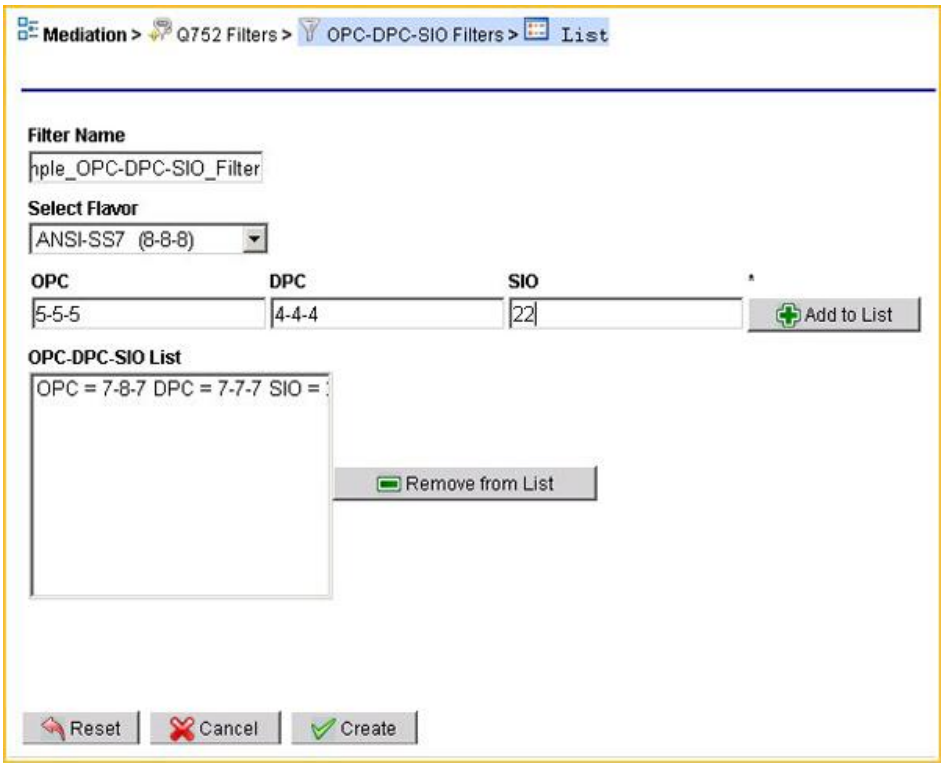


Figure 249: OPC-DPC-SIO Add Screen - Completed

4. Enter a **Filter Name**.
5. Select a **Flavor**.
6. Enter a **OPC** (same format as selected).
7. Enter a **DPC** (same format as selected).
8. Enter a **SIO** (integer between 1-1 million).
9. Click **Add** to List.
   The *OPC-DPC-SIO* is added to the list.
10. Repeat steps 4 & 5 to add more OPC-DPC-SIOs.
11. Click **Create**.
    The *Filter* is added to the OPC-DPC-SIO List screen shown below.

Figure 250: OPC-DPC-SIO Filter Add Completed

Modifying an OPC-DPC-SIO Filter

Complete these steps to modify an OPC-DPC-SIO from a filter:

Note: If the OPC-DPC-SIO filter is associated with a Q.752 configuration and the filter is modified, it results in the modification of the Q.752 configuration internally.

1. Select **Mediation > Q.752 Filters > OPC-DPC-SIO Filters**.
   The *List* screen opens.
2. Select the **OPC-DPC-SIO Filter** to be modified.
3. Click **Modify**.
   The *Modify* screen opens shown below.
4. Make the **needed modifications**.
5. Click **Modify**.
   The *Record* is modified.

Removing an OPC-DPC-SIO number from filter List

Complete these steps to remove an OPC-DPC-SIO from a filter using the remove from list operation:

1. When the filter record is open, (either in the add mode or modify mode), **highlight** the **OPC-DPC-SIO** to be removed.
2. Click the **Remove from List** button.
3. Click either **Create** or **Modify** (depending on which mode you are in).
   The *OPC-DPC-SIO* is removed from the list.

Deleting an OPC-DPC-SIO Filter

Complete these steps to delete an OPC-DPC-SIO from a filter:

Note: If the OPC-DPC-SIO filter is associated with a Q.752 configuration you cannot delete the filter in this location. You have to manually remove the filter by navigating to the Q.752 configuration and setting the OPC-DPC-SIO filter to none. You will then have to return to this location to delete the filter.

1. Select **Mediation > Q.752 Filters > OPC-DPC-SIO Filters**.
   The *List* screen opens.
2. Select the **OPC-DPC-SIO Filter** to be deleted.
3. Click **Delete**.
4. Click **OK** at the prompt.
   The *Filter* is deleted.

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 PIC 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.

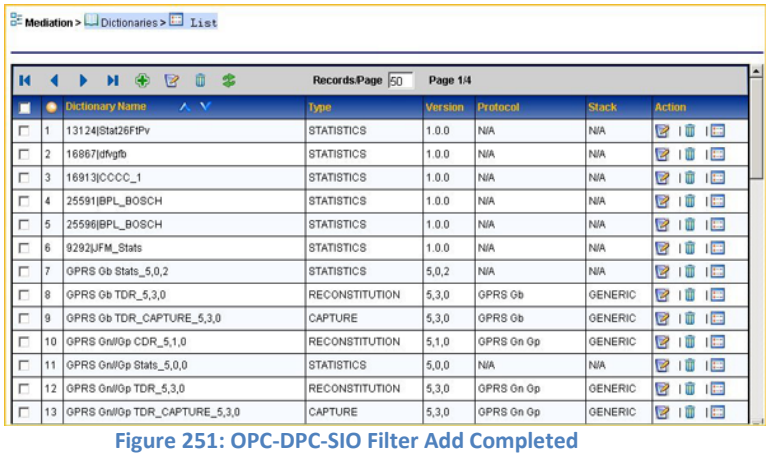


Figure 251: OPC-DPC-SIO Filter Add Completed

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.

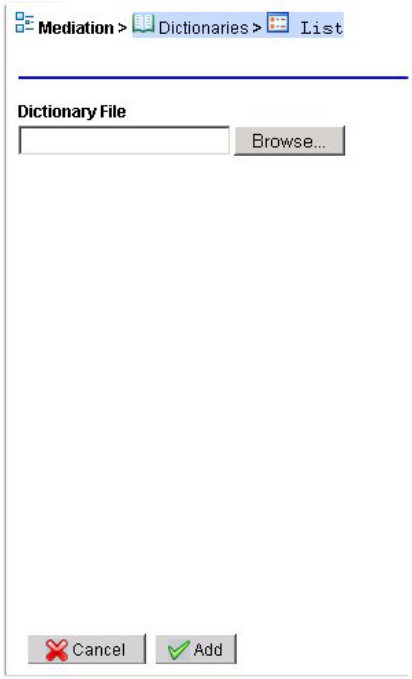


Figure 252: Add Dictionary Screen

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.

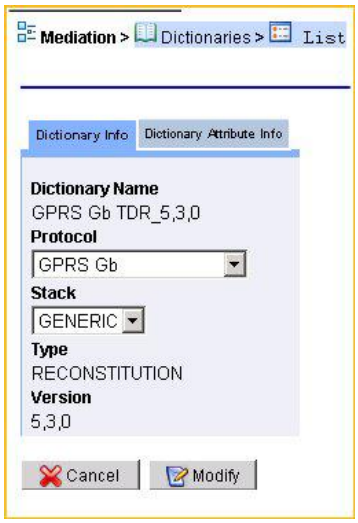


Figure 253: Modify Dictionary - Dictionary Info Tab

4.Select **Dictionary Info** tab.
5.Modify either the **Protocol** or **Stack** information.
6.Select **Dictionary Attribute Info** tab shown below.

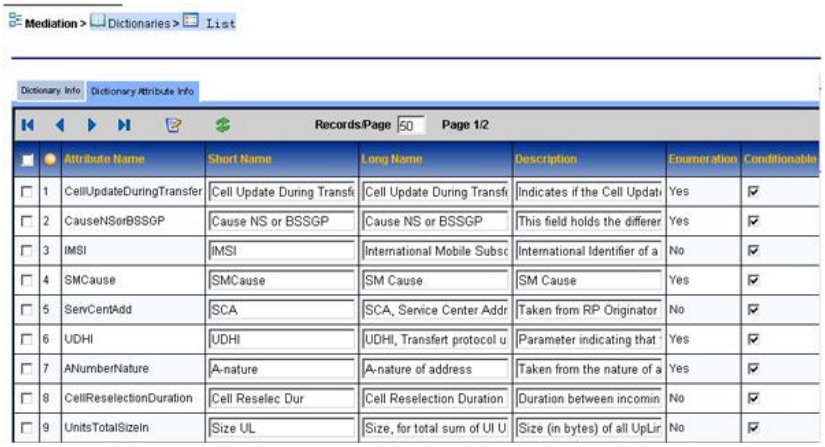


Figure 254: Modify Dictionary - Dictionary Attribute Info Tab

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 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 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 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**.

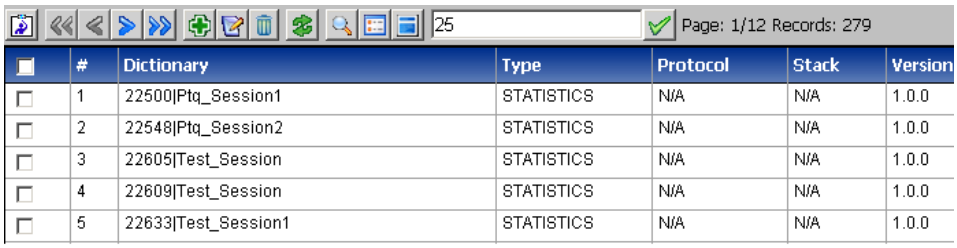
   Note: To delete only one dictionary file, click Delete in the actions column. To delete several dictionary files, select each file and click Delete on the toolbar.

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|Ptq_Session1	STATISTICS	N/A	N/A	1.0.0
2	22548|Ptq_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 255: Modify 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.

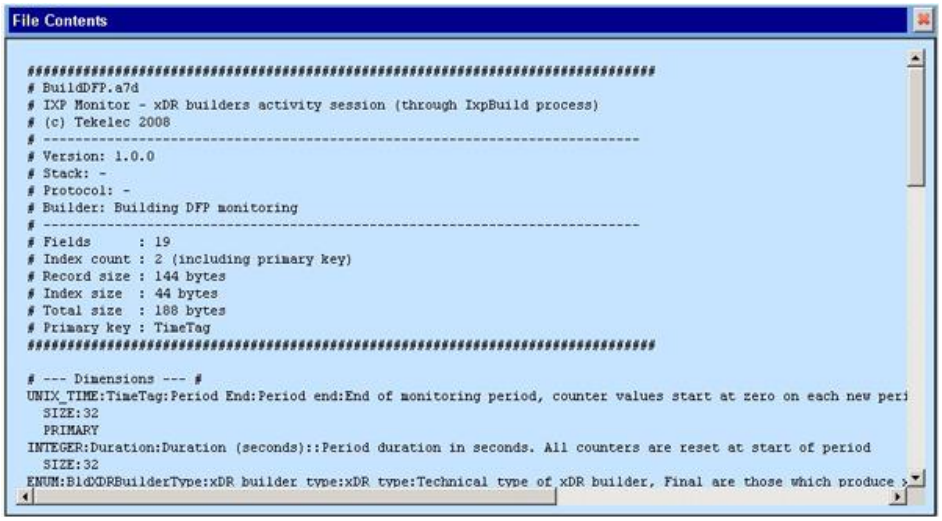


Figure 256: Dictionary List Screen

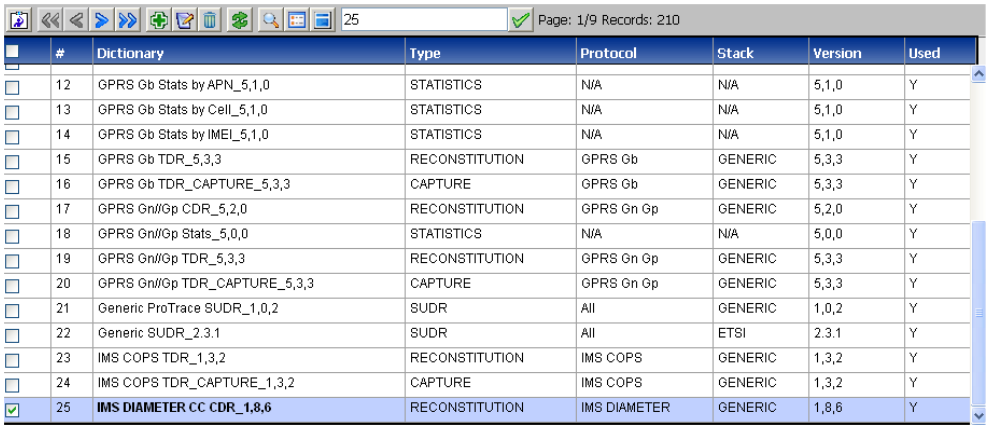
Click the **Close Icon** at the top right-hand corner of the screen to close the file.

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 257: Dictionary List with Unused Dictionary Selected

3. Select the **View Discrepancy Report** button on the tool bar to generate the report (last button on the right). The *Report* screen opens.

   The Report shows:

   - Basic Information
   - Non-ENUM Field(s) Descrepencies
   - ENUM Field(s) Descrepencies

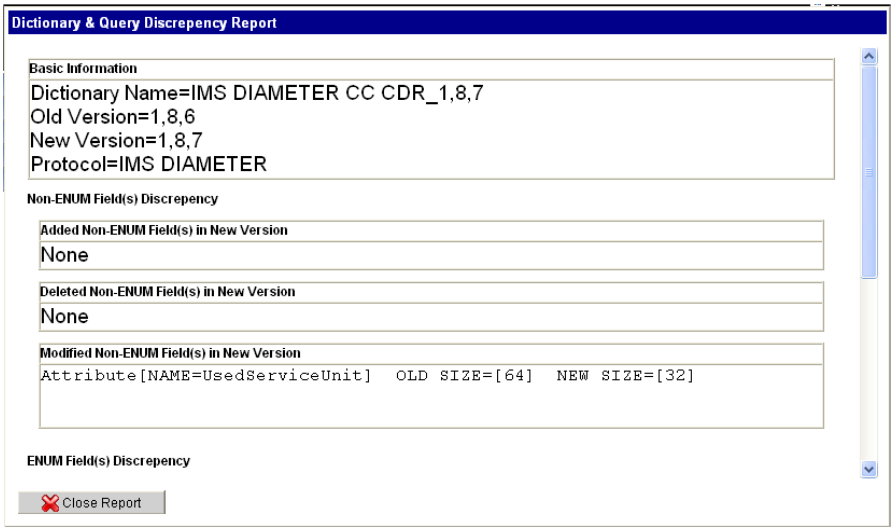


Figure 258: Unused Dictionary Discrepency Report

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.

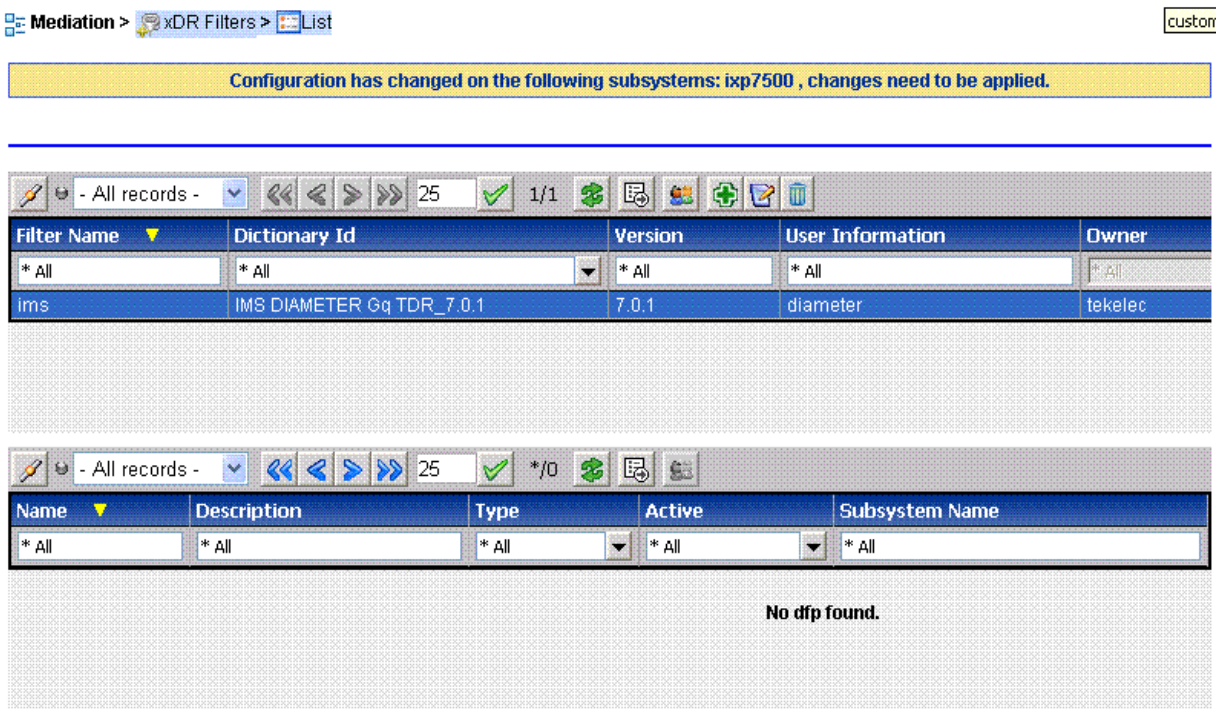


Figure 259: Xdr Filter List Screen

The child window at end of screen shows the information about associated DFPs with xDR Filter selected in master window.Figure below shows the sample screen

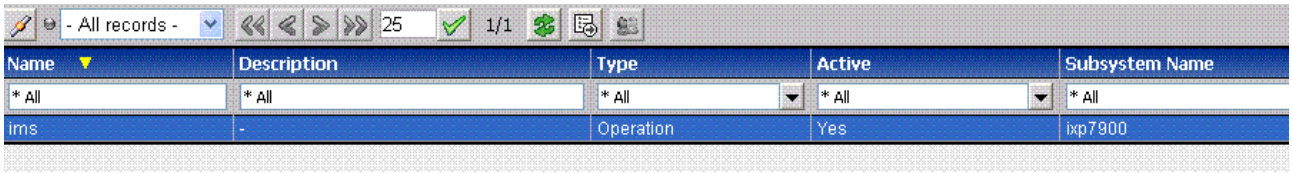


Figure 260: Associated DFP List

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 opens show below.

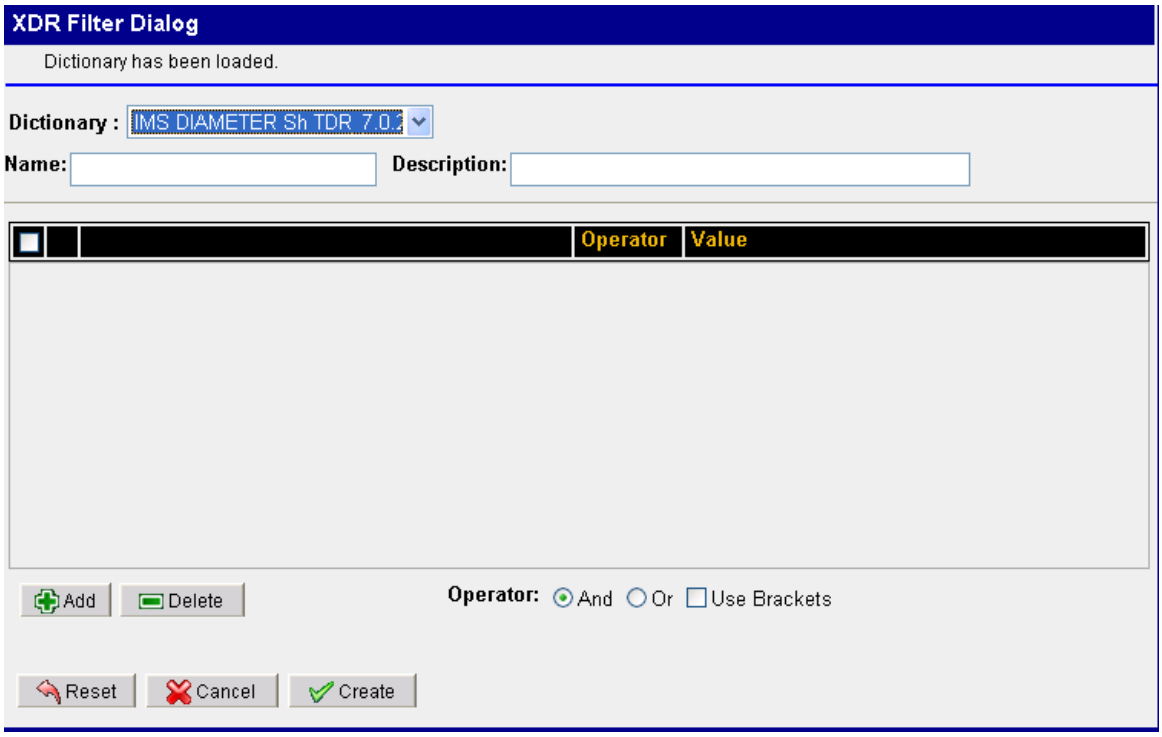


Figure 261: Xdr Filter Add Screen

3. Type in a **Filter Name**.
4. (Optional) Type in a description.
5. Select the **Dictionary** that is associated 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.

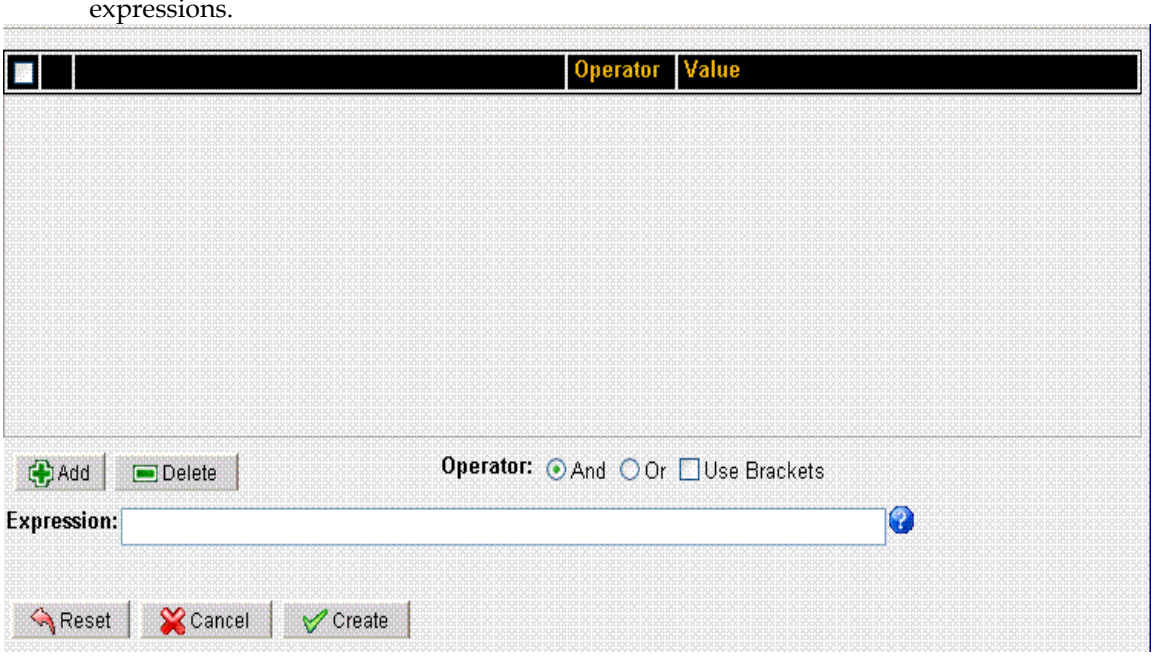


Figure 262: Filter Definition Screen

b. 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.

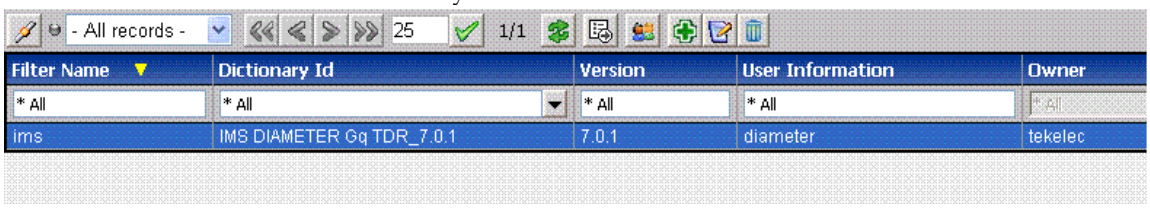


Figure 263: Added Xdr Filter To List

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* popup 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.

Note: Please refer **Appendix E: xDR Filters during Protocol Upgrade** for behavior during Protocol Upgrade.

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 Dataserver, but Sessions can have identical names if they reside on separate IXP Subsytems.

Selecting the Sessions object from the Object tree opens the xDR Sessions List screen.

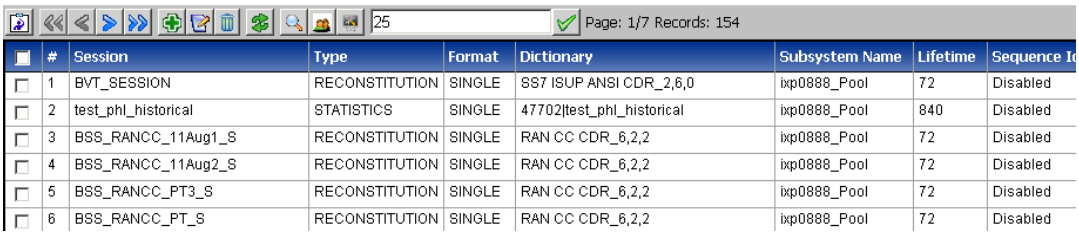


Figure 264: xDR Sessions List Screen

About xDR Session Table Layout

The *Sessions List* screen is in table format and has the follow information:

Column	Description
Select	Enables you to select one or more sessions
Session	Provides the name of the session
Type	Shows the type of session: • 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
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

TABLE 102: XDR TABLE LAYOUT

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:

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 mult-page list of sessions
Previous page	Enables you to go to the previous page of a mult-page list of sessions
Next page	Enables you to go to the next page of a mult-page list of sessions
Last page	Enables you to go to the last page of a mult-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

TABLE 103: XDR TOOL BAR

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 a 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.

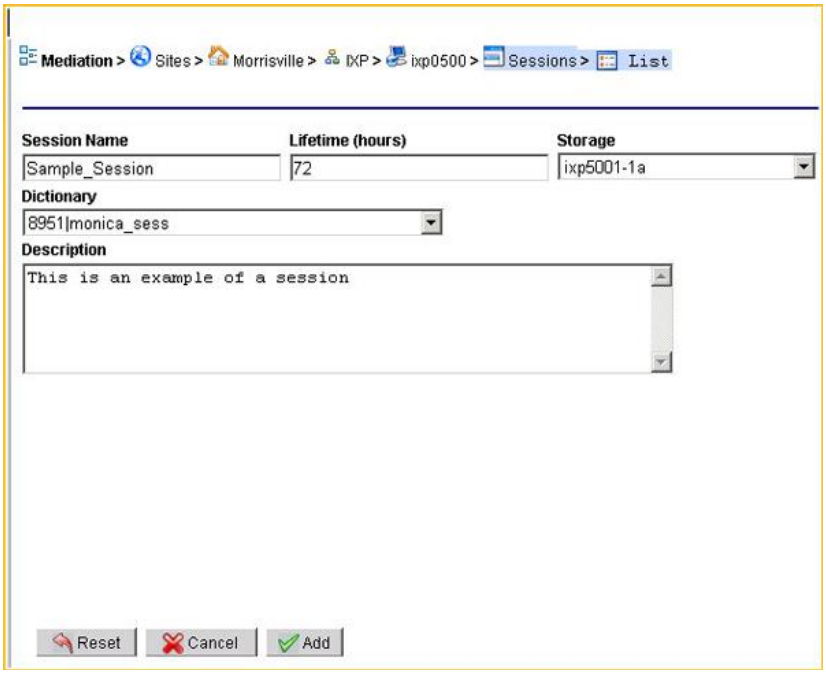


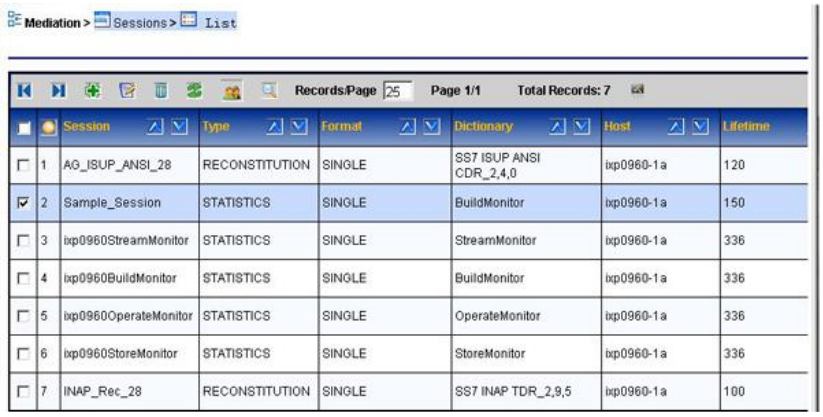
Figure 265: xDR Session Add Screen

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.



	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	ixp0960StreamMonitor	STATISTICS	SINGLE	StreamMonitor	ixp0960-1a	336
4	ixp0960BuildMonitor	STATISTICS	SINGLE	BuildMonitor	ixp0960-1a	336
5	ixp0960OperateMonitor	STATISTICS	SINGLE	OperateMonitor	ixp0960-1a	336
6	ixp0960StoreMonitor	STATISTICS	SINGLE	StoreMonitor	ixp0960-1a	336
7	INAP_Rec_28	RECONSTITUTION	SINGLE	SS7 INAP TDR_2,9,5	ixp0960-1a	100

Figure 266: 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
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	ixp5001StreamMonitor	STATISTICS	SINGLE	StreamMonitor	ixp5001-1a	336

Figure 267: Selected Session For Modification

3. Click **Modify** on the toolbar.
   The *Session Record* opens, shown below.

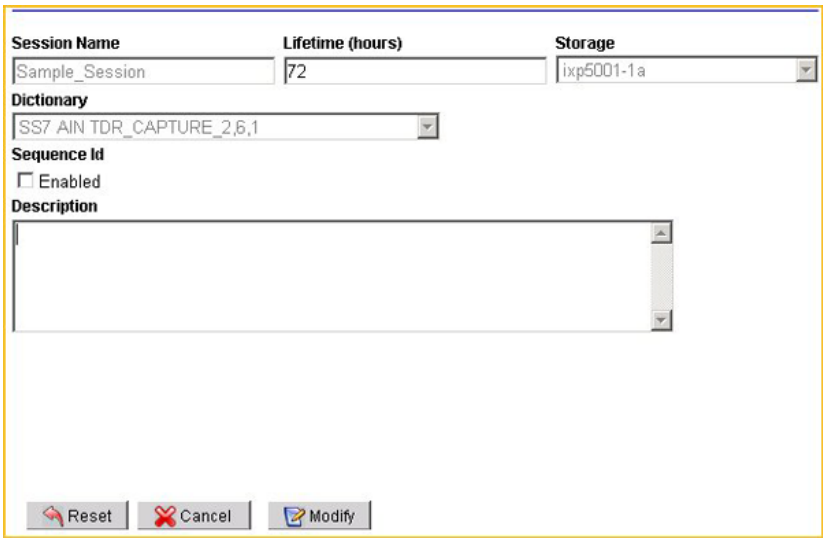


Figure 268: Modify Session Screen

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 cannot 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 *user-id* and *password* (password@db_stirng).
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.

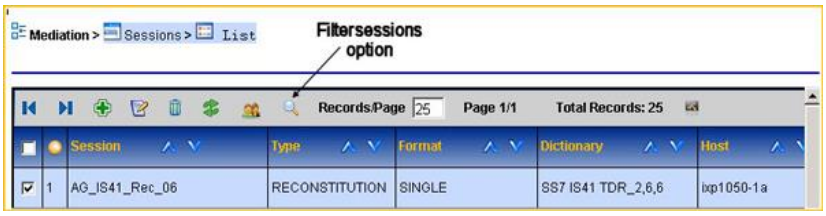


Figure 269: Xdr Session Filter Icon

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 270: 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.

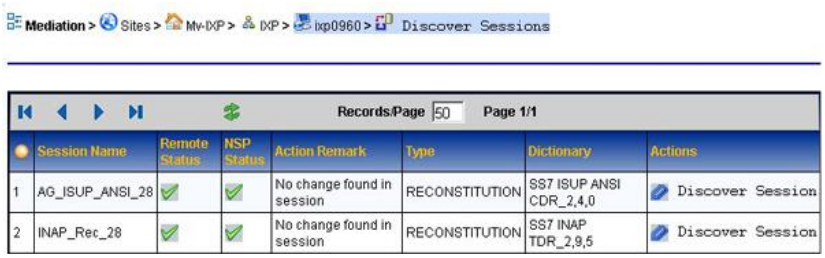


Figure 271: Sessions List

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**.

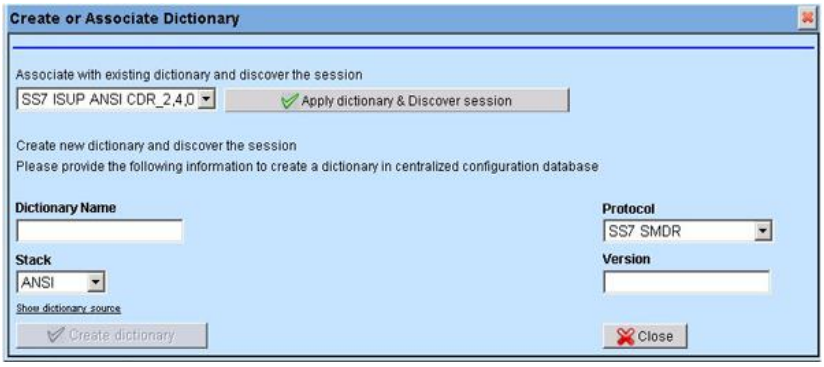


Figure 272: Associate Dictionary Screen

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 a Subsystem (Synchronizing)".

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.

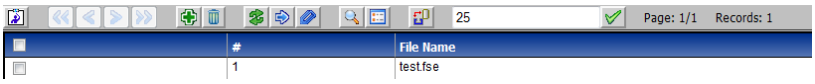


Figure 273: Enrichment Files List Screen

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.

Figure 274: 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.

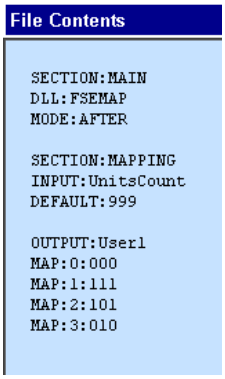


Figure 275: Source Code Screen

4. Click **Close** to close the screen.

Defining Enrichment file automated update

Complete these steps to define enrichment file automated update SFTP location:

1. Select **Mediation > Enrichment Files**.
   The *Enrichment Files List* screen opens
2. Click on automated update button in list toolbar .
   The *FSE Auto Update Configuration* screen opens.

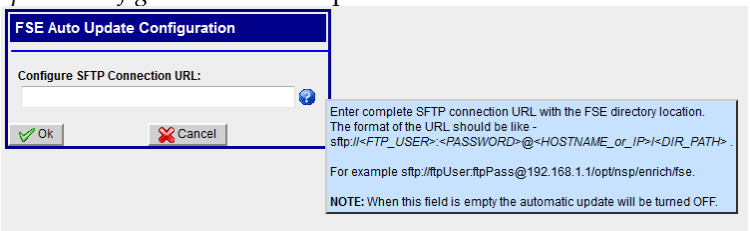


Figure 276: FSE automated update configuration screen

This settings refer to an SFTP location where system can find Enrichment FSE file.
URL should be like sftp://<USER>:<PASSWORD>@<HOSTNAME_OR_IP>/<PATH> where

- <USER> is username of SFTP server
- <PASSWORD> is password of SFTP user
- <HOSTNAME_OR_IP> is address of SFTP server
- <PATH> is relative path under user home folder in SFTP server

Note: Empty string turns off automated update

NSP scan regurlarly this folder and its subfolder (every 30 mn) to find files with same name as the those declared. In this case it loads file to replace exsiting FSE and reapply it automatically to selected session.

3. Click **OK** to validate changes.

Note: See Appendix F for typical FSE enrichment file

Chapter 10: Monitoring Policies

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 policies 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).

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 Checkbox 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 PMF sends FULL control plane and FULL user plane packets for the selected on-demand users.
GTP-C-TCs	• 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	• 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

TABLE 104: ADD POLICIES SCREEN FIELD DESCRIPTIONS

3. Enter the **Name** of the policy.
4. (Optional) Enter a **Description**.
5. If the policy is to be *On Demand*, select **Yes**.
6. If the policy is to have *Sampling* capabilities, select **Yes**.
7. If the policy is to have *Forward Statistics* capabilities, select **Yes**.
8. (Optional) Select **GTP-C-TCs** that will be associated with the Policy.
9. (Optional) Select **GTP-U-TCs** that will be associated with the Policy.
10. Click **Add** to add the Policy to the system.

Modifying a Monitoring Policy

Complete the following steps to modify a monitoring policy:

1. Select **Monitoring Policies > 3G Policies**.
2. Select the **Policy** to be modified from the *Policy* (top) table.
3. Click **Modify** from the tool bar.
4. Modify the **appropriate values**.

5. Click **Modify**.
   The database is updated with the change.

Deleting a Monitoring Policy

Complete these steps to delete a monitoring policy:

1. Select **Monitoring Policies > 3G Policies**.
2. Select the **Policy** to be deleted
3. Click **Delete**.
4. 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 policies 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 selected 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

Provisioning Guide for Configuring a PIC System

This outline represents the main steps in configuring a PIC system using CCM.

Creating sites (see Sites)

- Discover Legacy subsystems and create destinations if traffic needs to be routed to them.
- Discover xMF subsystem (see About xDR Filters and Adding a PMF Subsystem to a Site).
- Discover IXP subsystem (see Site Creation and Discovery Process).
- Discover DWH subsystems (if external DWH is present or else DWH gets discovered as a part of IXP) see Site Creation and Discovery Process.

Discovering or manually configuring (for PMF) Network Elements (see Adding a PMF Subsystem to a Site and Modifying a PMF Subsystem Host)

Configure Network Views (see Network View Configuration)

Configure xMF Subsystem (see xMF Acquisition)
If configuring an IMF Subsystem:

- Assign Linksets for Monitoring Groups (see About Monitoring Groups (IMF)).
- Assign Linksets to Network Views (see Adding an SS7 Linkset to a Link View).
- Create Dataflows (see About PDU Dataflows).
- Assign Linksets to Dataflows.
- Route Dataflows to Input Streams on IXP*/Legacy systems.
- Create and configure Associations (IMF or PMF).

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 see About Subsystem Preferences.

Setting up PIC Sites

This procedure must be followed by users who are setting up the PIC System for the first time, adding new PIC Servers or adding new applications on an existing Server.

Complete these steps (and refer to sections for detailed information), for setting up a PIC 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 an IMF subsystem (see Adding an IMF Subsystem to a Site).
4. Add a PMF subsystem (see Adding a PMF Subsystem to a Site).

SS7 Data Acquisition Using IMF

Complete these steps when adding an IMF Subsystem:

1. Create a Site, Hosts and Applications (see Setting up PIC Sites).
2. Ensure the Eagle is set up to communicate with the IMF (see About xDR Filters).
3. Discover the Network Elements from the IMF subsystem.
   At the end of this operation, a list showing the discovered Network Elements is displayed. You can also view the Network Elements from either the Home screen (see Network Elements) or from Network Elements Object Tree Perspective.
4. Distribute the discovered linksets to the IMF Applications that are part of the Subsystem by assigning selected linksets to each IMF Application.

   Care must be taken to ensure that traffic is distributed evenly across the available IMF servers. A common practice is to assign one of the Servers as a spare server and not assign any linksets to it.

   When one of the active IMF Servers fails, the linksets monitored by the failed server are automatically switched over to the spare Server.

   Note: Repeat steps 3-4 whenever new linksets have been added to IMF.

SS7 Data Acquisition Using PMF

Complete these steps to set up PMF monitoring of an SS7 link:

1. If this is a new PMF subsystem, (see Setting up PIC Sites) for setting up the site, hosts and applications.
2. Create a node for each end of the link to be monitored, if not already created, (see About Nodes).
3. Create a SS7 signaling point, if it does not already exist, under each node involved with the link to be monitored.
4. Create a linkset for the link to be monitored, if it does not't already exist.
   This can be done from either of the two signaling points (see Creating a Linkset).
5. Create the SS7 link to be monitored, if it does not't already exist.
6. Next, create or discover the PMF card that will do the monitoring under the PMF application if it does not already exist (see Modifying a PMF Subsystem Host).
   Ensure that the card has the correct firmware load, and set the card's attributes appropriately.
7. Select a port on the PMF card and activate it (see Adding IP Port PDU Filters).
   Set the port attributes appropriately.
8. Assign the link to the port (see Adding an SSN Filter).

GPRS Network Data Acquisition Using PMF

Complete these steps to set up PMF monitoring of a Gb link:

1. Create one node to contain the link's SGSN, if it doesn't already exist, (see Creating a Node).
2. Create a SGSN signaling point, if it doesn't already exist, under the node (see Creating and associating a Dictionary with a Session).
3. Create the Gb link to be monitored, if it doesn't already exist, (see Adding a Gb Link).
4. Select a port on the PMF card and activate it (see Adding a PMF Subsystem to a Site).
   Set the port attributes appropriately.
5. Assign the Gb link to one or more of the channels belonging to the port (see About Gb Links).

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 a PIC 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 IMF or PMF to ICP or IXP. When you assign links), linksets, or create IP Streams, the PDUs are collected by the IMF/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 linksets, 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 (for creating different types of Dataflows, see About Managing Dataflow Processings Manually):

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 (see About SS7 Q.752 Dataflows).

Routing PDUs to xDR Builders for SigTran

These steps are used to route PDUs from IMF or PMF to IXP. When you assign links, linksets , or create IP Streams, the PDUs are collected by the IMF/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 linksets, 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 a SigTran PDU filter that you need to classify PDUs as described in (see About PDU Filters).
4. Create a Traffic Classification (TC) and connect the filter to the TC, see Adding a Traffic Classification (PMF).
5. Create a PDU data flow process by specifying (for creating different types of dataflows, see About Managing Dataflow Processings Manually):
   a. The type of traffic.
   b. Optional filters.
6. Select the data flow you created and select the list route option (see About PDU Dataflows) or traffic classification.
   The system displays all the datasources where the PDUs are being collected and cached for that data flow.
7. Assign the routes by specifying one or more datasources for every data flow (see About SS7 Q.752 Dataflows).

Points to consider when creating Routes and Data Flows

- A given IXP input stream cannot receive PDUs coming from more than one IMF server. In addition, the current release of CCM only routes data on a subsystem basis. This may cause a problem if two IMF/PMF servers on a same subsystem are part of the same data flow. In this situation, you must create separate data flows for each IMF/PMF within a subsystem.
- xDR builders cannot handle PDUs that they cannot recognize. For example, if you route ISUP traffic to the LIDB builder, it will fail. Therefore, configure appropriate filtering using the PDU filters.
- An xDR builder running on an IXP can only handle a limited amount of traffic. To distribute the processing across multiple IXP servers, you must apply PDU filtering in order to split the traffic. While configuring such a splitting operation, make sure that the IXP can still correlate the PDUs. For example, you cannot split the ISUP traffic in a such a way that the IAM and the ACM for the same call go to different builders. A number of PDU filters are available to split the traffic properly, and you can use combination filters and raw filters (SS7 only) to design the flows.
- For SS7 networks, RID groups are created and assigned to linksets in order to handle duplicate PDUs. In this situation, while configuring the MSU dataflows, check the option to send the RID ID to the xDR generator.

Associating Sessions for Link-based Network Views

Since CCM does not configure the xDR generation process, it does not have the information about what link-based network views feed into which xDR sessions. Some applications like *ProTrace* need this information for link-based monitoring and protocol analysis. CCM provides a way to configure the relationship between Datasources and xDR sessions. Once this information is in the database, applications can find the link-based networks views feeding a given xDR session.

Note: This step is optional and is only required if you need to use link-based monitoring and protocol analysis which are needed for applications like ProTrace.

1. Follow the procedure for routing PDUs to IXP (see Adding a Protocol-Specific xDR Session).
2. Configure the IXP to generate and store XDR Records based on the PDUs.
3. Using CCM, select the Datasources described in Creating a Dictionary.
4. Assign one or more xDR Sessions to the Datasources described in Creating a Dictionary. Check that the information matches the actual xDR builder configuration. Otherwise, applications may not output proper information.
5. Repeat steps 1-5 when there have been changes in PDU Dataflows, routing and xDR Session configurations.

Configuring Q.752 Processing

All Q.752 data flows are configured using the Q.752 data flow assistant. Each data flow is configured for each subsystem.

Alarm Configuration

Alarms generated by various IMF and PMF modules can be globally enabled or disabled from CCM. The alarms can be categorized. Follow these guidelines when configuring alarms.

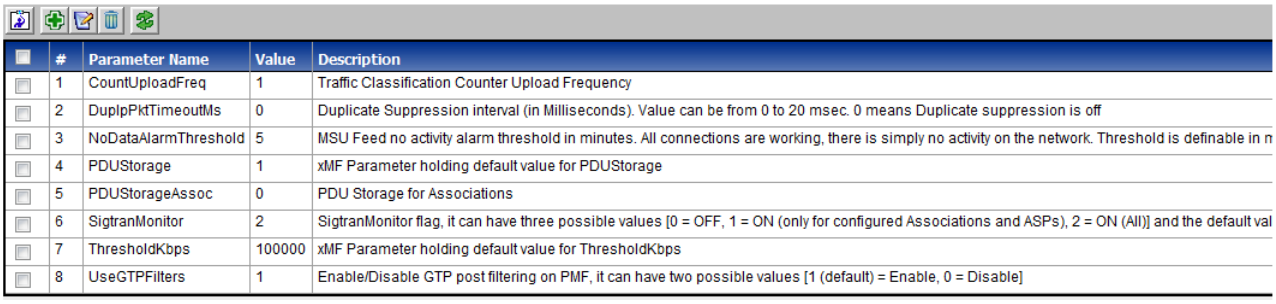
1. Enable or disable individual alarms originating from the monitored Eagles (see About SS7 OAM Alarms).
2. Enable or disable individual alarms originating from the IMF and PMF servers (see About SS7 OAM Alarms).
3. Follow the procedure described in Managing SLOR Thresholds to enable or disable individual Q.752-related alarms and set related alarm thresholds.

Duplicate IP Packet Suppression Configuration

The duplicate IP packet suppression feature works on the suppression interval, the packet is suppressed if the same packet is received within the suppression interval. This interval "DupIpPktTimeoutMs" is configured from the CCM per acquisition system. The duplicate packets are suppressed per traffic classification, the user can enable/disable the Duplicate IP Packet suppression by selecting "Duplicate Suppression".

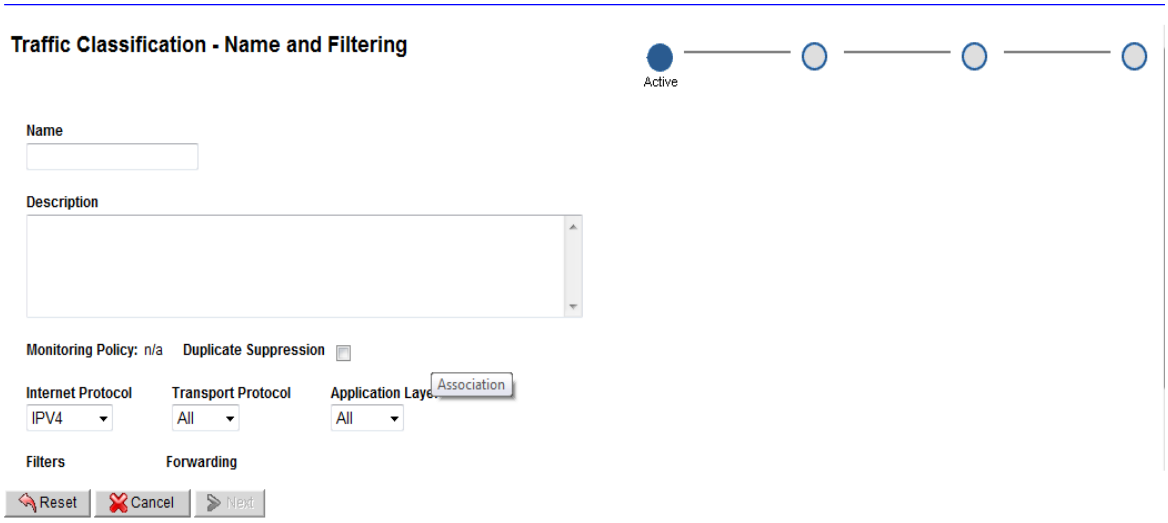
The Duplicate IP Packet Suppression can be configured as follows:

1. Modify the DupIpPktTimeoutMs in Settings on Acquisition sub-system level. The value can be configured between 0 to 20 ms, with 1ms interval. 0 means suppression off.



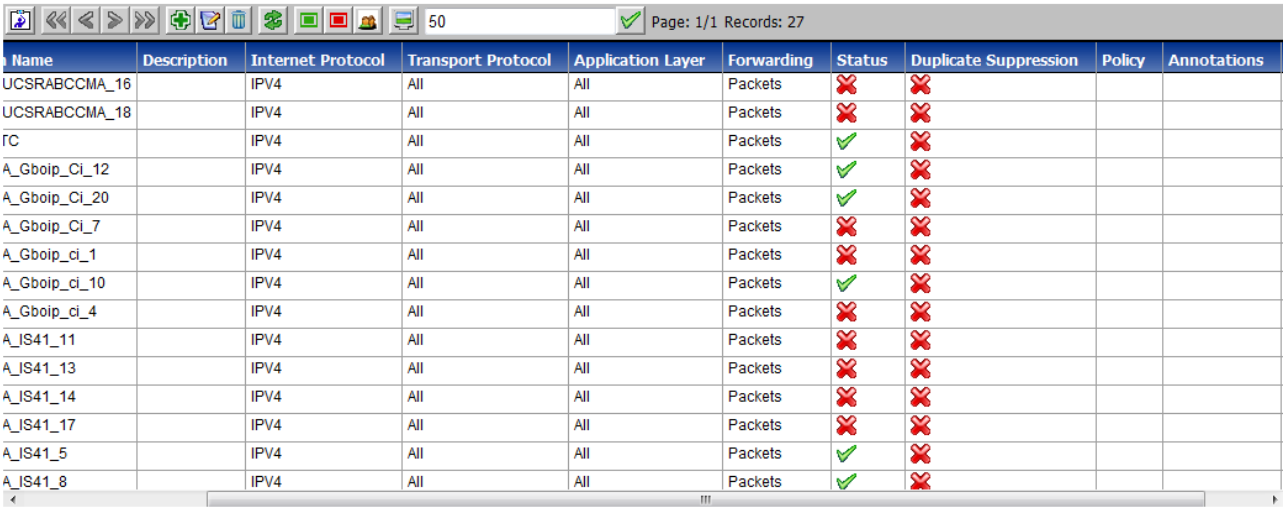
#	Parameter Name	Value	Description
1	CountUploadFreq	1	Traffic Classification Counter Upload Frequency
2	DupIpPktTimeoutMs	0	Duplicate Suppression interval (in Milliseconds). Value can be from 0 to 20 msec. 0 means Duplicate suppression is off
3	NoDataAlarmThreshold	5	MSU Feed no activity alarm threshold in minutes. All connections are working, there is simply no activity on the network. Threshold is definable in n
4	PDUStorage	1	xMF Parameter holding default value for PDUStorage
5	PDUStorageAssoc	0	PDU Storage for Associations
6	SigtranMonitor	2	SigtranMonitor flag, it can have three possible values [0 = OFF, 1 = ON (only for configured Associations and ASPs), 2 = ON (All)] and the default val
7	ThresholdKbps	100000	xMF Parameter holding default value for ThresholdKbps
8	UseGTPFilters	1	Enable/Disable GTP post filtering on PMF, it can have two possible values [1 (default) = Enable, 0 = Disable]

2. Enable the "Duplicate Suppression" while creating the TC. If this is not selected then no duplicate packets will be suppressed for that TC.



Activate/Deactivate Duplicate IP Pkt Suppression

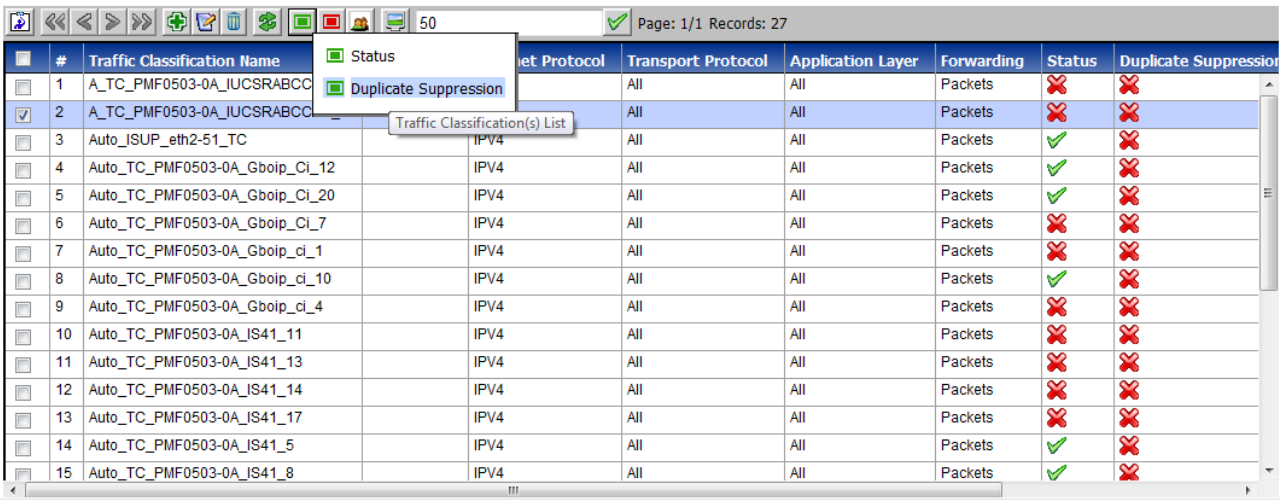
The feature can be activated or deactivated for the traffic classification. This can be done from the Traffic Classification listing screen.



Name	Description	Internet Protocol	Transport Protocol	Application Layer	Forwarding	Status	Duplicate Suppression	Policy	Annotations
UCSRABCCMA_16		IPV4	All	All	Packets	✗	✗		
UCSRABCCMA_18		IPV4	All	All	Packets	✗	✗		
ГС		IPV4	All	All	Packets	✓	✗		
A_Gboip_Ci_12		IPV4	All	All	Packets	✓	✗		
A_Gboip_Ci_20		IPV4	All	All	Packets	✓	✗		
A_Gboip_Ci_7		IPV4	All	All	Packets	✗	✗		
A_Gboip_ci_1		IPV4	All	All	Packets	✗	✗		
A_Gboip_ci_10		IPV4	All	All	Packets	✓	✗		
A_Gboip_ci_4		IPV4	All	All	Packets	✗	✗		
A_IS41_11		IPV4	All	All	Packets	✗	✗		
A_IS41_13		IPV4	All	All	Packets	✗	✗		
A_IS41_14		IPV4	All	All	Packets	✗	✗		
A_IS41_17		IPV4	All	All	Packets	✗	✗		
A_IS41_5		IPV4	All	All	Packets	✓	✗		
A_IS41_8		IPV4	All	All	Packets	✓	✗		

Activate

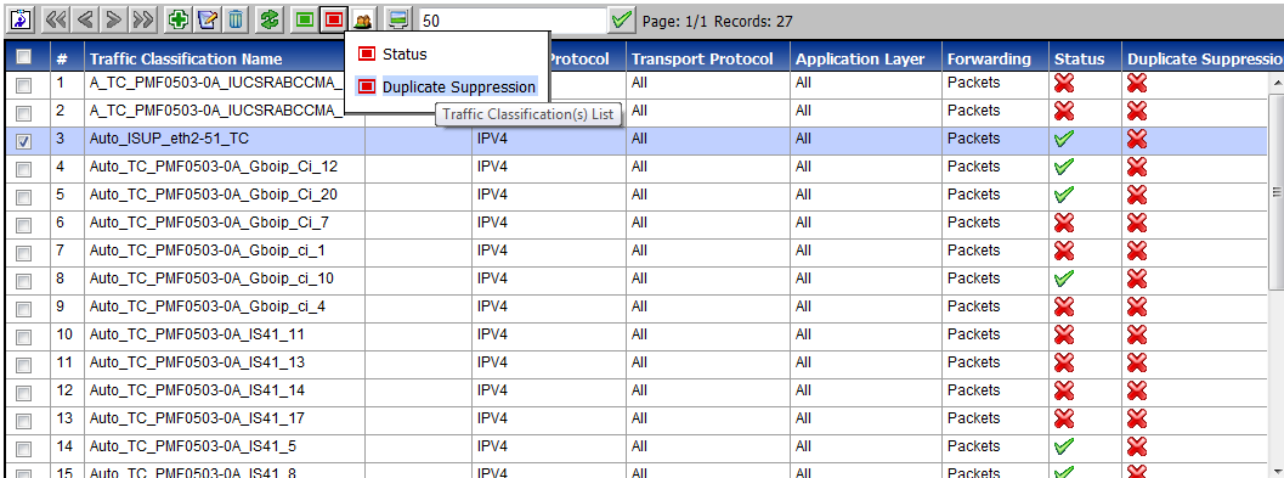
1. Select the TC and click on "Activate" button.
2. Select "Duplicate Suppression" to activate duplicate packet suppression for the TC.



#	Traffic Classification Name	Protocol	Transport Protocol	Application Layer	Forwarding	Status	Duplicate Suppressior
1	A_TC_PMF0503-0A_IUCSRABCC		All	All	Packets	✗	✗
2	A_TC_PMF0503-0A_IUCSRABCC_		All	All	Packets	✗	✗
3	Auto_ISUP_eth2-51_TC	IPV4	All	All	Packets	✓	✗
4	Auto_TC_PMF0503-0A_Gboip_Ci_12	IPV4	All	All	Packets	✓	✗
5	Auto_TC_PMF0503-0A_Gboip_Ci_20	IPV4	All	All	Packets	✓	✗
6	Auto_TC_PMF0503-0A_Gboip_Ci_7	IPV4	All	All	Packets	✗	✗
7	Auto_TC_PMF0503-0A_Gboip_ci_1	IPV4	All	All	Packets	✗	✗
8	Auto_TC_PMF0503-0A_Gboip_ci_10	IPV4	All	All	Packets	✓	✗
9	Auto_TC_PMF0503-0A_Gboip_ci_4	IPV4	All	All	Packets	✗	✗
10	Auto_TC_PMF0503-0A_IS41_11	IPV4	All	All	Packets	✗	✗
11	Auto_TC_PMF0503-0A_IS41_13	IPV4	All	All	Packets	✗	✗
12	Auto_TC_PMF0503-0A_IS41_14	IPV4	All	All	Packets	✗	✗
13	Auto_TC_PMF0503-0A_IS41_17	IPV4	All	All	Packets	✗	✗
14	Auto_TC_PMF0503-0A_IS41_5	IPV4	All	All	Packets	✓	✗
15	Auto_TC_PMF0503-0A_IS41_8	IPV4	All	All	Packets	✓	✗

Deactivate

1. Select the TC and click on "DeActivate" button.
2. Select "Duplicate Suppression" to deactivate duplicate packet suppression for the TC.



#	Traffic Classification Name	Protocol	Transport Protocol	Application Layer	Forwarding	Status	Duplicate Suppressio
1	A_TC_PMF0503-0A_IUCSRABCCMA_		All	All	Packets	✗	✗
2	A_TC_PMF0503-0A_IUCSRABCCMA_		All	All	Packets	✗	✗
3	Auto_ISUP_eth2-51_TC	IPV4	All	All	Packets	✓	✗
4	Auto_TC_PMF0503-0A_Gboip_Ci_12	IPV4	All	All	Packets	✓	✗
5	Auto_TC_PMF0503-0A_Gboip_Ci_20	IPV4	All	All	Packets	✓	✗
6	Auto_TC_PMF0503-0A_Gboip_Ci_7	IPV4	All	All	Packets	✗	✗
7	Auto_TC_PMF0503-0A_Gboip_ci_1	IPV4	All	All	Packets	✗	✗
8	Auto_TC_PMF0503-0A_Gboip_ci_10	IPV4	All	All	Packets	✓	✗
9	Auto_TC_PMF0503-0A_Gboip_ci_4	IPV4	All	All	Packets	✗	✗
10	Auto_TC_PMF0503-0A_IS41_11	IPV4	All	All	Packets	✗	✗
11	Auto_TC_PMF0503-0A_IS41_13	IPV4	All	All	Packets	✗	✗
12	Auto_TC_PMF0503-0A_IS41_14	IPV4	All	All	Packets	✗	✗
13	Auto_TC_PMF0503-0A_IS41_17	IPV4	All	All	Packets	✗	✗
14	Auto_TC_PMF0503-0A_IS41_5	IPV4	All	All	Packets	✓	✗
15	Auto_TC_PMF0503-0A_IS41_8	IPV4	All	All	Packets	✓	✗

Appendix B: xDR Builder Parameters

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

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)	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. 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. 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).
Garbage period (s)	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.
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.
Defaults button	Click this button to reset the screen to default values.

TABLE 105: INITIAL STEP SCREEN

IP Transport 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)	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. This parameter is displayed only if "reconstitution" is part of the xDR builder name. It

Field	Description
	is used only if the garbage period is different from 0. 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).
Garbage period (s)	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.
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	Select this parameter is you want to determine the Way and set inactivity garbage. In this format: Protocol Name [Ports] (Max inactivity in seconds)
Run IP reassemble function	Select this if you want to run reassemble function. Default is selected.
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.

TABLE 106: INITIAL STEP SCREEN

SS7 SCCP Parameters

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)	Defines (in seconds) the maximal accepted duration of a transaction (or communication). When a transaction duration exceeds this value, an xDR is generated

Field	Description
	(with "timer expiry" or "long call" status), even if the transaction is not really terminated. 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. 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).
Garbage period (s)	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.
Monitored	This check box indicates if the builder is being monitored or not. This check box cannot be selected in this screen.
Specific Parameters	
RANAP Routing: Listed Point Codes to Include or Exclude	Pull-down list to select if point codes are: Excluded Included
Filter = Accept source SSN to sink SSN	Enables you to add an source SSN. To add an item, click **plus** and select the source SSN and sink SSN from the pull-down lists
Period of flow trace displaying (s)	Numerical field to set the period of flow trace displays. Default is 0.
Definition of INAP interfaces = Source SSN to sink SSN for INAP protocol	Similar to the Filter = *Accept source* SSN *to sink* SSN field.
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.
SCCP Format	Pull-down list for selecting the SCCP format can be either: ANSI (default) ITU
RANAP Routing: List of Point Codes	Enter text in the alphanumeric field and add or remove point codes to list.
BSSAP Routing: Listed Point Codes to Include or Exclude	Can select to include or exclude listed point codes. (Default is excluded.)
BSSAP Routing: Priority on Point Codes or SSN (default)	Pull-down list to select either: SSN routing is priority rule (default) PC filtering is priority rule
Processed Segmentation	Select is segmentation is processed. Default is selected.
BSSAP Routing: List of Point Codes	Can add or remove routing point codes.
RANAP Routing: Priority on Point Codes or SSN (default)	Pull-down list to select either: SSN routing is priority rule (default) PC filtering is priority rule
Definition of MAP interfaces = Source SSN to sink SSN for MAP protocol	You can add source SSN and sink SSNs. You can remove selected maps by clicking **minus.**
Trace period	Select if there is to be a trace period. Default is not selected.

Field	Description
Analyze SSN	Select if you want to analyze SSNs. Default is selected.
Default button	Click this to return the screen to its default values.

TABLE 107: SS7 SCCP SCREEN

SS7 SUA Parameters

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)	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. 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. 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).
Garbage period (s)	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.
Monitored	This check box indicates if the builder is being monitored or not. This check box cannot be selected in this screen.
Specific parameters	
Period of flow trace displaying (s)	Numeric field to enter the time for displaying traces. Default is 0.
Filter = Accept source SSN to sink SSN	Enables you to add or remove source and sink SSNs.
Definition of INAP interfaces = Source SSN to sink SSN for INAP protocol	Enables you to add, modify or remove INAP source and sink SSNs for INAP protocols. Click **plus** to add a definition . Click **minus** to remove a definition. Select alternate source and sink SSNs to modify a definition.
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.
Trace period	Select if there is to be a trace period. Default is not selected.
Analyze SSN	Select if you want to analyze SSNs. Default is selected.
Definition of MAP interfaces = Source SSN to sink SSN for MAP protocol	Enables you to add, modify or remove MAP source and sink SSNs for MAP protocols. Click **plus** to add a definition . Click **minus** to remove a definition. Select alternate source and sink SSNs to modify a definition.
Defaults button	Click this to return screen to default values.

TABLE 108: SS7 SUA SCREEN

SS7 Transport Parameters

Field	Description
Generic Parameters	
No PDU timeout (s)	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. 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.

Field	Description
	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).
Max transaction duration (s)	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.
Garbage period (s)	This check box indicates if the builder is being monitored or not. This check box cannot be selected in this screen.
Monitored	Defines the duration (in seconds) beyond which an alarm is generated if no PDU has been detected.
Specific parameters	
Period of flow trace displaying(s)	Numerical field to set the period of flow trace displays. Default is 0.
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.
SIGTRAN MTP3 Point Code Format (ITU: 14 bits, ANSI: 24 bits)	Pull-down list enables you to select between ITU or ANSI. The default is ITU

TABLE 109: SS7 TRANSPORT SCREEN

Appendix C: About STC Copy and Fast Copy Effects on Monitoring Groups and Dataflows

There is an impact to Monitoring Groups and Dataflows when changing links from STC Copy to Fast Copy and the automatic configuring of the system via the xMF discovery process.

It is important to understand how to configure and manage Monitoring Groups and Dataflows when switching between STC Copy and Fast Copy.

Considerations When Working with STC/Fastcopy

The following is a list of points one should consider when working with the STC/Fastcopy feature:

- Existing STC links that are monitored remain in the same Monitoring Group.
- Monitored links which were part of an Association and are changed back to STC copy will remain in the same Monitoring Group if the linkset belongs to the same Monitoring Group.
- Monitored links that are part of an Association and are changed back to STC copy will switch to the same Monitoring Group as part of the linkset if the linkset belongs to a different Monitoring Group.
- Any un-monitored links which are part of an Association and are changed back to STC Copy will be added to the same Monitoring Group as the linkset.
- The Monitoring Group panel in CCM does not show Association as a possible selection to monitor if the Association no longer contains Fast Copy links. However, the linkset(s) will be available as a possible selection.
- Un-monitored links that switch from STC to an Association will be added to the same Monitoring Group as the Association if the Association is monitored.
- The Monitoring Group panel is CCM does not show a linkset as a possible selection if all the links in the linkset belong to Association(s). However, the Association(s) will be available as a possible selection.
- If a Monitoring Group no longer contains any links, then the Monitoring Group is automatically deleted.
- If a Dataflow no longer contains any links, then the Dataflow is automatically deleted.
- If the movement of linksets or Associations from one Monitoring Group to another results in removal of all routes in one or more Dataflows, then those Dataflows are deleted automatically. You will then need to create new or modify existing Dataflows in order to re-route the linksets or Associations.
- Dataflows may need to be modified or added in order to accommodate automatic Monitoring Group changes. The routes within the existing Dataflows may be removed automatically, but may need to be added manually by selecting the necessary linksets or Associations.
- The Dataflow Processings and streams will not be modified or removed automatically due to any automatic changes to Dataflows during the STC-FC switching, although you may need to manually modify or remove the Dataflow Processings later.
- Because Associations are included in the calculation of Monitoring Group capacity, it is possible for some of the links that changed from STC to FC to be monitored after the discovery process. For example, the Monitoring Group capacity for a linkset containing 3 M2PA Associations and 12 STC links would equate to 18. Therefore, it is highly recommended that after synchronizing the IMF that the Monitoring Groups, Dataflows and number of Streams should be verified of changes prior to applying changes to the IMF Subsystem. The verification also applies to the load balance on IMF based on Monitoring Groups, Dataflows, and Streams.
- Make sure that you **Apply Changes** in CCM when converting STC to Fast Copy or Fast Copy to STC because of the possibility of traffic loss during the Synchronization period up until you have applied all changes to the Subsystem (modifying or removing Dataflows and Monitoring Groups).

About STC Copy to Fast Copy Interactions

Monitoring Groups and Dataflows are affected when switching one or more links from STC Copy to Fast Copy and vice versa.

It is important to understand how to configure and manage Monitoring Groups and Dataflows when switching between STC Copy to Fast Copy.

Automatic Monitoring of Un-Monitored Links

In this scenario there are previously discovered network elements configured on the Eagle using STC Copy including two linksets belonging to the same Monitoring Group and a linkset that does not belong to a Monitoring Group. The configuration on the Eagle is changed the so that now both linksets contain the same M3UA Association containing several links.

Monitoring Groups Impacted **in this Scenario**

When the operator re-discovers the network elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored Links which are now part of an association will remain in same monitoring group.
- Un-Monitored inks which are now part of an Association will be added to the same monitoring group as the Association, and the Association is monitored automatically..
- The Monitoring Group panel in CCM longer shows a linkset as a possible selection if all the links in the linkset belong to Associations. However, the associations are available as a possible selection.

  Note: Because associations are included in the calculation for Monitoring Group capacity it is possible that some of the links that changed from STC Copy to Fast Copy to be un-Monitored.

The tables show the associations A1, A2, A3 and A4 are added to the configuration, the link L-13 remains in the same Monitoring Group (MG1) and the un-monitored links (L-21) are added to the same Monitoring Group (MG1). Link L-31 remains in the same Monitoring Group (MG1).

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	
LS2			
	L-21		
	L-22		
	L-23		
LS3			
	L-31	MG1	
	L-32		

TABLE 110: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			

Linkset	Link	Monitoring Group	Association
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	**A1**
LS2			
	L-21	MG1	**A1**
	L-22		
	L-23		
LS3			
	L-31	MG1	**A2, A3, A4**
	L-32		

TABLE 111: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

There is no impact to the SS7 Dataflows for this scenario.

Inter-monitoring Groups Link Transfer (M3UA)

In this scenario there were previously discovered Network Elements configured on the Eagle using STC including linksets that belong to different Monitoring Groups. The configuration on the Eagle was changed so that now the linkset contains an M3UA Association containing several links. Although this is a separate "Delete" and "Add" operation on the Eagle, it is possible that the operator failed to Synchronize after each operation.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the Network Elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored links which are part of an association remain in same Monitoring Group as the Association.
- Un-monitored links which are part of an Association will be added to the same Monitoring Group.
- The Monitoring Group panel in CCM will no longer show a linkset as a possible selection if all the links in the linkset belong to Associations. However, the Associations will be available as a possible selection.

The tables show the Associations A1, A3, A4 and A5 are added to the configuration and the additions of link L-21 is added to the same Monitoring Group MG1. Link L-31 remains in the same Monitoring Group MG2.

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	
LS2			

Linkset	Link	Monitoring Group	Association
	L-21	MG2	
	L-22	MG2	
	L-23	MG2	
LS3			
	L-31	MG2	A2
	L-32		

TABLE 112: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	**A1**
LS2			
	L-21	**MG1**	**A1**
	L-22	MG2	
	L-23	MG2	
LS3			
	L31	MG2	A2, **A3, A4, A5**
	L-32		

TABLE 113: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

There would not be any impact to the SS7 Dataflows for this example, but if LS2 initially contained only L-21 and if a dataflow was created only with LS2, then after the migration and the synchronization this Dataflow would be deleted as the route involving MG1 would be removed and the Dataflow would become empty.

Monitoring as Before (M3UA)

In this scenario there were previously discovered Network Elements configured on the Eagle using STC, including Linksets that belong to different Monitoring Groups. The configuration on the Eagle was changed so that now the Linksets contains M2PA Associations for several links.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the network elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored Links which are part of an Association will remain in same Monitoring Group.
- Un-Monitored Links which are part of an Association will remain un-monitored.
- The Monitoring Group panel in CCM will no longer show a Linkset as a possible selection if all the links in the Linkset belong to Associations. However, The Associations will be available as a possible selection.

The tables show the Associations A1 - A10 is added to the configuration and the links remain in the same Monitoring Group (MG1).

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	
LS2			
	L-21	MG2	
	L-22	MG2	
	L-23	MG2	
LS3			
	L-31	MG2	
	L-32	MG2	

TABLE 114: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	**A1**
	L-12	MG1	**A2**
	L-13	MG1	**A3**
LS2			
	L-21	MG2	**A4**
	L-22	MG2	**A5**
	L-23	MG2	**A6**
LS3			
	L31	MG2	**A7, A8, A9, A10**
	L32		

TABLE 115: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

There would not be any impact to the SS7 Dataflows for this user case.

Inter-monitoring Groups Link Transfer (M2PA)

In this scenario there were previously discovered Network Elements configured on the Eagle using Fast Copy including M2PA Associations that belong to a Monitoring Group. The configuration on the Eagle was changed so that now one of the links is switched to M3UA. Although this is a separate "Delete" and "Add" operation on the Eagle, it is possible that the operator failed to Synchronize after each operation.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the Network Elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored links which are part of an Association remain in same Monitoring Group when the linkset belongs to the same Monitoring Group.
- Monitored STC links will switch to the same Monitoring Group as the Association.
- Un-monitored links that are part of an association are added to the same Monitoring Group as the new Association.

The tables show the Link L-13 is moved to Association A3 and will be added to the same Monitoring Group (MG1).

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	A1
	L-12	MG1	A2
	L-13	MG1	
LS2			
	L-21	MG2	A3
	L-22	MG2	A5
	L-23	MG2	A6
LS3			
	L-31	MG2	A3
	L-32		

TABLE 116: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	**MG2**	**A3**
LS2			
	L-21	MG2	A3
	L-22	MG2	A5
	L-23	MG2	A6
LS3			
	L-31	MG2	A3
	L32		

TABLE 117: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

There would potentially be changes to the Dataflow for this scenario assuming the Linkset LS1 is part of an SS7 Dataflow. If the SS7 Dataflow does not contain any STC links after the re-discovery process, then the dataflow would not be removed.

About Fast Copy to STC Copy Interactions

When moving from Fast Copy back to STC Copy where the current IMF configuration has been previously discovered using Fast Copy, there are two scenarios that can occur when moving from Fast Copy to STC Copy.

Note: Associations will NOT be removed automatically; you will have to remove them manually in the Network Elements Perspective.

- Automatic Monitoring of Un-monitored Links (Linkset)
- Inter-monitoring Groups Link Transfer (Linkset)

Automatic Monitoring of Un-Monitored Links (Linkset)

In this scenario there are previously discovered network elements configured on the Eagle using Fast Copy including a linkset belonging to a Monitoring Group and a linkset that does not belong to a Monitoring Group. The configuration on the Eagle has changed the so that now both linksets are switched back to STC copy and no longer contain the M3UA Association.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the Network Elements from the IMF the following changes occur:

- Existing STC links that are monitored remain in the same Monitoring Group.
- Monitored Links which are now part of an Association will remain in same Monitoring Group.
- Any un-monitored links that are part of a linkset are added to the same Monitoring Group as the Association.
- The Monitoring Group panel in CCM no longer shows Association A1 as a possible Association to monitor.

The tables show that Associations A1, A2, A3 and A4 are remove from the configuration, the Link L13, L-21 and L-31 remain in the same Monitoring Group (MG1) and the Un-Monitored Links (L-22, L23 and L-32) are added to the same Monitoring Group (MG1).

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	**A1**
LS2			
	L-21	MG1	
	L-22		**A1**
	L-23		
LS3			

Linkset	Link	Monitoring Group	Association
	L-31	MG1	**A2, A3, A4**
	L-32		

TABLE 118: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	
LS2			
	L-21	MG1	
	L-22	**MG1**	
	L-23	**MG1**	
LS3			
	L-31	MG1	
	L-32	**MG1**	

TABLE 119: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

Potentially, there can be changes to the Dataflow for this scenario assuming that Association A1 is part of an IP Dataflow. If the IP Dataflow does not contain any Fast Copy links after the re-discovery process, then the Dataflow would be removed. That is, an IP Dataflow automatically is removed if, after discovery, all the Fast Copy Links belonging to the Dataflow are switched to STC Copy Links. An SS7 Dataflow may need to be modified or added to add STC links

Inter-monitoring Groups Link Transfer (Linkset)

In this scenario there are previously discovered Network Elements configured on the Eagle using Fast Copy including an Association belonging to a Monitoring Group and a linkset that belongs to a different Monitoring Group. The configuration on the Eagle has changed the so that now both linksets are switched back to STC copy and no longer contain the M3UA Association.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the Network Elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored links which were part of an Association remain in same Monitoring Group when the linkset belongs to the same Monitoring Group.
- Monitored links which were part of an Association will switch to the same Monitoring Group as the linkset when the linkset belongs to a different Monitoring Group.
- Any un-monitored links which were part of an Association will be added to the same Monitoring Group as the linkset.
- The Monitoring Group panel in CCM will no longer show Association A1 as a possible Association to monitor.

The tables show the Associations A1 and A2 are removed from the configuration, the link L13 will remain in the same Monitoring Group (MG1) and the Llnk L21 will switch to the Monitoring Group (MG2) that has linkset LS2. Link L-32 will be added to Monitoring Group (MG1) that has Linkset LS3.

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	**A1**
LS2			
	L-21	MG2	**A1**
	L-22	MG2	
	L-23	MG2	
LS3			
	L-31	MG1	**A2**
	L-32		

TABLE 120: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	MG1	
LS2			
	L-21	**MG2**	
	L-22	MG2	
	L-23	MG2	
LS3			
	L-31	MG1	
	L32	**MG2**	

TABLE 121: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

Potentially, there can be changes to the Dataflow for this scenario assuming that Association A1 is part of an IP Dataflow. If the IP Dataflow does not contain any Fast Copy links after the re-discovery process, then the Dataflow would be removed. That is, an IP Dataflow is automatically removed after discovery of all the Fast Copy Links belonging to the Dataflow are switched to STC Copy Links.

About Moving Fast Copy from M3UA to M2PA

When moving from Fast Copy from M3UA to M2PA and vice-versa there are two scenarios that can occur when changing Fast Copy Links. They are:

- Inter-monitoring Groups Link Transfer (M2PA to M3UA)
- Inter-monitoring Groups Link Transfer (M3UA)

Inter-monitoring Groups Link Transfer (M2PA to M3UA)

In this scenario there are previously discovered network elements configured on the Eagle using Fast Copy, including M2PA Associations belong to a Monitoring Group. The configuration on the Eagle has changed so that one of the Associations is switched to M3UA. Although this is a separate "delete" and "add" operation on the Eagle, it may be possible that the operation failed to Synchronize after each operation.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the Network Elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored links which were part of an Association remain in same Monitoring Group.
- Monitored links that are part of changed Association now belong to Monitoring Group of the Association.

The tables show the Association A4 is removed from the configuration; Link L-21 is moved to Association A3 and is added to the same Monitoring Group (MG1).

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	A1
	L-12	MG1	A2
	L-13	MG1	A3
LS2			
	L-21	MG2	A4
	L-22	MG2	A5
	L-23	MG2	A6
LS3			
	L-31	MG2	A4
	L-32		

TABLE 122: BEFORE

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	A1
	L-12	MG1	A2
	L-13	MG1	**A3**
LS2			
	L-21	**MG1**	**A3**
	L-22	MG2	A4
	L-23	MG2	A5

Linkset	Link	Monitoring Group	Association
LS3			
	L-31	MG2	A4
	L-32		

TABLE 123: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

Potentially, there are changes to the Dataflow for this scenario assuming that Association A4 is part of an IP Dataflow. If the IP Dataflow does not contain any Fast Copy links after the re-discovery process, then the Dataflow is removed. That is, an IP Dataflow is automatically removed if, after discovery, all the Fast Copy Links belonging to the Dataflow are switched to STC Copy Links.

Inter-monitoring Groups Link Transfer (M2PA)

In this scenario there were previously discovered Network Elements configured on the Eagle using Fast Copy including M2PA Associations that belong to a Monitoring Group. The configuration on the Eagle was changed so that now one of the links is switched to M3UA. Although this is a separate "Delete" and "Add" operation on the Eagle, it is possible that the operator failed to Synchronize after each operation.

Monitoring Groups Impacted in this Scenario

When the operator re-discovers the Network Elements from the IMF the following changes occur:

- Existing STC links that are monitored will remain in the same Monitoring Group.
- Monitored links which are part of an Association remain in same Monitoring Group when the linkset belongs to the same Monitoring Group.
- Monitored STC links will switch to the same Monitoring Group as the association.
- Un-monitored links that are part of an Association are added to the same Monitoring Group as the new Association.

The tables show the Link L-13 is moved to association A3 and will be added to the same Monitoring Group (MG1).

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	A1
	L-12	MG1	A2
	L-13	MG1	
LS2			
	L-21	MG2	A3
	L-22	MG2	A5
	L-23	MG2	A6
LS3			
	L-31	MG2	A3
	L-32		

TABLE 124: BEFORE

Linkset	Link	Monitoring Group	Association

Linkset	Link	Monitoring Group	Association
LS1			
	L-11	MG1	
	L-12	MG1	
	L-13	**MG2**	**A3**
LS2			
	L-21	MG2	A3
	L-22	MG2	A5
	L-23	MG2	A6
LS3			
	L-31	MG2	A3
	L-32		

TABLE 125: AFTER (IMPACTS BOLDED)

Dataflows Impacted in this Scenario

There would potentially be changes to the Dataflow for this scenario assuming the Linkset LS1 is part of an SS7 Dataflow. If the SS7 Dataflow does not contain any STC links after the re-discovery process, then the Dataflow would not be removed.

Appendix D: Defining and Modifying Flavor (PC Format) of Session at CCM

Define Flavor (PC Format) of Session

Flavor associated with session can be defined in CCM by one of following scenarios:

- Defining flavor while creating session through xDR Data Flow Assistant
- Defining flavor while adding session
- Defining flavor while defining store DFP

Defining flavor while creating session through xDR DataFlow Assistant

- Login to CCM application
- Go to Mediation->Sites->Site->IXP->Server->DataFlowProcessings
- Define DFP by selecting “xDR DataFlow Assistant” in right click menu.
- Wizard will also ask for flavor if underlying protocol has point code fields.

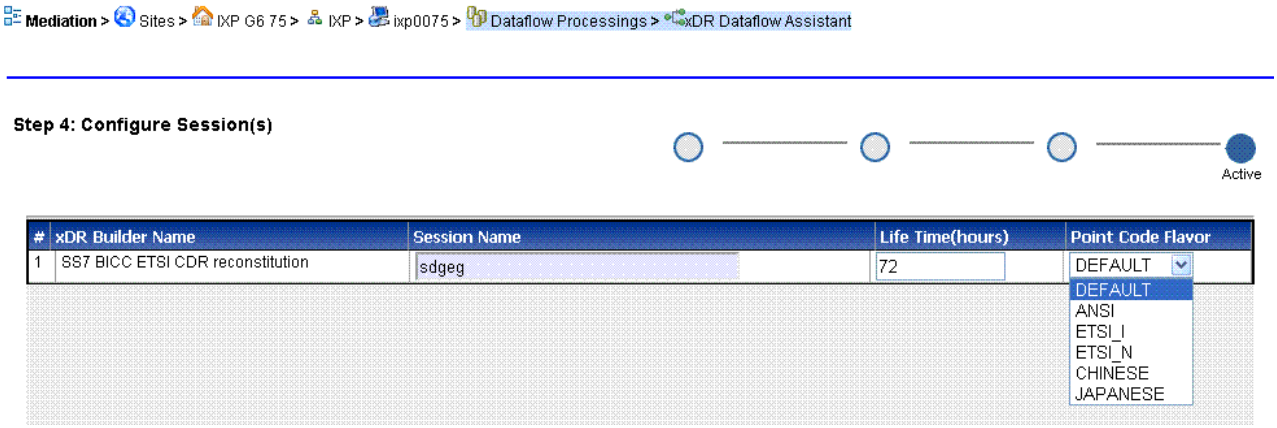


Figure 277: Associate flavor while creating session through xDR Data Flow Assistant

Defining flavor while adding Session through session list

- Login to CCM application
- Click on xDR Sessions. This will display of list of sessions
- Click on Add Button on toolbar.
- The wizard will ask for Point Code Flavor only when the dictionary has point code type field. In this case, select the flavor for the session from drop down.

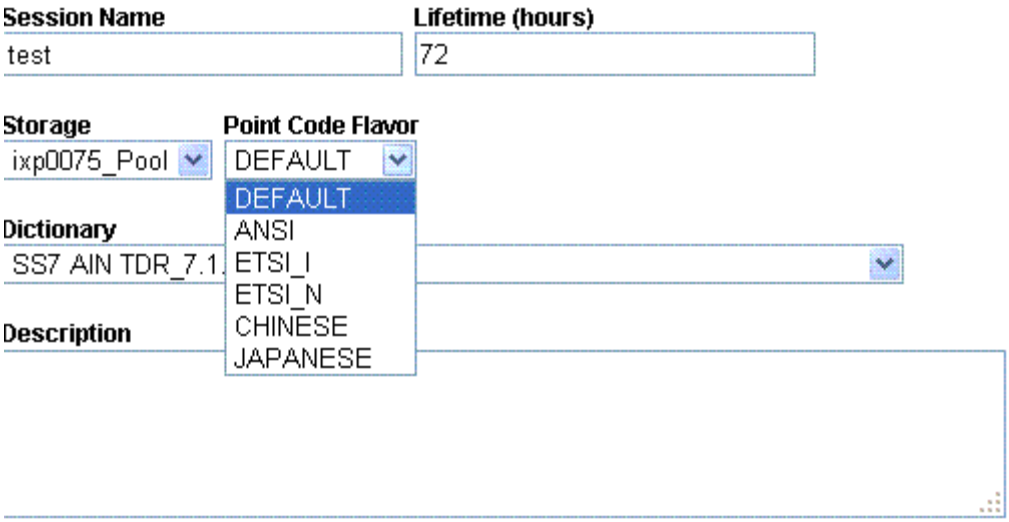


Figure 278: Associating flavor with Session

Defining flavor while defining store DFP

- Login to CCM application
- Go to Mediation->Sites->Site->IXP->Server->Data Flow Processings
- Select “Add” in right click menu and define store DFP
- Define flavor in wizard where it asks for create session

  Note: The flavor dropdown will come only if underlying protocol has point code fields.

Modifying flavor of a xDR Session

To modify PC Format of a session, follow the following steps

- Login to CCM application
- Click on xDR Sessions. This will display of list of sessions.
- Click on Modify Button on toolbar.
- Change the flavor for the session by selecting new flavor in drop down and Click OK.

Note: The flavor dropdown will come only if underlying protocol has point code fields.

Appendix E: xDR Filters during Protocol Upgrade

During Protocol Upgrade, if all the sessions based on a dictionary are not upgraded then the dictionary is considered as not completely upgraded. In this intermediate state when dictionary is not completely upgraded, there are some limitations on addition and modification of xDR filters as described below.

Adding xDR Filters

While adding an xDR filter if user selects a dictionary, which has been replaced (upgraded) by dictionary of different version then the creation of xDR filter is not allowed. An error is displayed to user mentioning that "The dictionary:<*Dictionary_Name*> has been upgraded. Filter creation using old dictionary is not allowed"

Note: Same behavior will be demonstrated if xDR filter is added while creating Dataflow Processing.

Modifying xDR Filters

While modifying an xDR filter if user selects a dictionary which is not completely upgraded then an error message is displayed to user mentioning "All Sessions are not upgraded for this dictionary. Please upgrade all sessions and then try again."

Appendix F: FSE enrichment file syntax

The first step in configuring an xDR Static Enrichment file is the naming process. Static enrichment files must begin with a dollar sign character ($) and have an extension of fse. The name of the enrichment file determines the processing order in the case of multiple files, as the data server processes the files in alphabetical order.

For example, a file with the name *$0addfile.fse* will process before a file with the name *$testfile.fse*.

A static enrichment file must contain three sections:

- Main
- Filter
- Mapping

All of your MAIN sections should look like the following:

```
SECTION:MAIN
VERSION:200
DLL:FSEMAP
MODE:BEFORE
```

It should be noted that each of your filter sections will be a little different, depending on the type and field that the enrichment is changing. The following sample should appear similar to your Filter section:

```
SECTION:FILTER
NAME:Not_International
EXPR:A
COND:A:BNumberNature:<>:International number
```

The mapping section will be different for each enrichment being done. Each file should reflect a different "INPUT" and "OUTPUT" field. The following is an example of a MAPPING section with sample data:

```
SECTION:MAPPING
INPUT:BNumber
OUTPUT:OCNB

MAP:201007:7229
MAP:201032:0138
MAP:201040:9206
MAP:201200:9206
MAP:201202:6630
```

The above statement specifies that for this particular enrichment, we will take the value from the column "BNumber", and if it matches a predefined value, populate a column called "OCNB" with the specified "new" value. In the example above, if the column "BNumber" is populated with a value of "201007", place a value of "7229" in the column called "OCNB".