What's New in IPI Reference Guide Version 7.13.2?

Software Version 7.13.2

Iris™

Iris Performance Intelligence Reference Guide

User Documentation

Tektronix communications

Tektronix Communications
3033 W President George Bush Highway
Plano, Texas 75075
+1 469-330-4000 (voice)
www.tekcomms.com Web site

uadocfeedback@tek.com (Technical Publications email)

Tektronix Communications, Inc. Proprietary Information
992-0422-08-001-140228

The products and specifications, configurations, and other technical information regarding the services described or referenced in this document are subject to change without notice. All statements, technical information, and recommendations contained in this document are believed to be accurate and reliable but are presented “as is” without warranty of any kind, express or implied. Users must take full responsibility for their application of any products specified in this document. Tektronix Communications, Inc. makes no implied warranties of merchantability or fitness for a purpose as a result of this document or the information described or referenced within, and all other warranties, express or implied, are excluded.

Except where otherwise indicated, the information contained in this document represents the planned capabilities and intended functionality offered by the product and version number identified on the front of this document. Screen images depicted in this document are representative and intended to serve as example images only. Wherever possible, actual screen images are included.

What's New in IPI Reference Guide Version 7.13.2?

The following table describes IPI Reference Guide 7.13.2 enhancements.

Feature ID	Description	Refer to:
F-02336	**Emergency Call Support and Service Filtering** All IPI workflows now include a Service options menu that enables you to filter by Full Network or a specific service, including the new Emergency Service.	■ IPI Services ■ IPI User Interface
F-02041	**IPI Dashboard Improvements** You can set IPI and IPI to open dashboards and drilled-to dashlets in a new browser tab or window or in the current window.	■ IPI User Preferences
F-02298	**Consistent Filter Support** With the new Dimension Type and Dimension Search filters, IPI advanced filtering now has consistent dimensional filtering capability across all workflows except FastPath.	■ IPI User Interface

About the Iris Performance Intelligence User Guide

What Is in this Guide

This guide contains information necessary for using the Iris Performance Intelligence (IPI) assurance tool and covers the following topics:

- IPI Services
- Key Performance Indicators / Key Quality Indicators
- Proactive Network Analysis
- Proactive Group Analysis
- Proactive Element Analysis
- Failed CDR Log
- Cause Code Analysis
- FastPath
- Historical Reports (Management and Query Reports)
- Alarms Policy Management
- IPI Best Practices

TYPOGRAPHIC CONVENTIONS

The Iris Performance Intelligence User Guide incorporates standard Microsoft Windows conventions and functionality. For more information about working in a Microsoft Windows environment, refer to your operating system documentation. The following table describes typographic conventions that this guide uses throughout this book.

Convention	Description
>**initAdminConfig**	This convention indicates Bold Courier text that represents a command or script when a procedure consists of entering DOS or UNIX commands and scripts.
Courier font	This convention indicates Courier text that represents a system message, prompt, or information that must be typed exactly as shown, including program code.
Italic type	This convention indicates a Bold Italic typeface that represents a document title.
System	This convention indicates Blue text that represents a cross-reference to a section that relates to the topic in the current section. By clicking the Blue text, the related section appears.

MESSAGE FORMATS

The following table describes the message formats that the Iris system uses throughout this guide.

Message Format	Description
 *The **Pass/Block** option functions like the **Yes/No** option.*	Notes contain information that is supplemental to the main topic of the section in which you find it, such as an explanation, tip, comment, or other useful but not imperative information.
 Log out of the program before turning off the power to avoid corrupting your data.	Cautions are notes that are used to advise you that failure to take or avoid a specified action could result in loss of data or damage to files.

How This Guide is Organized

Beyond this introductory section, this guide is divided into several sections. The section organization suggests a best practice approach for working with the IPI application. Although the guide is set up in this sequence, you can read it in any order and refer to sections as needed. Following is a brief description of the topics covered in each section.

Chapter 1, Iris Performance Intelligence Overview
This chapter provides background information on IPI and an overview of FastPath, Proactive Network Analysis, Proactive Group Analysis, CDR Direct Access, Policy Management, Historical Reporting, and IPI KPIs.

Chapter 2, IPI Best Practices
This chapter provides several use cases for IPI in both FastPath and Proactive Network Analysis dashboards.

Iris Documentation

Online Documentation is provided for the Iris solution hardware and software. The documentation covers all information necessary for the operation and maintenance of the applications within this solution. Tektronix Communications may elect to rearrange the contents of the Iris solution documentation, as appropriate, to improve document usability. Documentation is provided in English and is delivered at the time Tektronix Communications deploys the Iris applications.

Related information is available in the following documents:

- ***Iris G10 Installation Guide***—contains installation instructions for the GeoProbe G10 probe.
- ***Iris G10 Media Probe Installation Guide***—contains installation instructions for the GeoProbe G10 Media probe.
- ***Iris G10 LTE Control Plane Probe Installation Guide***—contains installation instructions for the GeoProbe G10 LTE Control Plane probe.
- ***Iris G10 Hardware Maintenance Guide***—contains hardware reference information about GeoProbe G10.
- ***Iris Getting Started Guide***—contains an introduction to the Iris solution and applications and information to help the user get started with the Iris software.
- ***Iris Admin Online Help and PDF Guide***—contains instructions for the Iris system administrator on managing applications, topology, XDR profiles, G10 probes, software, system, and licenses.
- ***Automated Controller Engine (ACE) User Guide***—contains information for configuring the ACE application and for managing ACE policies.
- ***Iris Online Help—***contains procedures, tutorials, use cases, and GUI descriptions for the Iris applications and IrisView framework.

Additional IPI Documentation

The following documents are available in the Online Help for download as individual PDF files. These are not included in the IPI Reference Guide.

- **Iris User Privileges**—describes the privileges needed to access IPI and Alarm features.
- **IPI Interfaces and Protocols**—describes the interfaces and protocols supporting LTE, VoIP/IMS, and 2G/3G networks.
- **IPI Key Performance Indicators**—contains a list of KPIs supported by IPI, including interfaces, protocols, dimensions, node types, and QoS parameters supported.
- **Bin Count Calculation**—contains the Bin count calculations used for IPI KPIs and the MOS score for Bin counts.
- **IPI Management Reports**—describes all the predefined Management Reports supported by IPI, including dimensions and QoS parameters.
- **IPI Query Reports**—describes all the IPI KPIs and dimensions available for generating Query Reports.

IPI KPI White Papers

Table 1 lists available white papers for IPI KPIs. To obtain a copy of a white paper, contact Tektronix Communications Customer Support.

Table 1 - Available IPI KPI White Papers

Network	KPI Summary	White Papers	Comments
Fixed Voice and IMS	▪ Voice Signaling ▪ Voice Media ▪ Voice Session ▪ Voice Call QoS	▪ IPI SS7 KPI Algorithms	Describes the KPI algorithms for the following SS7 protocols: ▪ ISUP ▪ BICC ▪ GSM MAP ▪ CAMEL

Table 1 - Available IPI KPI White Papers (Continued)

Network	KPI Summary	White Papers	Comments
Fixed Voice and IMS	▪ Voice Signaling ▪ Voice Media ▪ Voice Session ▪ Voice Call QoS	▪ IPI Voice Signaling KPI Algorithms	Describes the Signaling KPI algorithms for the following signaling protocols: ▪ SIP ▪ H.248 ▪ H.323 ▪ MGCP ▪ Diameter ▪ DNS ▪ ENUM ▪ BICC ▪ GSM MAP ▪ CAMEL ▪ RTSP
		▪ IPI Media KPI Algorithms	Describes the KPI algorithms for the following media protocols: ▪ SIP/SIP EoCQ ▪ H.248 ▪ RTP ▪ RTCP ▪ RTCP-XR ▪ MGCP
		▪ IPI Sonus MCS and Diameter+ KPI Algorithm	Describes the KPI algorithms for VoIP Sonus MCS Diameter+ for IPI.
Mobile LTE Voice	▪ Voice Signaling ▪ Voice Media ▪ Voice Session	▪ IPI LTE KPI Algorithms ▪ IPI Voice Signaling KPI Algorithms ▪ IPI Media KPI Algorithms	Describes the KPI algorithms for VoLTE.

Table 1 - Available IPI KPI White Papers (Continued)

Network	KPI Summary	White Papers	Comments
Mobile LTE Data	▪ Data User and Control Plane KPIs	▪ IPI LTE KPI Algorithms	
Mobile 2G/3G Data	▪ User Plane KPIs ▪ Data KPIs for Gn, Gb, and IuPS	▪ IPI Gn/Gi KPI Algorithms	
		▪ IPI IuPS KPI Algorithm	
		▪ IPI Gb KPI Algorithm	
Mobile 2G/3G Voice	▪ Voice KPIs for IuCS and Aif	▪ IPI IuCS KPI Algorithm	
		▪ IPI A interface KPI Algorithm	

Online Help

The IrisView framework provides user assistance via online help. The help system opens in a local Web browser that is launched from the application software (see **Figure 1**). Browser requirements are the same as for the Iris clients.

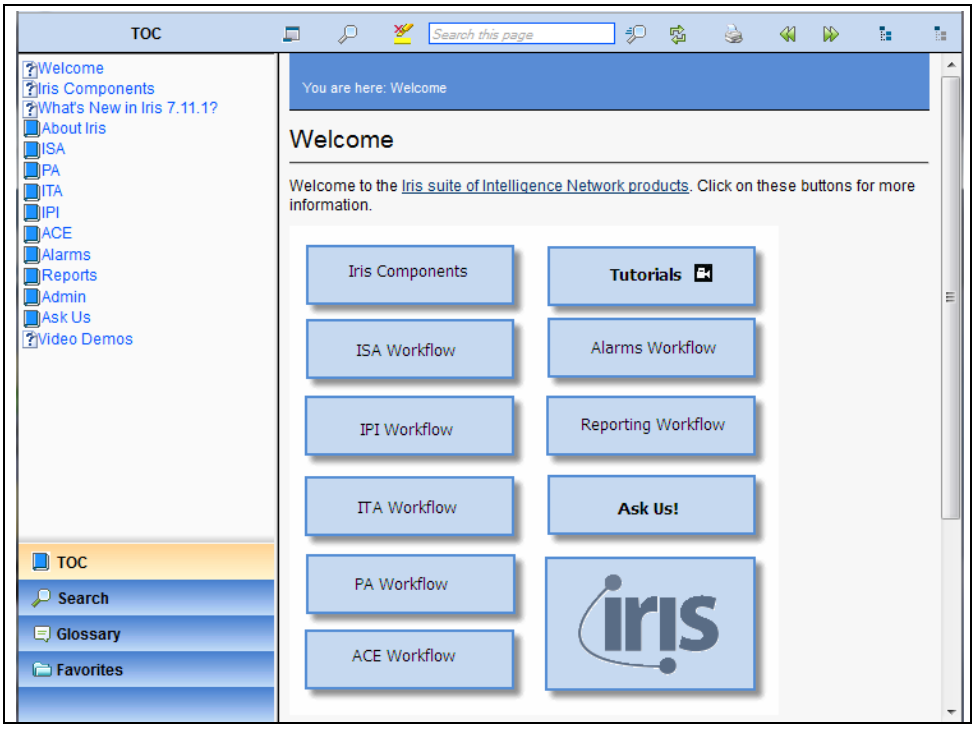

Figure 1 - Iris Online Help Window Example

The IrisView online help contains procedures, tutorials, and GUI descriptions for the Iris Analyzer applications (ISA, ITA, and PA), Iris Assurance (IPI and ACE), Alarms, Historical Reporting, and IrisView framework. It also includes the following features:

- A table of contents spanning the entire help system
- A search engine enabling use of Boolean expressions in advanced searches, use of application-specific search filters, and the ability to search only the current page
- A glossary that includes acronym expansions and term definitions
- A Favorites feature, similar to Internet favorites, where you can save links to favorite topics and search expressions
- Complete description of user interface and task-based procedures
- Detailed use cases
- Multimedia tutorials that guide you step-by-step through application workflows

Separate online help applications for Operations, Administration, and Maintenance (OAM) and Unified User Management System (UUMS) are available for system administrators and can be accessed from the Admin and UUMS dashboards respectively.

Contact Us

Customer Support

Plano, Texas USA - serves North America, South America, Latin America
+1 469-330-4581 (Customer Support voice)
uaservice@tek.com (Customer Support USA email)

London, England UK - serves Northern Europe, Middle East, and Africa
+44-1344-767-100 (Customer Support voice)
uaservice-uk@tek.com (Customer Support UK email)

Frankfurt, Germany DE - serves Central Europe and Middle East
+49-6196-9519-250 (Customer Support voice)
uaservice-de@tek.com (Customer Support DE email)

Padova, Italy IT - serves Southern Europe and Middle East
+39-049-762-3832 (Customer Support voice)
uaservice-it@tek.com (Customer Support IT email)

Melbourne, Australia - serves Australia
+61-396-330-400 (Customer Support voice)
uaservice-ap@tek.com (Customer Support Australia and APAC email)

Singapore - serves Asia and the Pacific Rim
+65-6356-3900 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Documentation Feedback

uadocfeedback@tek.com (Technical Publications email)

Table of Contents

1 Iris Performance Intelligence Overview

This chapter provides an overview of the Iris Performance Intelligence (IPI) system which is part of the Tektronix Communications Network Management Intelligent Network solution. The following components are described:

- IPI Overview
- IPI Services
- Key Performance Indicators / Key Quality Indicators
- Node Groups and User Groups Used as Filters
- IPI User Interface
- Historical Reporting Overview
- Alarms Policy Management Overview

IPI Overview

The Tektronix Communications IPI application enables supervision and troubleshooting of mobile data network resources and services to ensure quality of service; that is, accessibility, retainability, and performance. Combining network and service analysis, the IPI application monitors how applications perform and allows a deeper analysis of the network resources that are responsible for degradation of service.

IPI Services

Using application modeling, IPI enables users to monitor and report the services that provide them the highest value. For example, operators can use application modeling to define and monitor any number of the base applications or services, such as Emergency Services, Web browsing, Email, and Multimedia Messaging Service (MMS), and they can monitor user-defined applications such as Apple iPhone Web browsing, or Google Gmail. IPI enables users to define the services that are important to them through application modeling.

Services Defined by Tektronix Communications

IPI includes models for the following basic services: Data Network, Emergency Services, Web Browsing, MMS, and Email. The basic services are default services provided with each system. Application modeling includes definitions for the following:

- Protocols—Applications are associated to application protocols and to underlying network protocols. In addition, the base model includes a generic Internet Protocol (IP) application that reports on all IP traffic not bound to a specific application.
- QoS Categories—Quality of Service (QoS) categories are a logical grouping of indicators (KPIs/KQIs) for the quality of service. They focus on the following parameters: Accessibility, Retainability, Performance, and Others.
- Measures (KQIs/KPIs)—For each KPI category, a set of KPIs is defined. The overall status of an application is tracked by Key Quality Indicators (KQIs).
- Dimensions—Different sets of Dimensions for reporting the KPIs/KQIs are defined in the model, to identify the area responsible for the QoS degradation.

User-Defined Services

User-defined IP services are defined by the user and created in the IPI application by Tektronix Communications Customer Support; contact them if updates are needed. User-defined services can be associated to alarms and are reported through FastPath service analysis. Some services are also reported through Historical reports. Refer to the list of reports in the Online Help for more details. You can define IP services by customizing Services Defined by Tektronix Communications and linking them to the specific elements of their dimensions, described in **Table 1.1**.

Table 1.1 - Elements Used for Default User-Defined IPI Services

Network	Parameters
LTE Data 2G/3G Data	▪ Uniform Resource Locators (URL) ▪ IP addresses (application servers/nodes) ▪ Application protocols (identified by their UDP/TCP port number) ▪ APNs (Access Point Name) ▪ Handset Type ▪ User Plane Signaling Protocol (such as Hypertext Transfer Protocol (HTTP))
VoIP/IMS and Fixed Voice VoLTE	▪ Called Number ▪ To URI (SIP)
IMS (Diameter interfaces)	▪ Services can be defined by Source and Destination node for the following interfaces: Gx, STa, SWx, Gy, Rf, and Gxx (Gxa, Gxc).
Core Infrastructure	▪ Source Node ▪ Destination Node

Key Performance Indicators / Key Quality Indicators

IPI provides KPIs, which are defined in the application models and delivered with the application for the supported protocols, including Long Term Evolution (LTE), 2G/3G, and VoIP protocols. KPIs are based on measures available in the configured data sources (detail records generated by SPIprobes and G10 probes). Mobile LTE data records are only generated by G10 probes.

KQIs can be configured as combinations or mathematical expressions of KPIs. The definition of a KQI can include KPIs from different protocols; for example, GTP PDP Context Create Success Rate and MMS Submit Success Rate. KQIs are then associated with a specific application and specific KPI QoS category. Contact Tektronix Communications Customer Support for KQI configuration details.

Refer to the Online Help for KPI details.

KPI Quality of Service Categories

The KPIs are aggregated within the application by the following QoS categories:

- Accessibility—Can customers access the application?
- Retainability—Once customers are in the application, can they continue to access it?
- Performance—What is the customer experience in using the application?
- Others—Contains KPIs that do not fit into the previously mentioned categories; you can contact Tektronix Communications Customer Support to move these KPIs to one of the existing categories.

Available KPIs

IPI includes KPIs for performing analysis in the following networks (**Table 1.2**). For a complete list of KPIs supported, see IPI KPI White Papers.

Table 1.2 - Available IPI KPIs

Network	KPIs
Fixed Voice and IMS	▪ Voice Signaling ▪ Voice Media ▪ Voice Session ▪ Voice Call QoS
Mobile LTE Voice (for VoLTE)	▪ Voice Signaling ▪ Voice Media ▪ Voice Session
Mobile LTE Data	▪ Data User Plane KPIs ▪ Data Control Plane KPIs
Mobile 2G/3G Data	▪ User Plane KPIs ▪ Data KPIs
Mobile 2G/3G Voice	▪ Voice KPIs

Exporting IPI KPIs

KPI Export enables more flexible information sharing between systems. IPI provides an export feature enabling you to routinely extract KPIs from the database, so you can share them with third-party applications. The intent is to obtain more meaningful information than is possible using IPI alone. KPIs can be exported according to the database tables that store them. The KPIs exported into files conform to a specific format. Contact Customer Support for more information about KPI Export.

With IPI, you can also export to a CSV file all CDR Log data, with or without Advanced filter data, for FastPath, PNA, PGA, PEA, and FCL workflows. For details, see Online Help.

IrisView Framework

This section provides an overview of the IrisView applications and tools that support IPI.

IrisView and IPI

Figure 1.1 shows the major IrisView framework components that support IPI. You launch IPI from IrisView. You can set IPI alarm thresholds with the Alarms Policy Engine and launch Iris Session Analyzer (ISA) from IPI to further isolate a problem in the ISA results window. You can launch Reports from IrisView to configure and generate both predefined Management Reports and Query Reports for performing IPI historical analysis.

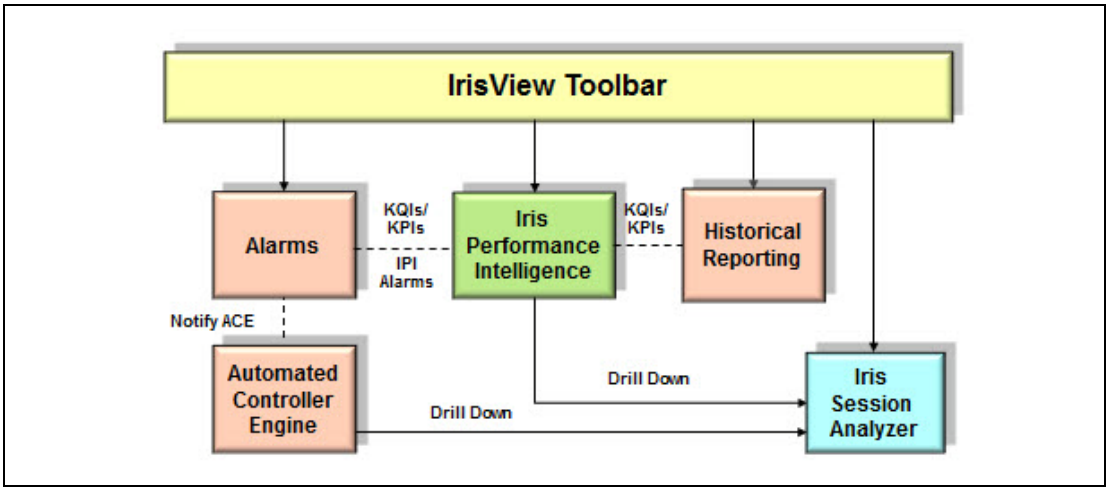

Figure 1.1 - IrisView Components Used with IPI

IPI Components

Made up of workflow-directed dashboard views and auxiliary reporting functions, IPI delivers value to multiple organizations responsible for managing the health and profitability of the network. The solution components in Iris Performance Intelligence are as follows:

- FastPath—Alarm-driven, QoS-based workflow for accelerated investigation of threshold breeches
- Proactive Network Analysis (PNA)—Operations workflow highlighting the poorest performing entities within the context of traffic volume and in relation to other elements
- Proactive Group Analysis (PGA)—Operations workflow that enables you to identify the worst groups for the selected KPI and determine the root cause for their bad performance

- Proactive Element Analysis (PEA)—Operations workflow that enables you to analyze the behavior of the network, focusing on specific elements such as APNs, Handset, or Network nodes.
- Failed CDR Log (FCL)—Operations workflow that enables you to access the DR log for failed calls when you already know the interfaces to be investigated and the faults being experienced
- Cause Code Analysis (CCA)—Operations workflow that enables you to analyze failure cause code counting over time
- Historical Reports Management—Both flexible snapshot reporting and the ability to create customized reports, based on direct access to a database of collected metrics
- Alarm Policy Management—Performance thresholds defined by system administrators for any QoS parameter: Retainability, Accessibility, Performance, and Others

Networks Supported

IPI supports these networks; for interface, protocol, and probe support, see IPI Online Help.

- Fixed Voice and IMS networks
- Mobile 2G/3G Voice and Data networks
- Mobile LTE Voice and Data networks

IPI Capabilities

Table 1.3 lists the IPI unique capabilities and benefits.

Table 1.3 - IPI Unique Capabilities and Benefits

IPI Feature	Capabilities	Benefits for Network Operations, Engineering, and Planning
Proactive Network Analysis (PNA)	**Full view of the network**—ability to report and alarm on network and application KPIs	▪ Leverage of existing Tektronix Communications probe investments ▪ KPIs for all monitored nodes and dimensions ▪ Reduced applications for different domains (Data Center, Core, Access, Transport)
Proactive Group Analysis (PGA)	**Full view of defined groups** (based on IMSI and MS IP address of end users such as IMSI groups, MS IP Pool, and inbound roamers by PLMN and by Country)—ability to report on groups, network, and application	▪ Quick identification of user groups not performing as defined by SLA ▪ Performance behavior of the groups split among different network elements ▪ Impact of Network elements performances on groups

Table 1.3 - IPI Unique Capabilities and Benefits (Continued)

IPI Feature	Capabilities	Benefits for Network Operations, Engineering, and Planning
Proactive Element Analysis (PEA)	**Full view of logical elements**—ability to analyze the behavior of the network while focusing on specific elements, such as APNs, Handset, or Network nodes	▪ Quick identifications of elements, such as Handset and APN, that are responsible for poor performances in the network ▪ Fast identification of failure causes for the element being analyzed
Failed CDR Log (FCL)	**Quick failed calls analysis**—ability to access the DR log and filter on the interface, protocols, nodes and user to be analyzed	▪ Reduce time to access DRs when the interface, protocol, nodes, or users are known
Cause Code Analysis (CCA)	**Cause code analysis**—ability to analyze cause code counting over time	▪ View the peg counts of the failure response cause codes that contributed to the failure KPI
FastPath	**Tailored workflows for faster troubleshooting—**ability to classify and capture data into quality of service categories	▪ Reduced resolution time for trouble tickets ▪ Increased visibility and verification of carrier quality goals ▪ Reduced alarms and false positives
Historical Reporting	**Model-driven historical reporting and trending**—flexible and reliable reporting tailored to business processes	▪ Ability to understand level and pattern of service usage at high data rates and with service proliferation ▪ Automatic delivery of scheduled overnight reports
Policy Engine	**Centralized policy management**—designed to create, manage and evaluate policies all the time in real-time	▪ Visibility of issues with corporate Service Level Agreements (SLA) ▪ Shorter time to repair for trouble tickets ▪ Ability to do proactive management by setting higher thresholds and watching trends
KPI Exporting	**Database export of KPIs**—export KPIs from database to third-party application.	▪ Provide high-value KPIs to third-party applications, thus enabling deeper integration of IPI with other tools currently being used. For more details, see OAM online help.

IPI User Interface

After launching Iris, you can access from the IrisView toolbar any Iris application for which you are licensed. When you click on the Iris Performance Intelligence button in the IrisView toolbar, several workflow buttons appear in the toolbar. Each button opens a dashboard that supports a different workflow. This section describes the following user interfaces:

- Proactive Network Analysis User Interface
- Proactive Group Analysis User Interface
- Proactive Element Analysis User Interface
- Failed CDR Log User Interface
- Cause Code Analysis User Interface
- FastPath User Interface

Network Analysis Modeling

IPI provides quick troubleshooting for problems occurring in the monitored network. Users troubleshoot using a model of the network driving the workflow, thus allowing you to analyze each single KPI defined on the monitored interfaces. The Proactive Network Analysis (PNA) and Proactive Group Analysis (PGA) workflows allow for configuration in Network and KPI models.

Network Modeling

Network modeling includes the description of the Mobile Network Elements, such as GGSN, SGSN, RNC, and others. These elements are identified by user-configurable names automatically associated with addressing information detected in the network traffic, such as the IP address.

KPI Modeling

KPIs are defined in the network interface models delivered with the application based on measures available in the configured data sources. Currently, Mobile 2G/3G data and VoIP are retrieved from data records generated by SpIprobes and G10 probes. Mobile LTE data is only retrieved from records generated by G10 probes. For probe support details, see ***IPI Interfaces and Protocols*** document provided in the Online Help.

Node Type Support

You can analyze, using specific dashlets in Proactive Network Analysis, the different node types for all LTE, 2G/3G, and Voice KPIs. Node types are visible as filters in the FastPath landing page dashlets. You can also use node types as filters in PGA, in the DR Logs for any IPI workflow, or in Cause Code Analysis (CCA). You can use node type as a filter, as well, in Historical Reporting.

IPI node types are different than the node types configured in OAM for other Iris applications. For a list of node types supported in IPI, see the ***IPI Key Performance Indicators*** document available in the IPI Online Help.

Node Groups and User Groups Used as Filters

Node Groups are filters that enable users to select the relevant portion of the network to focus on. Node Group filters are available for FastPath, Proactive Network Analysis, Cause Code Analysis, Historical Reports, and IPI Alarms.

User Groups enable operators to identify high value subscriber groups on VoIP and IMS networks that are experiencing degraded QoS. User Groups allow users to define IPI alarms that can later be analyzed through FastPath. Moreover, Proactive Group Analysis and Proactive Network Analysis workflows enable users to identify the worst User Groups and detect which high-value customers are getting poor service.

Users can obtain reports on both User Groups and Node Groups using Query Reports. Node Groups are also supported in predefined historical reports. **Table 1.1** shows the KPIs available for each user group dimension.

Table 1.1 - User Group Types and KPIs

User Group Dimensions	KPIs
Inbound Roaming Country/PLMN Dimensions - for Voice/SMS KPIs	■ Mobile 2G/3G Voice KPIs
Inbound Roaming Country/PLMN Dimensions - for Data KPIs	■ Mobile 2G/3G Data KPIs
MS IP Pooling Dimension - for Mobile KPIs	■ Mobile 2G/3G Voice KPIs ■ Mobile 2G/3G Data KPIs ■ Mobile LTE Data KPIs ■ Diameter Point-to-Point-based Procedural KPIs
High Value Account (HVA) User Groups for Mobile (IMSI Grouping)	■ Mobile 2G/3G Voice KPIs ■ Mobile 2G/3G Data KPIs ■ Mobile LTE Data KPIs ■ Diameter Point-to-Point-based Procedural KPIs
HVA User Groups for VoIP/Fixed	■ VoIP KPIs

User Group Support in FastPath

You can assign User Group dimensions when creating IPI service-based alarm policies. The User Group dimensions are visible in the FastPath landing page dashlets for the given service.

Node Group and User Group Support in IPI Historical Reports and Alarms

You can specify node groups as filters for Management Reports or select node groups and user groups as dimensions for Query Reports. The node group filter is available for all Management Reports, with some exceptions such as reports based on the Crosstab template or Handover reports. See Historical Reporting Overview and the Reports section in Online Help. You can alarm on the user group dimensions, so you can react sooner to quality issues with your highest-revenue-generating customers. See Alarms Policy Management Overview and the Alarms section in Online Help.

IPI User Preferences

The IPI dashboard Options menu enables you to save, apply, and reset dashboard preferences.

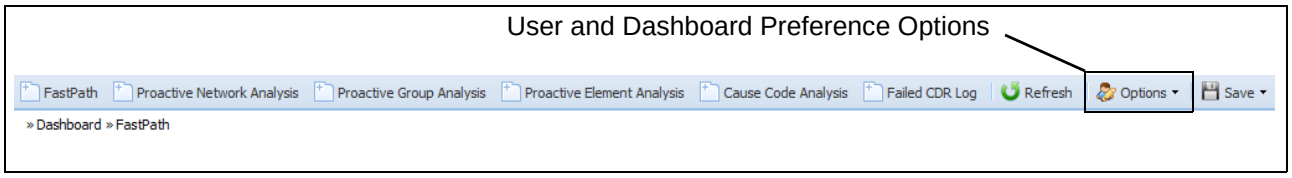

Figure 1.2 - IPI Dashboard

You can open the IPI User Preferences dialog box from the Options menu to set IPI to open dashboards or drilled-to dashlets in a current or new browser window or tab. The default setting is New Window.

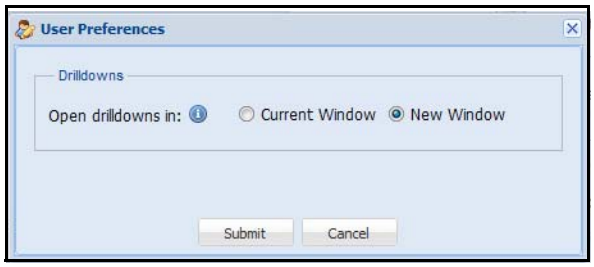

Figure 1.3 - IPI User Preferences Dialog Box

Proactive Network Analysis User Interface

Figure 1.4 shows the different graphical user interface (GUI) components of the PNA workflow. The Advanced filters are summarized in the graphic; for a complete list, see IPI Online Help.

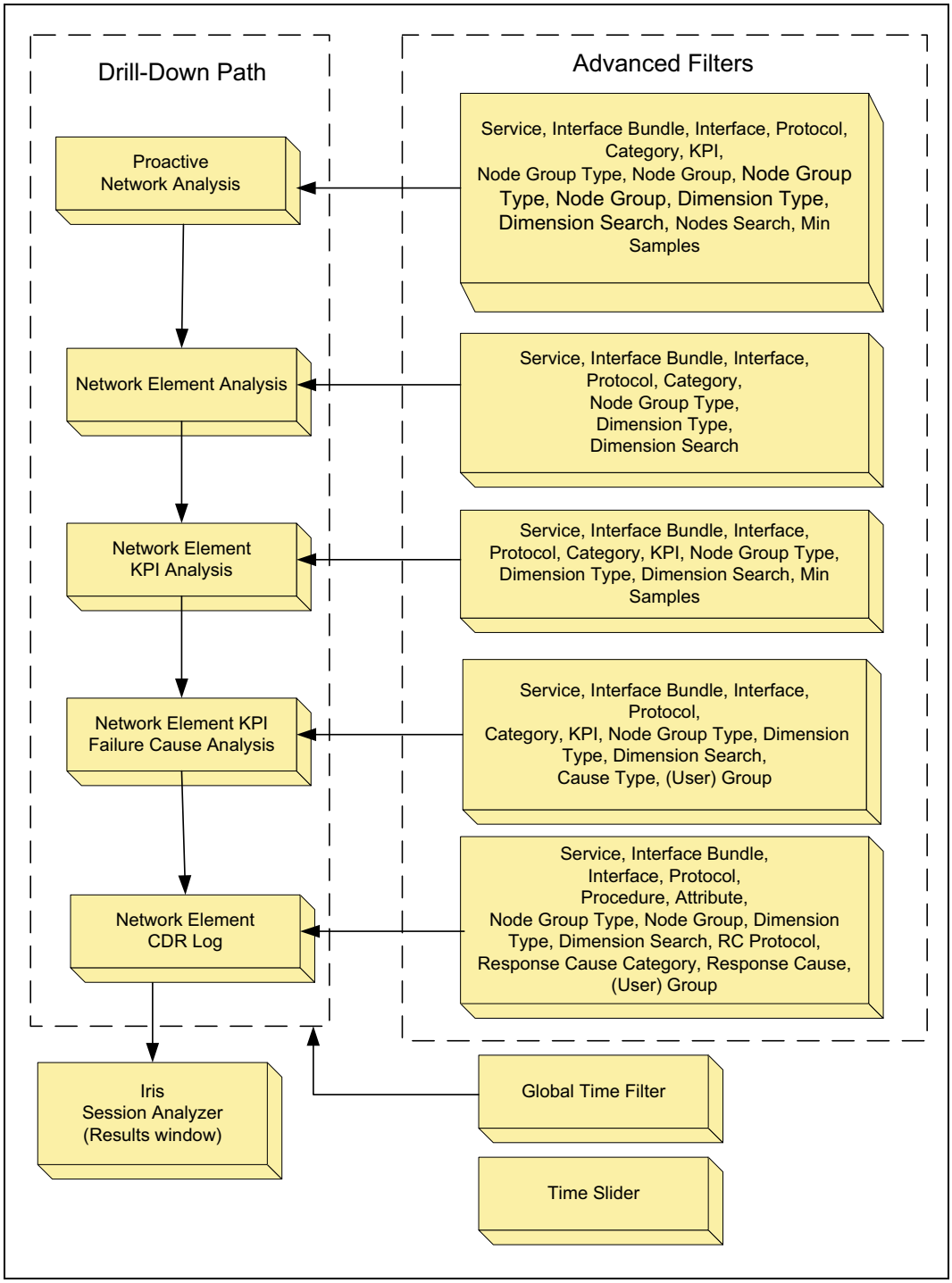

Figure 1.4 - Proactive Network Analysis User Interface

Proactive Network Analysis Workflow

PNA enables you to deflect problems by spotting trends in KPIs that could be potential problem areas. By reviewing the KPIs on an IP Application dashlet, you can drill down to specific KPIs, then to the Network Element Data Record (DR) Log, and finally to ISA, if necessary. **Figure 1.5** shows an example of using PNA to drill down in a VoIP network.

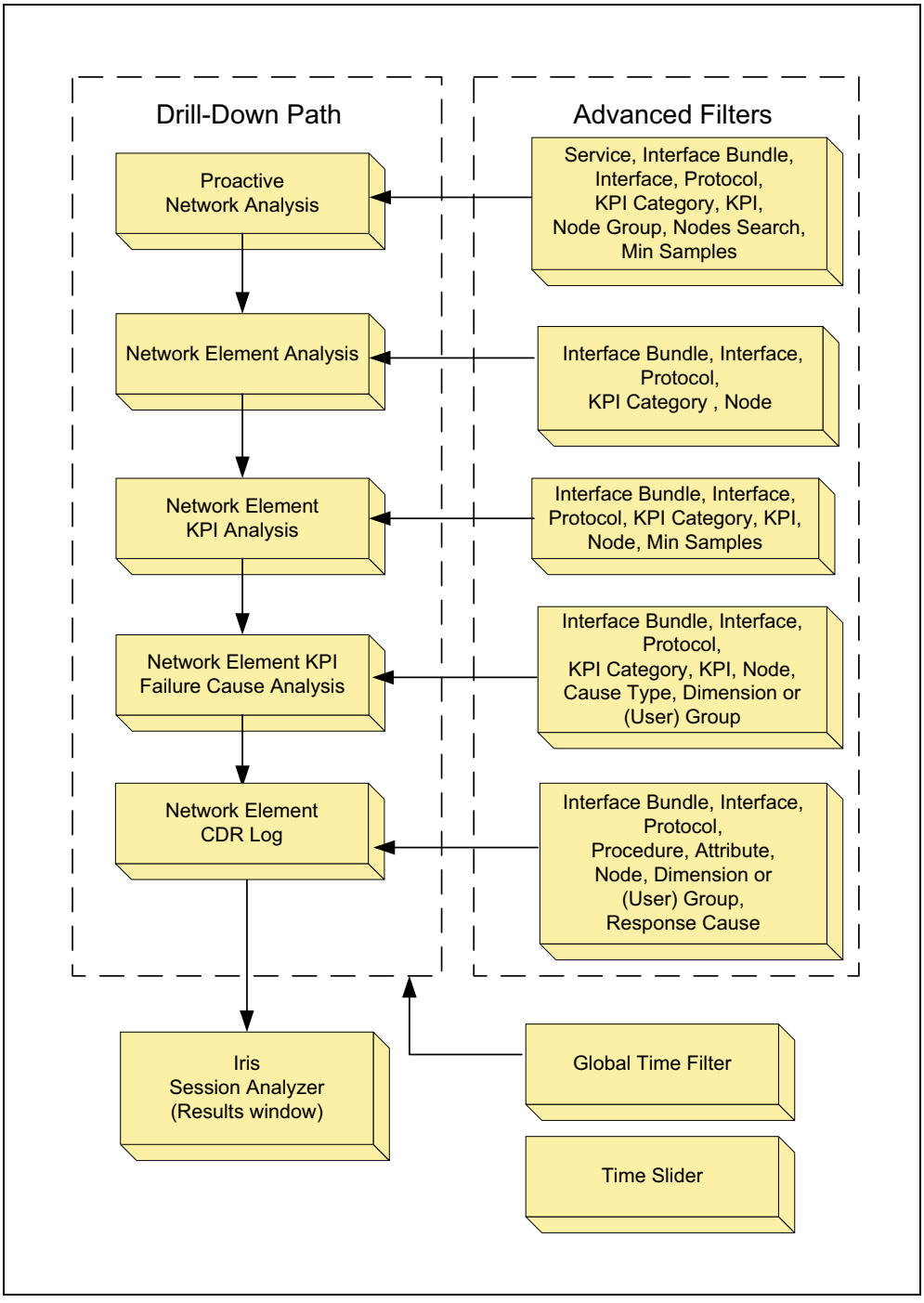

Figure 1.5 - Proactive Network Analysis Drill-Down Example for VoIP

Proactive Network Analysis Dashboard

The purpose of the PNA dashboard is to facilitate troubleshooting the network and to simplify accessing the application and identifying problems. In this dashboard, you can examine the KPIs, look for nodes, trends in the failures, and connections to those failures. The PNA workflow is proactive because you use it to discover issues you do not yet know exist; that is, you are not driven by an alarm. But it can also be considered reactive if you use its workflow to resolve an existing problem.

View Connections

The PNA workflow provides a starting point for isolating network problems and the network elements involved. Using the PNA Global Filters, you select one interface, one network protocol, one KPI category, and the KPI that is driving your analysis so you can see the trend analysis and volume for the KPI. Once you select the KPI, you can determine the worst elements in the network for each node type that is relevant (as traffic source or destination) for the selected protocol.

You are able to view together a network element's logical connections and dimension for faster troubleshooting. You can also examine the connections between different network elements to identify congestion points and from there drill down to the Network Element CDR Log and then drill down on each line to open ISA. You are able to make decisions faster because you can view the connections between KPIs and their associated nodes and dimensions.

KPI Analysis

When you drill down to the Network Element KPI Cause Code Analysis dashboard, you are presented with multiple KPIs for the node selected in the top landing page. For example, in addition to viewing failure rate KPIs, you can also view latency KPIs to determine if the user wait times exceed acceptable values. The dashboard displays the latency and the success KPI side by side, so you can compare them faster. Once you choose the KPI you want to examine in the Network Element KPI Analysis dashboard, you can drill down to the Network Element KPI Cause Code Analysis dashboard to see the selected KPI and the Top-N worst elements of the available dimensions.

Proactive Group Analysis User Interface

The PGA workflow enables you to identify the worst groups for the selected KPI and determine the root cause for their bad performance. **Figure 1.6** shows the different GUI components of the PGA workflow. The Advanced filters are summarized in the graphic; for a complete list, see IPI Online Help.

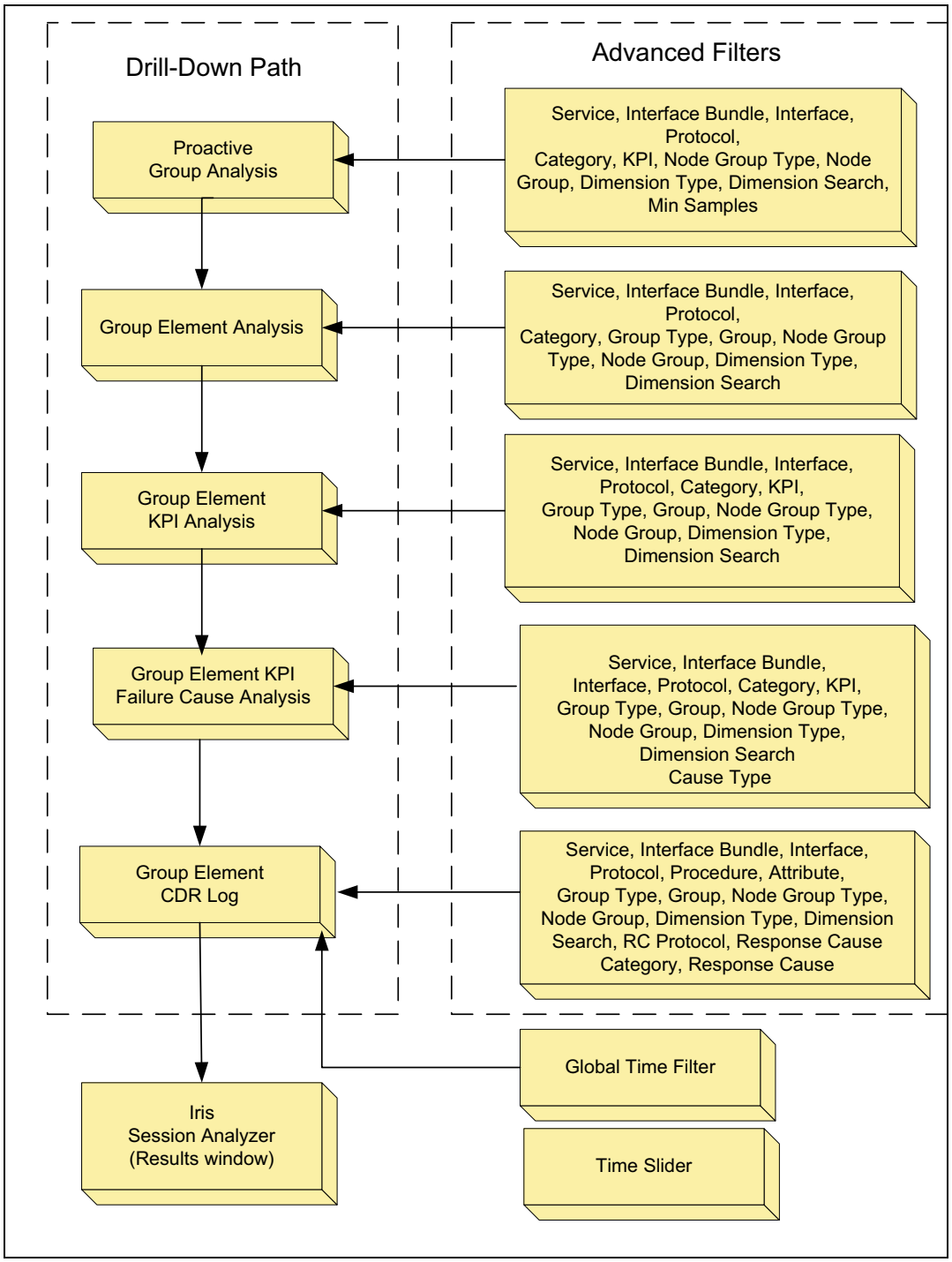

Figure 1.6 - Proactive Group Analysis User Interface

Proactive Group Analysis Workflow

The PGA drill-down feature provides an actionable path for troubleshooting at a group level. By reviewing KPIs on the Group Analysis dashlet, you can drill down to specific groups of elements and KPIs, then to the Group Element CDR Log, and finally to an ISA Results window, if necessary. **Figure 1.7** shows an example of using PGA in a Gi DHCP call.

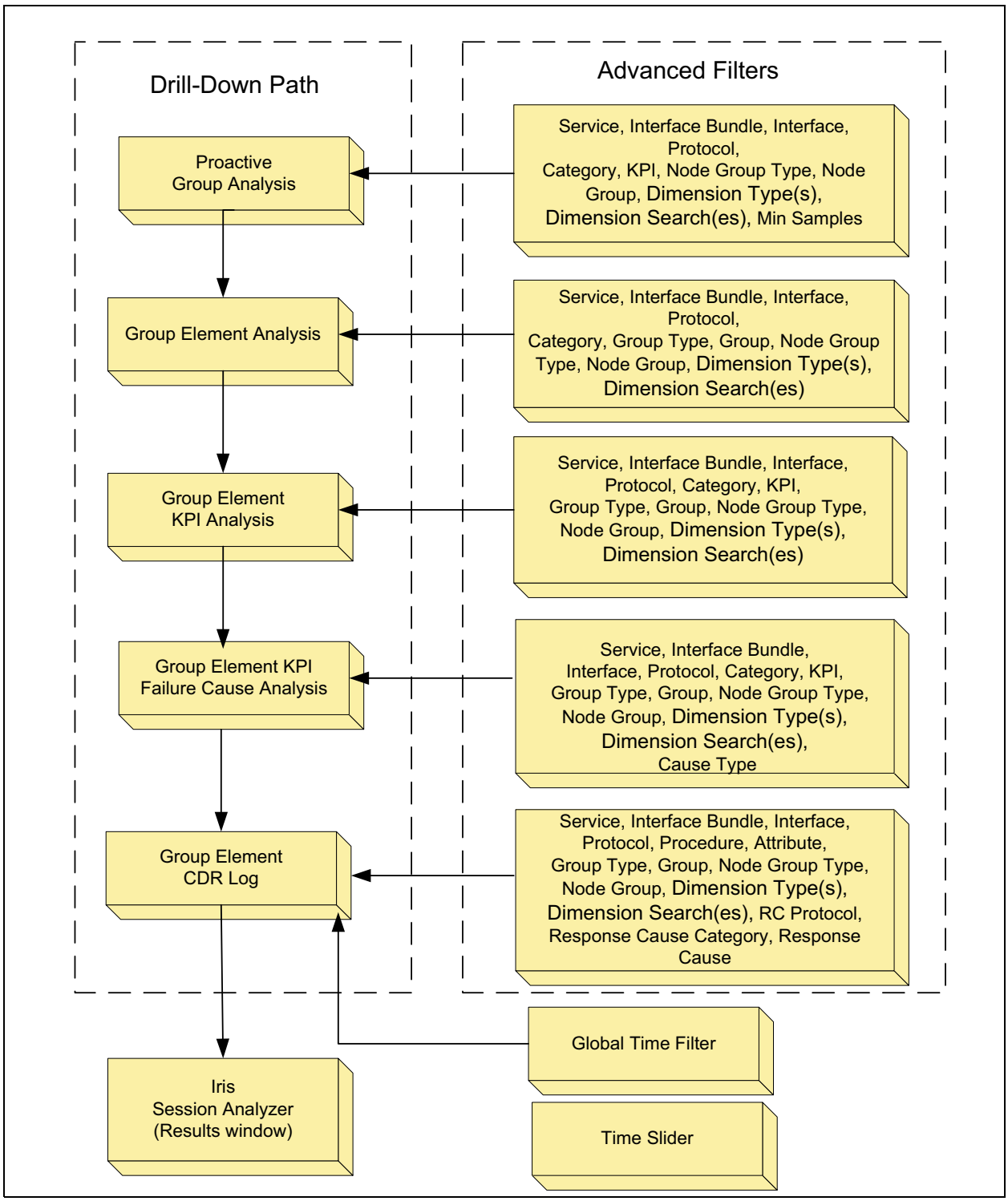

Figure 1.7 - Proactive Group Analysis Drill-Down Example for a Gn/Gi Network

Proactive Element Analysis User Interface

The PEA workflow enables a flexible analysis of the behavior of the network while focusing on specific network elements. **Figure 1.8** shows the different GUI components of the PEA workflow. The Advanced filters are summarized in the graphic; for a complete list, see IPI Online Help.

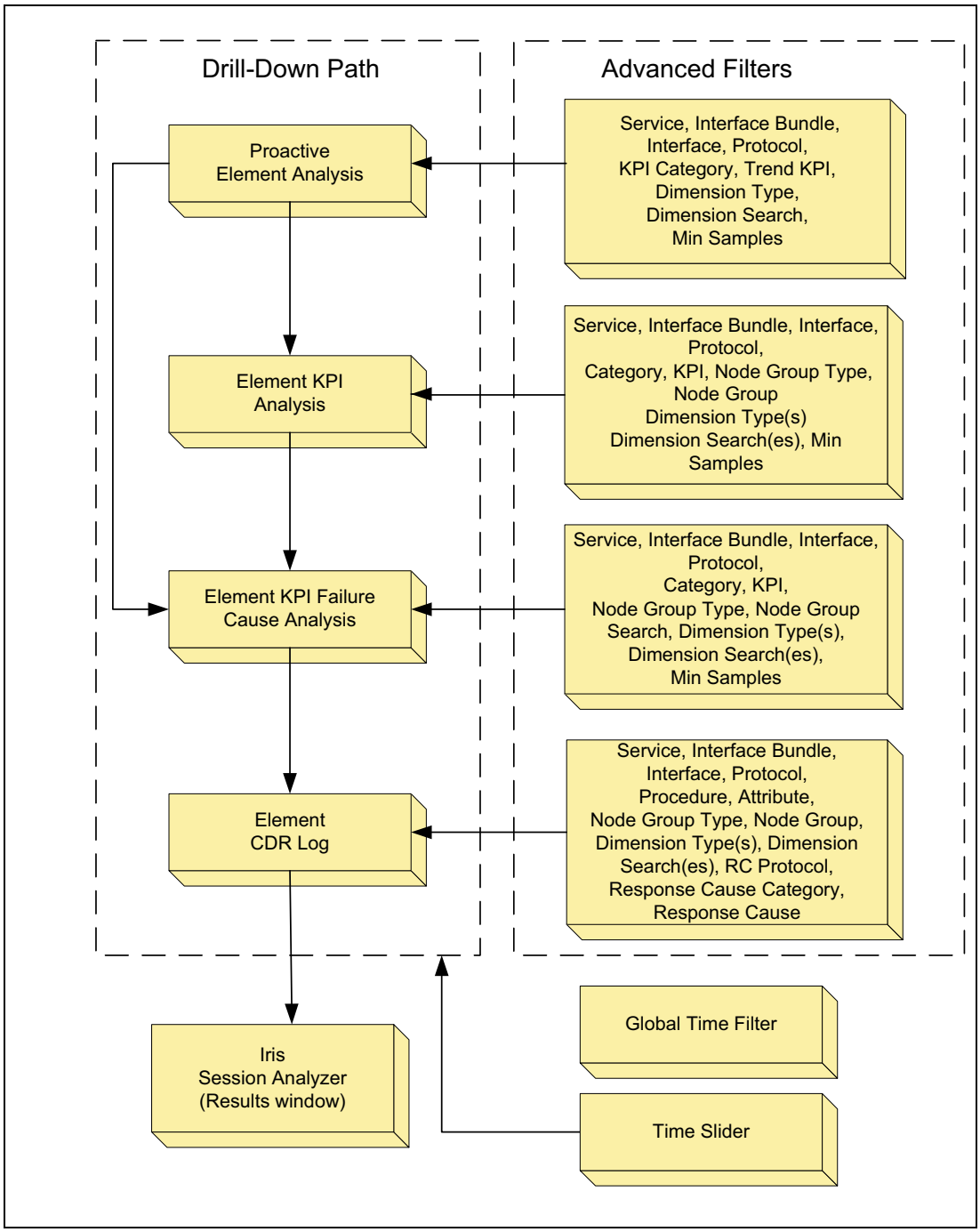

Figure 1.8 - Proactive Element Analysis User Interface

Proactive Element Analysis Workflow

The PEA workflow enables you to select drill down from a Top N worst performing element to view all failure causes for the element or directly to view the failure causes associated with a specific KPI. From there, you can drill down to the Element CDR Log, and finally to an ISA Results window, if necessary.

Figure 1.7 shows an example of using PEA in a Gi HTTP network.

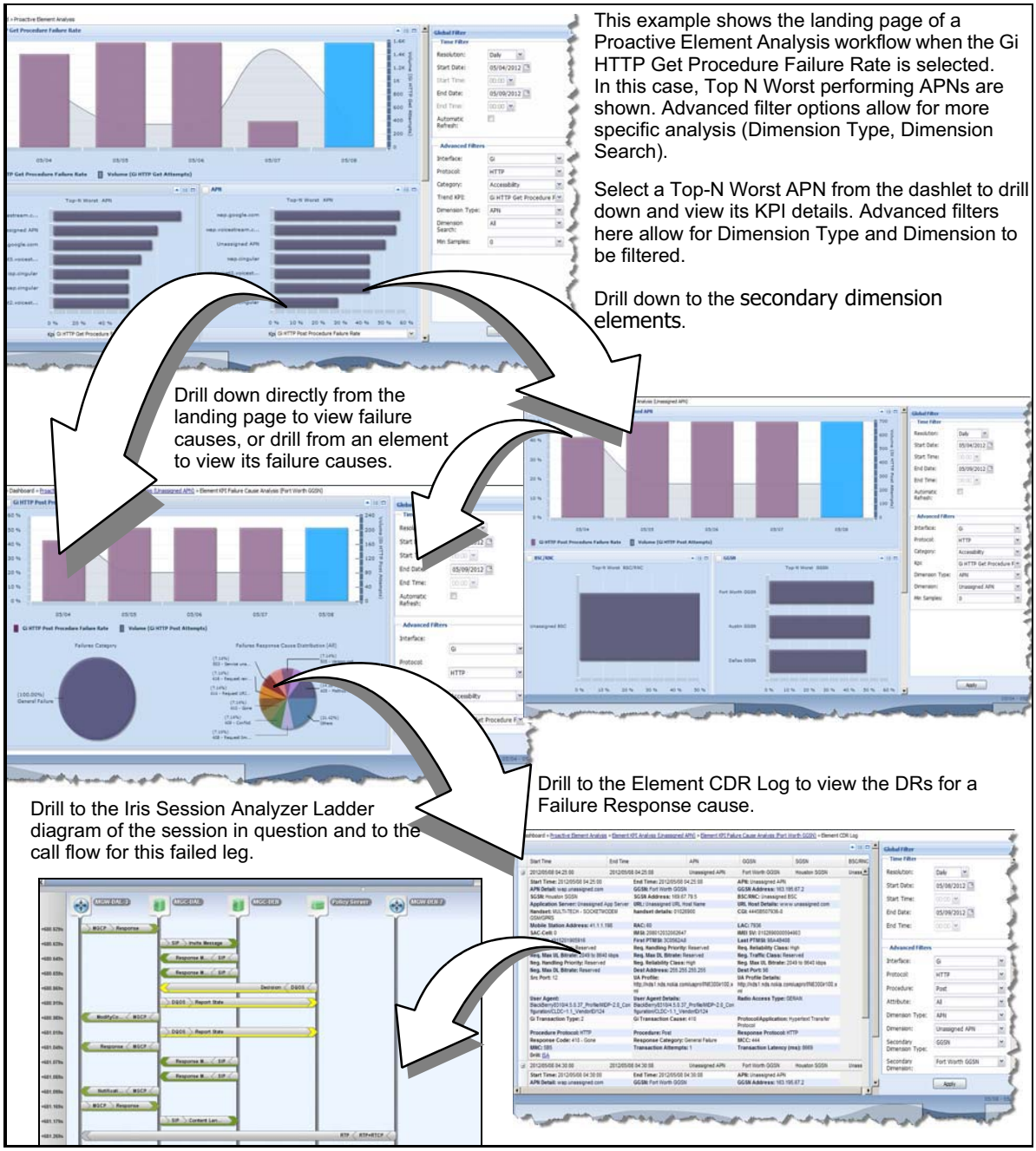

Figure 1.9 - Proactive Element Analysis Drill Down Example for a Gn/Gi Network

Failed CDR Log User Interface

IPI provides an option when users want to directly access the DR log to analyze failed calls. Using Advanced Filters, you can select a specific interface and protocol procedure to narrow the results in the Failed CDR log (FCL). You can also apply additional filters to select specific node types, response cause protocol, response cause category, and details. **Figure 1.10** shows the components of the FCL workflow. The Advanced filters are summarized in the graphic; for a complete list, see IPI Online Help.

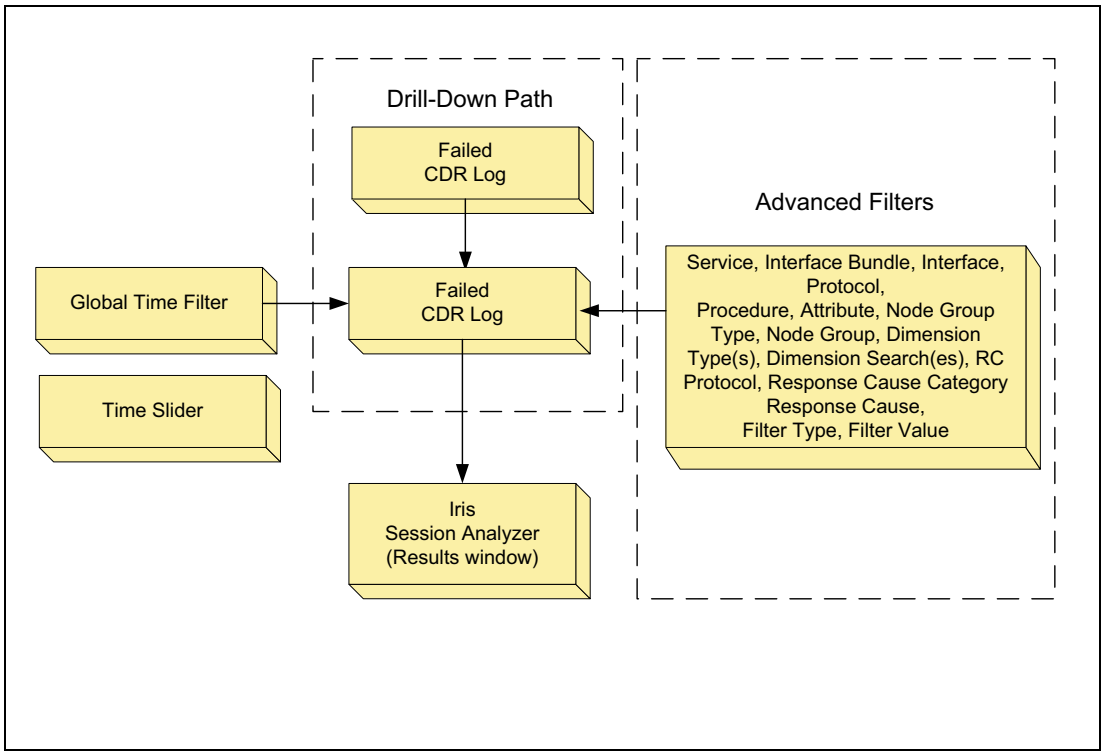

Figure 1.10 - Failed CDR Log User Interface

Failed CDR Log Workflow

The FCL workflow provides a quick and easy way to access the log by enabling you to drill down directly to the DR log. You can use the Advanced Filters to select an interface, protocol, and procedure. You can then select additional filters such as a specific node. Further analysis is available by drilling to the ISA results window. **Figure 1.11** is an example of the FCL window showing filtered results.

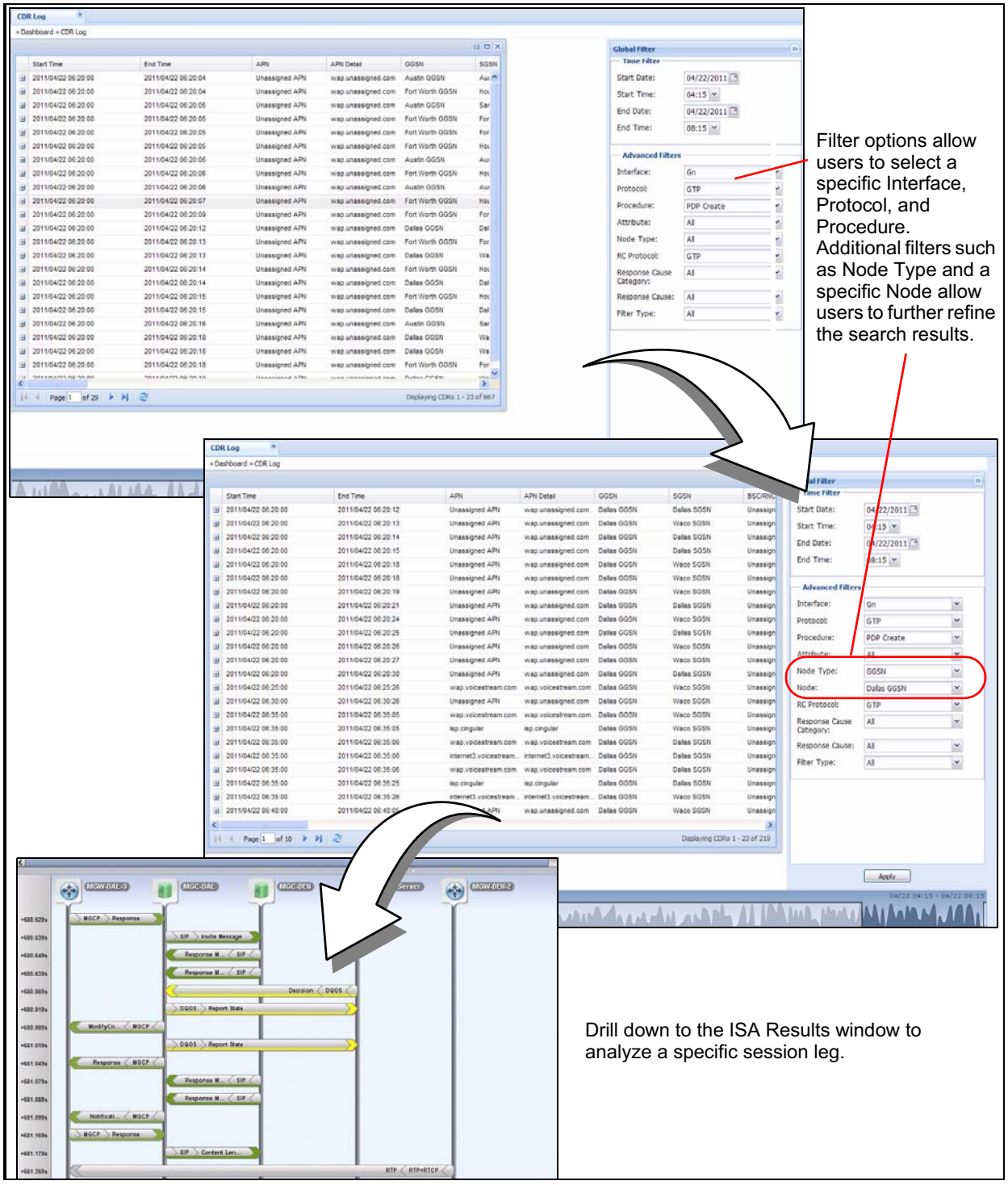

Figure 1.11 - Failed CDR Log Workflow Example for Node Analysis

Cause Code Analysis User Interface

The CCA dashboard provides operators with a network-level view of all failures across the network at any given instance over time. Operators can use this dashboard to proactively troubleshoot and resolve network issues as they arise, before a large network outage occurs. **Figure 1.10** shows the components of the CCA workflow. The Advanced filters are summarized in the graphic; for a complete list, see IPI Online Help. This workflow is supported by specific protocols; these are listed in the ***IPI Interfaces and Protocols*** document in the online help.

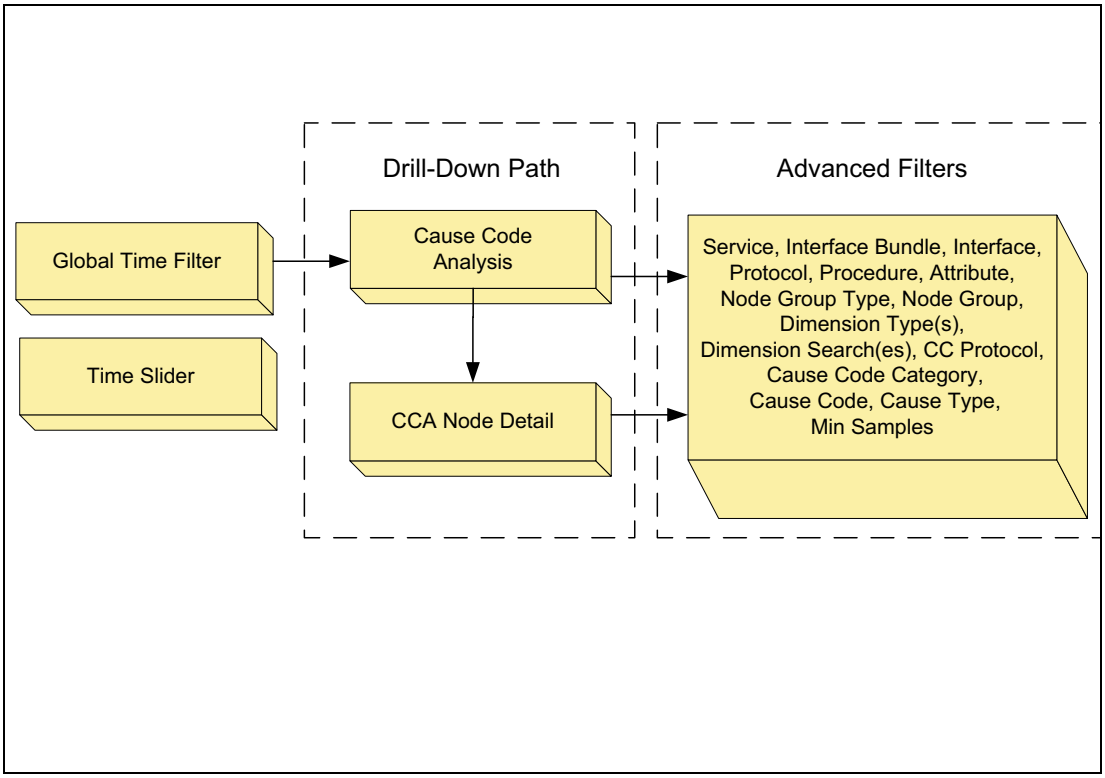

Figure 1.12 - Cause Code Analysis User Interface

Cause Code Analysis Workflow

The action path for the CCA is a quick and easy way to troubleshoot failures across the network. Response Code filters in the Global Advanced Filters area enable you to select specific failure root causes by which to analyze data. **Figure 1.11** is an example of the CCA window showing filtered results for a specific Interface, Protocol, and Failure KPI, then refining the search results by using specific response cause parameters as filters.

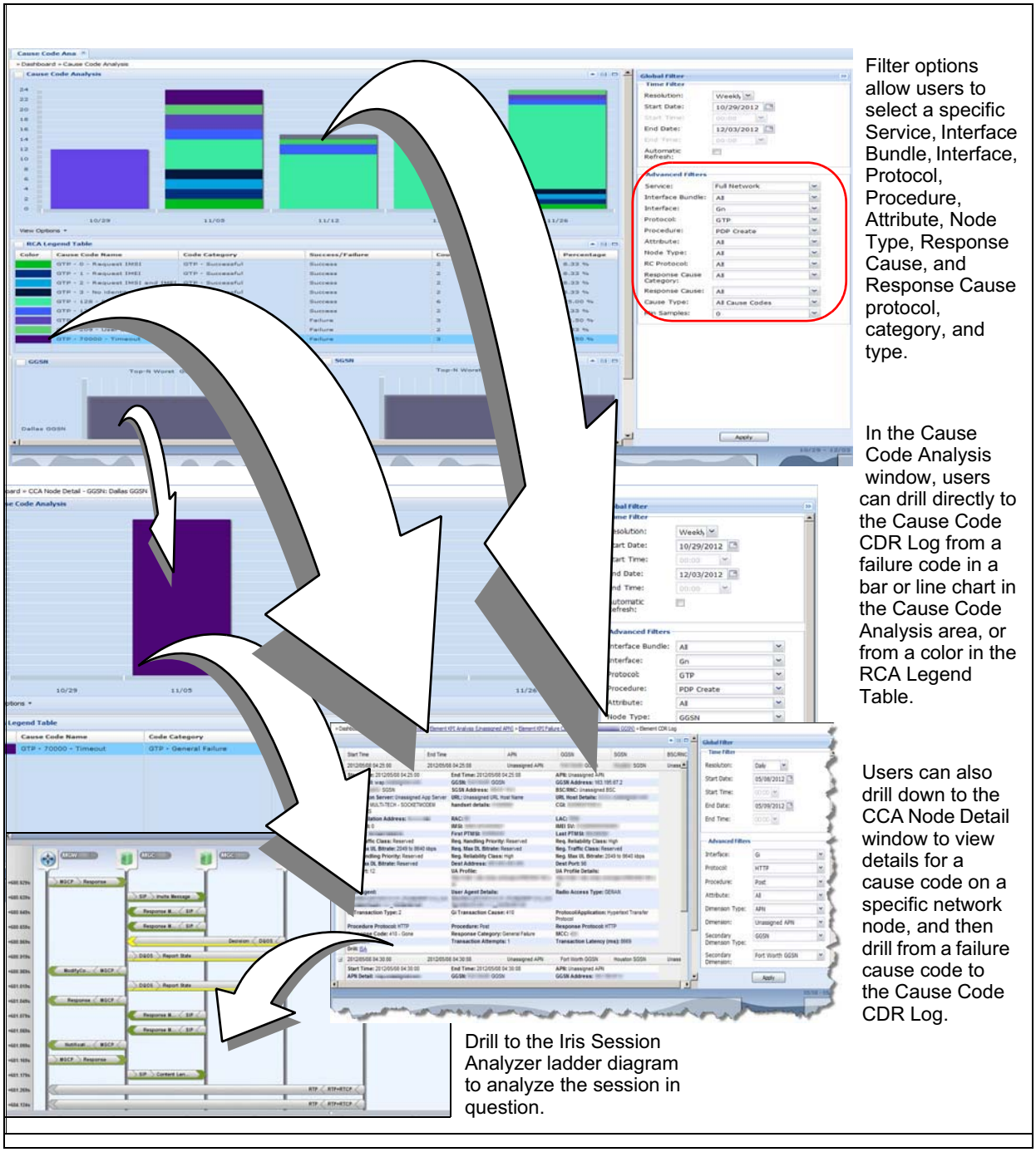

Figure 1.13 - Cause Code Analysis Workflow Example

FastPath User Interface

Top-level KPI category alarms link directly to KPI analysis views for the relevant underlying network elements. **Figure 1.14** shows the main components of the FastPath user interface. The Advanced filters are summarized in the graphic; for a complete list, see IPI Online Help.

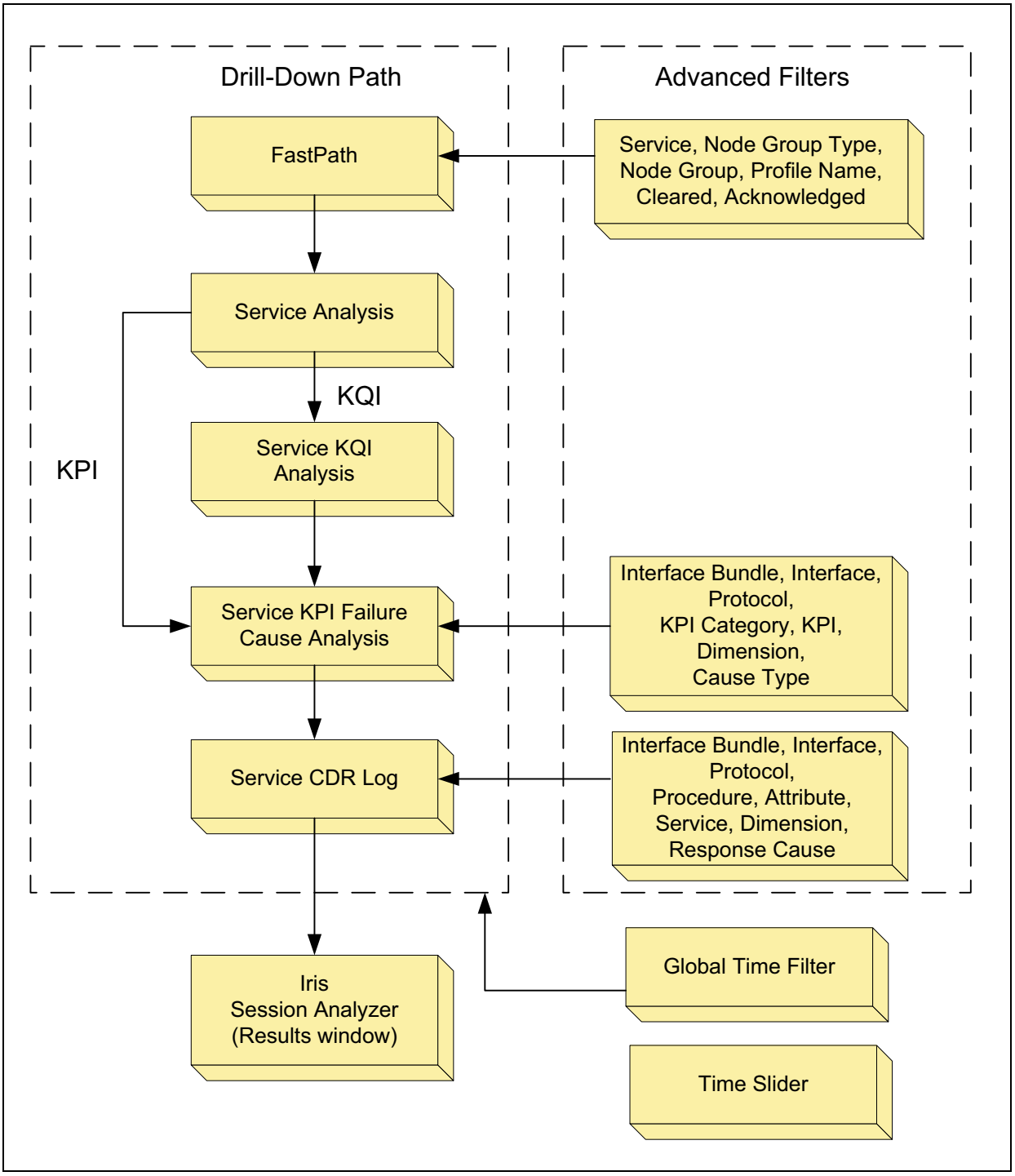

Figure 1.14 - FastPath User Interface

FastPath is an alarm-driven workflow designed for Network Operations and Engineering organizations that can tailor their workflows to their business model. FastPath is a reactive type of workflow, as you start troubleshooting from issues (alarms) that have already taken place. FastPath can also be considered proactive if you configure alarms to trigger when the network performance degrades to the point of impacting subscribers.

FastPath Dashboard

The FastPath user interface provides a snapshot of service performance for network elements and KPI thresholds. You can drill down from FastPath to a specific session in ISA. **Figure 1.15** shows an example FastPath dashboard.

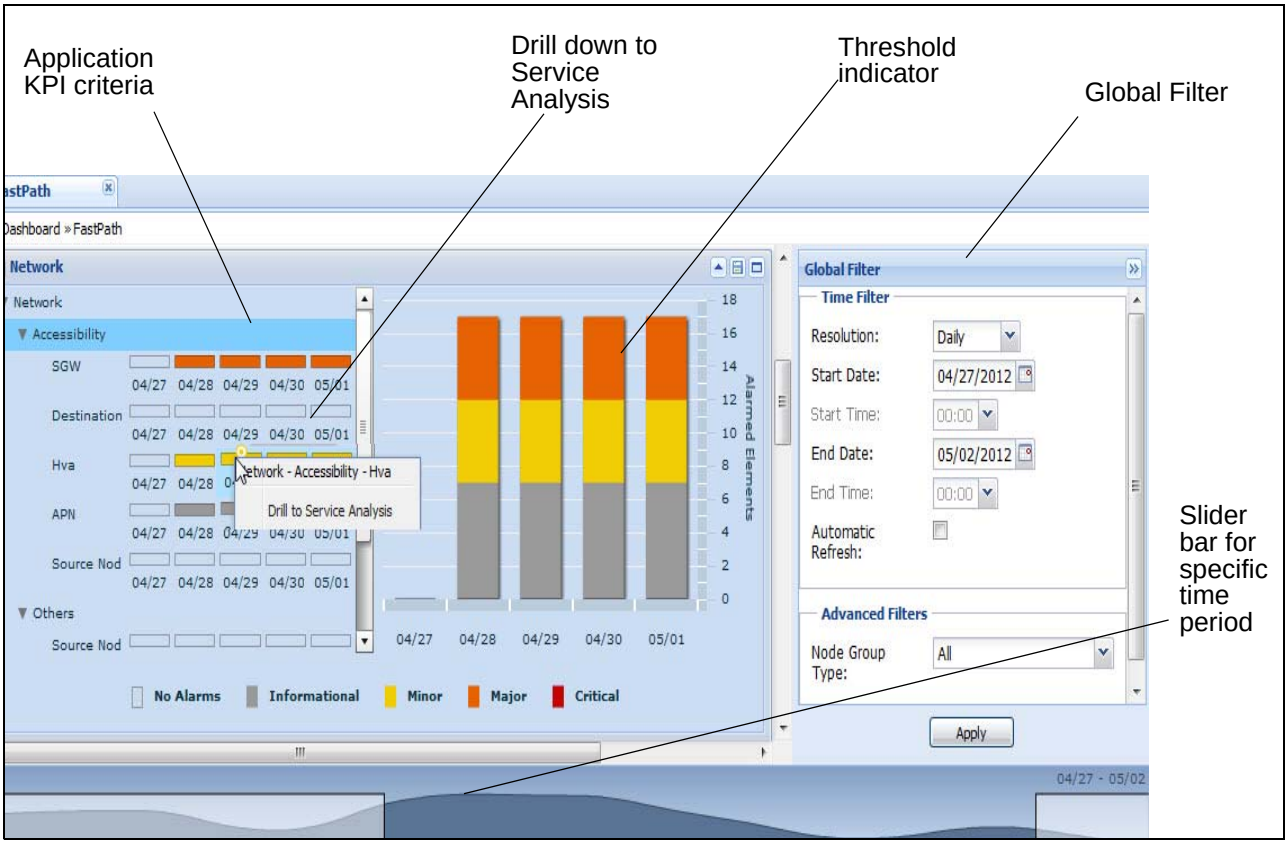

Figure 1.15 - IPI FastPath Dashboard Example Showing Mobile LTE Data

Services Support

The FastPath dashboard displays different dashlets; each dashlet is its own service. Typically a dashlet represents a VoIP/IMS, Mobile LTE Data, or Mobile 2G/3G Data service that you can purchase. For example, in **Figure 1.15**the dashlet represents Data Network services, which is a default Mobile LTE data service. Currently you contact Customer Support if you want to create new services tailored to your individual needs. Services can be created by specifying elements such as those described in **Table 1.1**. For example, if a carrier is selling the Apple iPhone they can create an iPhone service to track the behavior of those types of handsets.

IPI Alarms

Once the services are created, you can then create alarms on the services. The alarms fall in the QoS categories of Retainability, Accessibility, Performance, or Others. KPIs, categories, and services are model-driven, so everything can be changed. A carrier would create alarms on FastPath services that they already know they want to track, such as high-performing revenue services.

FastPath Workflow

The FastPath operations workflow enables you to inspect a specific alarm condition and isolate the area of failure. **Figure 1.16** shows an example drill down path in an LTE Mobile Data network starting with alarms, then to KPIs, to the Service CDR Log, and finally to ISA, if necessary.

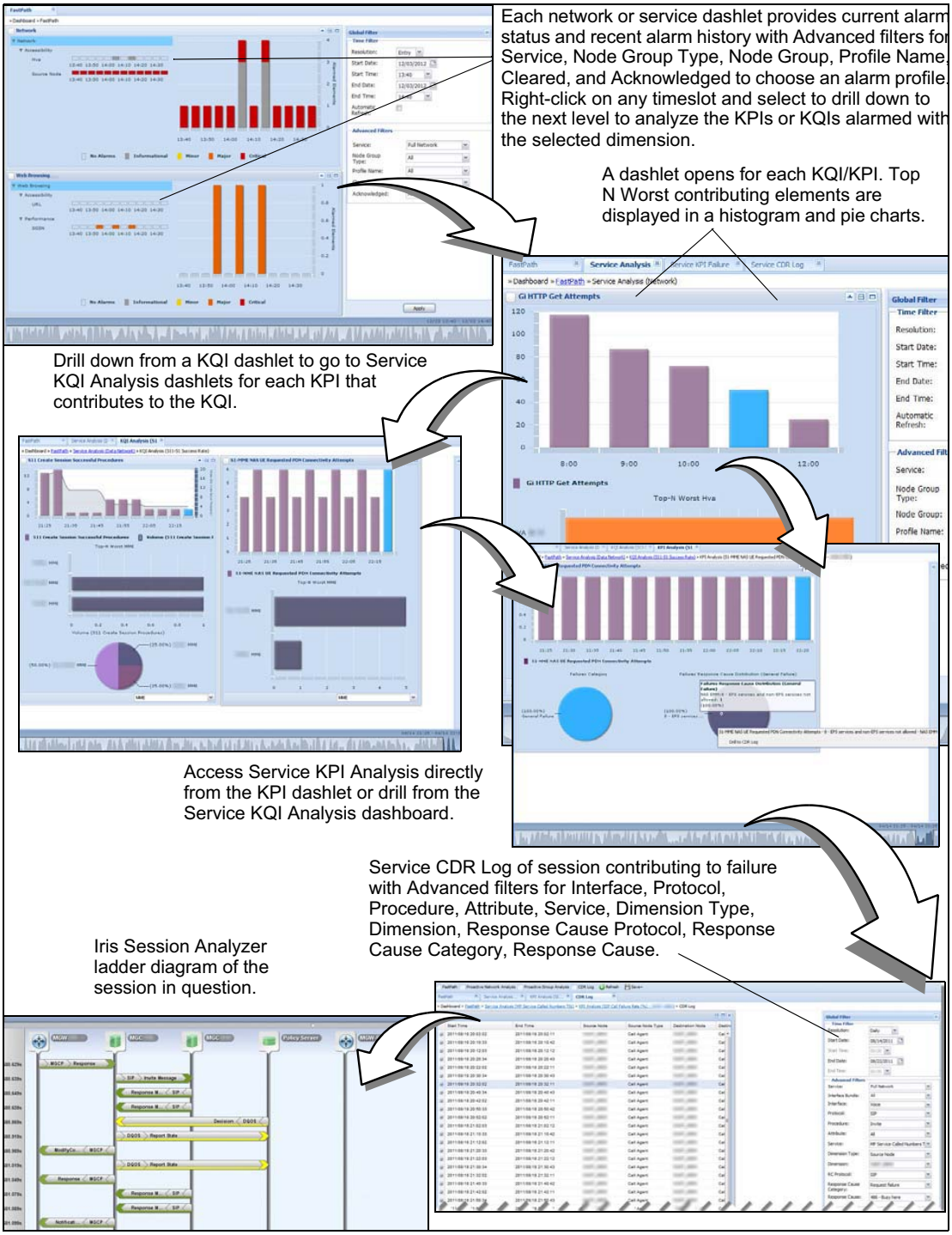

Figure 1.16 - FastPath Alarm Investigation Workflow Example for LTE Mobile Data

Alarmed Network Elements

After you create those service-based alarm policies in the policy engine, the corresponding alarmed elements show up in FastPath in a dashlet. For instance, in Data Network, FastPath can show you the last hour in five-minute increments with the alarmed elements with the worst severity showing up in that five-minute period. If you have a policy on Gateway GPRS Support Node (GGSN) dimension and the GGSN has several alarms in the time interval, it is counted only once in the chart with the worst severity being used.

Node Analysis

When issues are identified by KPI alarms on services, the FastPath workflow provides an effective drilldown to the ISA Ladder Diagram, enabling quick identification of the root cause of the problem. You can quickly react and solve problems on the most crucial services you are providing, protect revenue, and ensure quality expectations are met. You can concentrate the alarm analysis on a specific section of your network using node group filters, and you can also view node types as filters in the FastPath landing page dashlets.

Problem Analysis

FastPath can help carriers determine at a glance what anomalies to look at first. For instance, carriers can set alarm thresholds high enough so the carrier can find problems before the majority of their subscribers are affected. If the carrier sees the customer experience degrading, the carrier can tackle it right away by drilling down, isolating the problem, and resolving the issue before the customer ever knows about it.

Quality of Service Parameters

FastPath can display one or more of the following QoS parameters for a given service:

- Accessibility—the ability to get on the application
- Retainability—the ability to stay on the application
- Performance—the customer's experience while using the application
- Others—KPIs that do not fit into the previously mentioned categories; you can contact Tektronix Communications Customer Support to move these KPIs to one of the existing categories

For example, if a user is trying to get onto the network, Packet Data Protocol (PDP) Context would be an Accessibility KPI. The users' drop rate would be a Retainability KPI, and the jitter, delay, or latency would be performance KPIs.

FastPath Drill-Down Paths

When you see a critical alarm as shown in **Figure 1.15**, you can click on the alarm and drill to the next layer, Service Analysis, which represents the next alarm level. Service Analysis shows you the failing KPI; it shows you the worst time period where the alarm happened below the threshold and the volume of those attempts. Below the KPI is the Top N worst affecting elements and alarms. You drill down from there to Service KPI Failure Cause Analysis to dive deeper into that particular KPI. Now you can see below it the different failure categories that the carrier has already configured and the individual causes for those categories. Once you see a failure problem, you can drill to the Service CDR Log. For more details, see Drill to DR log and ISA to nail down the issue..

HISTORICAL REPORTING OVERVIEW

The Iris Historical Reporting feature assists service providers in validating market forecasts and benchmarking actual service uptake for more informed expansion planning. IPI leverages collected data for longer term reporting with a reporting component that includes predefined reports. The IPI Management Reports and Query Reports features provide you with the following capabilities:

- Deliver simple reports to key business owners on demand
- Schedule routine reports to meet the needs of downstream organizations
- Create and run Query Reports using customized forms to meet your needs
- Gain valuable insight into traffic trends with short- and long-term reporting options
- Build the case for further investigation of network hot spots, validation of capacity spending allocations, or selection of regions for service introductions

Historical Report Profiles

IPI provides a set of predefined profiles for monitored network elements and service, as well as report authoring capability using database queries. The Historical Reports feature enables you to track what applications are used, how much they are used, where they are used, with what device they are used, what load they generate on the network, and how well the network supports the load.

Management Reports

The predefined Management Reports are organized using the categories in **Table 1.4**. For more details on procedure analysis, network, and application reports, refer to the ***IPI Management Reports*** document in the Iris Online Help.

Table 1.4 - Predefined Management Reports Categories

Network	Analysis Types	Report Types
Mobile 2G/3G Data and Voice	Network Analysis	Accessibility Procedure Retainability Performance Top N
	Busy Hour Analysis	Busy Hour
	Service Analysis	Service
Mobile LTE Data	Network Analysis	Accessibility Procedure Retainability Performance Top N
	Service Analysis	Procedure
	Application Analysis	Service
	Busy Hour Analysis	Busy Hour
Fixed Voice, IMS, and VoLTE	Network Analysis	Procedure Performance Top N
	Busy Hour Analysis	Busy Hour

Busy Hour Management Reports

Busy Hour (BH) is a sliding 60-minute period during which the maximum value for a selected “Busy Hour KPI” in a given day occurs. To analyze the Busy Hour, you need to run Management Reports. BH reports provide a list of KPIs that enables you to understand the network behavior during periods of high traffic identified by the selected BH KPI.

To configure a BH report, you apply a network-wide or per-node filter and associate it with a KPI. For per-node BH, the busy hour interval can be different for each node. For network-wide BH, the busy hour interval is the same for all nodes. The output report shows only the “Start Time” of each BH interval. This means that the KPI selected for BH reached its maximum aggregated value 60 minutes after the start time. For more details, see ***IPI Management Reports*** document available in the IPI Online Help.

Top N Management Reports

Top N reports are Management Reports that enable you to identify the network elements with the most loading. Moreover, they provide the Access Point Names (APN) and Uniform Resource Locators (URLs) that have the most traffic and the Handset types that have been used the most. You configure N, the number of network elements to use in the report, in the Report Profile wizard. For details, see Reports topics in Iris Online Help.

Query Reports

Query Reports categories are shown in **Table 1.5**. For more details on available parameters and supported interfaces and protocols, refer to the ***IPI Query Reports*** document in the Iris Online Help.

Table 1.5 - Query Report Types

Network	Report Type
Mobile LTE Data	Procedure
	Performance
Mobile 2G/3G Data (Gn/Gi)	Control Plane Procedure
	User Plane Performance
Mobile Voice and Data (2G/3G - IuPS, IuCS, Gb, Aif)	Procedure
	Call Correlated
Fixed Voice, IMS, and VoLTE	Voice Procedure
	Core RTSP Procedure
	Call Signaling
	Media QoS

Historical Reporting User Interface

Figure 1.17 shows the Iris Reports user interface components. The reporting feature uses templates to represent the appearance of a given historical report. The IPI report is a link between a set of data and the report template. A set of Extensible Markup Language (XML) files are used to model the templates while another set of XML files represent the actual reports. The reports are model driven: KPIs in the reports can be customized leveraging on aggregated data in the measurement database. For detailed information on Historical Reporting components, see the Iris Online Help.

Using the Cognos report engine, you can generate two types of reports: Management Reports and Query Reports. You can generate Management Reports using predefined report templates, and you can also define your own queries using Cognos Query Studio. For changes to predefined reports or additional predefined reports, contact Tektronix Communications Customer Support.

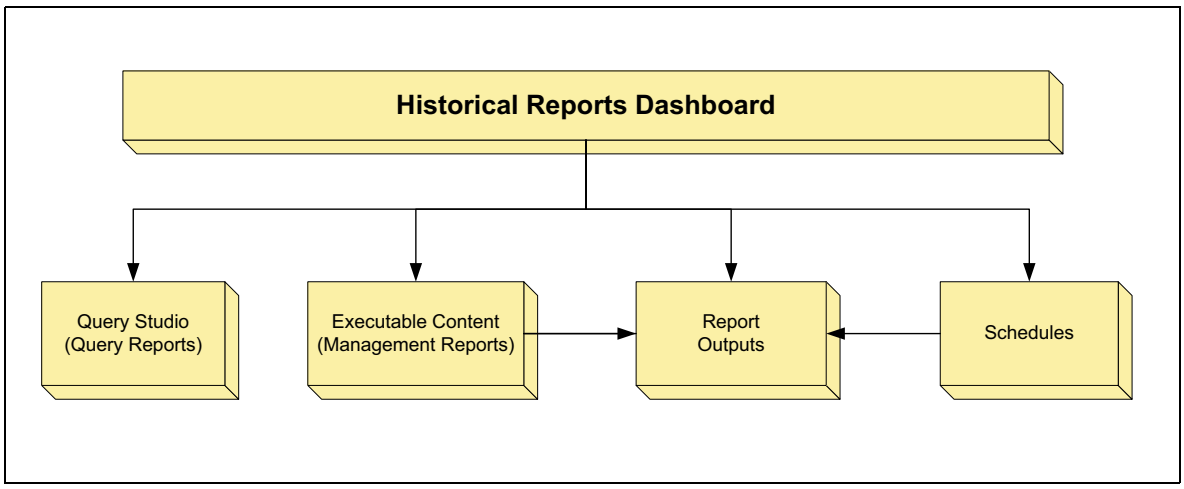

Figure 1.17 - IPI Reports User Interface

Management Reports User Interface Components

The following tabs are the key components of the Management Reports user interface:

- **Executable Content Tab**—This is the main Historical Reporting window. From here, you can configure and manage report profiles, schedule reports, and execute them. **Figure 1.18** shows a sample Executable Content tab.
- **Outputs Tab**—Reports can be saved in HTML, Portable Document Format (PDF), Microsoft Excel Spreadsheet (XLS), XML, and Character-Separated Values (CSV) formats and scheduled for automatic generation and distribution. The Outputs tab view enables you to manage report outputs that are scheduled for execution, are in the process of executing, or have finished executing.
- **Schedules Tab**—The Report Schedules window enables you to manage reports that are scheduled for execution. You can launch the Schedule wizard from the Executable Content tab, where you can schedule the report profiles and set the schedule date/time parameters.

Executable Content Tab Example

Figure 1.18 shows an example of an IPI Reports Executable Content tab. Before you execute a report profile, you must select a predefined report profile and click on the Edit Profile button to access the Profile Wizard. Then you must set up report filters and save the report. You can then select the new report profile and click the Execute button to generate the report. You can also define a report schedule by selecting a report and then clicking the Schedule button to access the Schedule Wizard. For details, see Reports Online Help.

From the left navigation pane, you can launch Query Studio in order to author Query Reports.

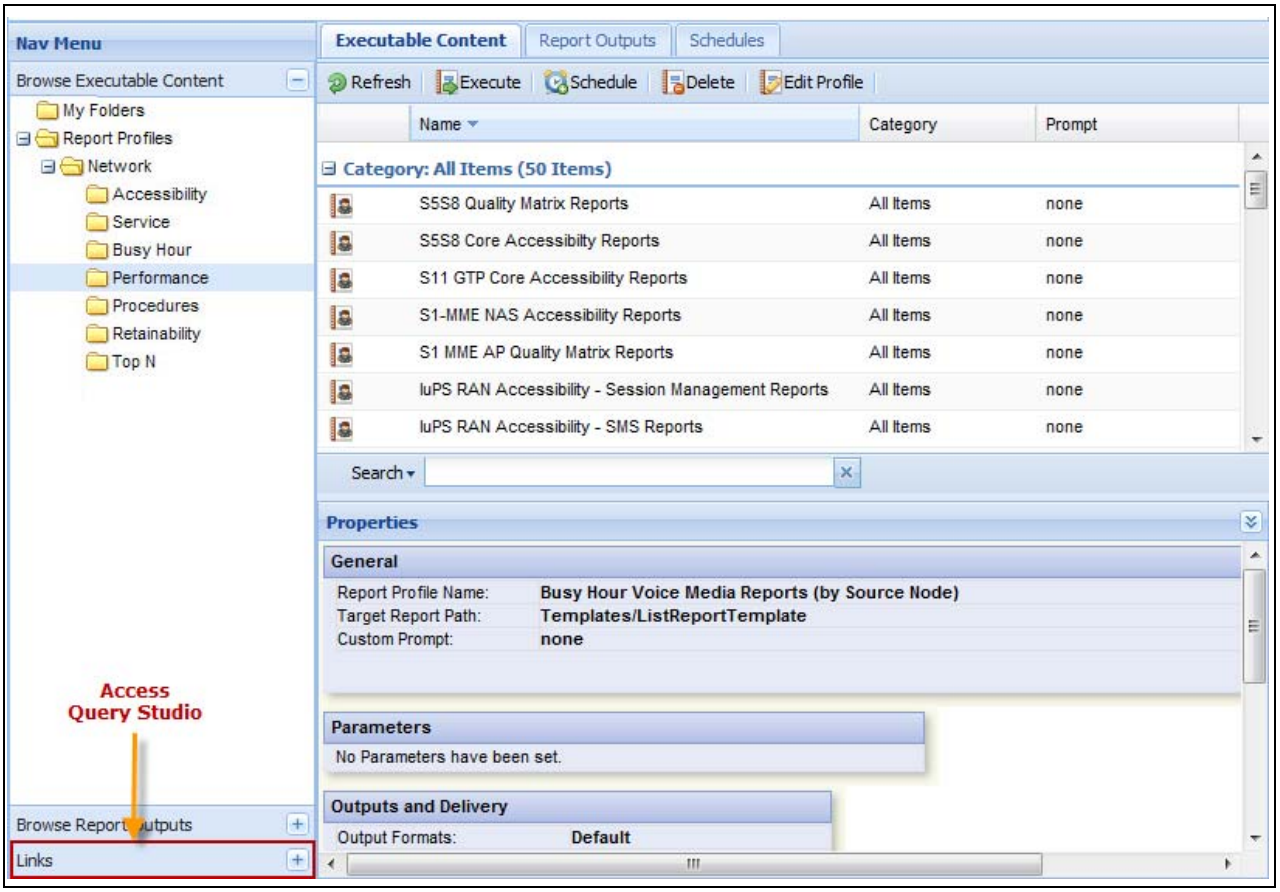

Figure 1.18 - IPI Reports—Executable Content Tab Example

Management Reports Workflow

The following steps describe a typical workflow for generating a Management Report on demand. For details, see Reports Online Help.

Step	Action
1.	From the Executable Reports tab, select one of the predefined report profiles in the list and then click **Edit Profile** to launch the Profile Wizard.
2.	In the wizard Parameters page, set up a time filter for the report data, and select dimensions and nodes for the report.
3.	Optionally, you can also change the default outputs and email delivery options.
4.	At this point, click **Save As** and save your report to My Folders. Then click **Run** to begin executing the report.
5.	From the Outputs tab, click **Refresh** to find the report you just started to run and monitor it as its status changes from Executing to Finished.
6.	To open the report in the Report Viewer, click **View**. From here, you can display the report in various formats and email it.

IPI Output Management Report Example

See **Figure 1.19** for an example IPI output Management Report using a Crosstab template and a predefined report profile.

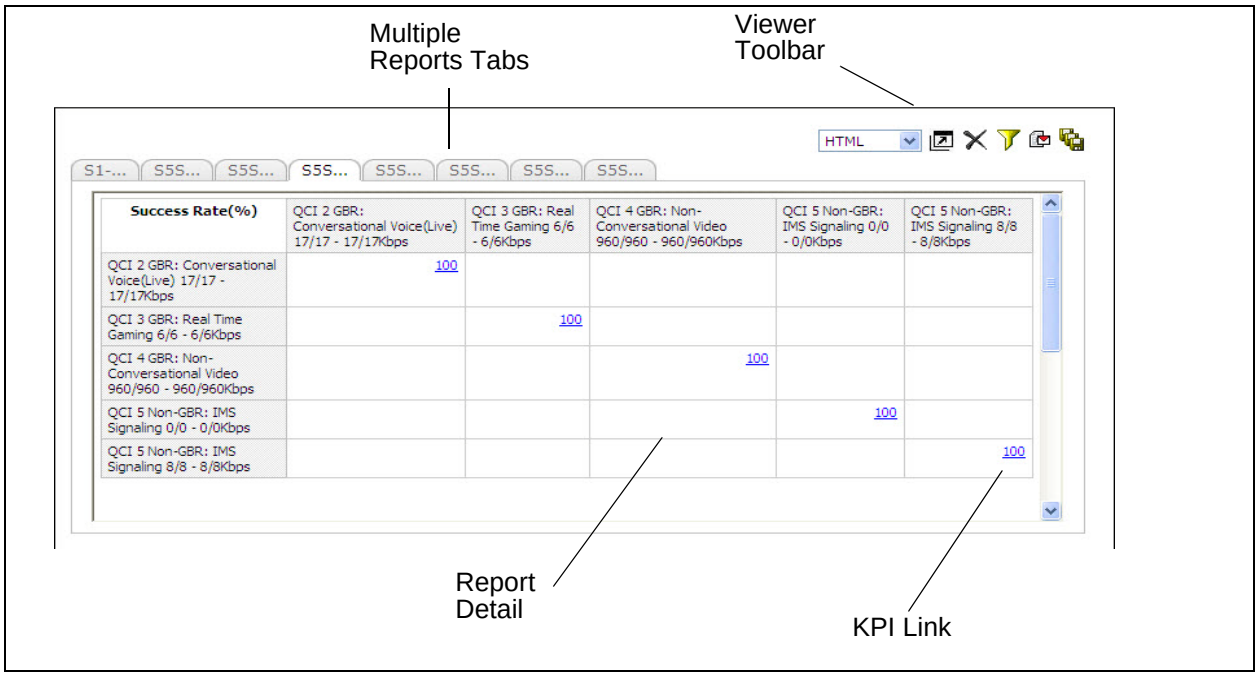

Figure 1.19 - IPI Output Management Report Example

Query Studio User Interface Components

The following are the key components of the Cognos Query Studio user interface, which are separate from the Management Reports components:

- **Main Window**—Select IPI KPIs and dimensions using drag and drop to build the query table, format the report, group data, define equations, and finally run the query.
- **Scheduler**—After defining a query, you can schedule it to run at a specified time.
- **My Folders**—Save Query Reports to the My Folder directory.
- **Email**—Send the link to a Query Report in an email.

Query Report Builder Example

Figure 1.20 shows the Query Studio main window, with LTE mobile data KPIs and dimensions. For a list of available parameters, see ***IPI Query Reports*** document in the Reports Online Help.

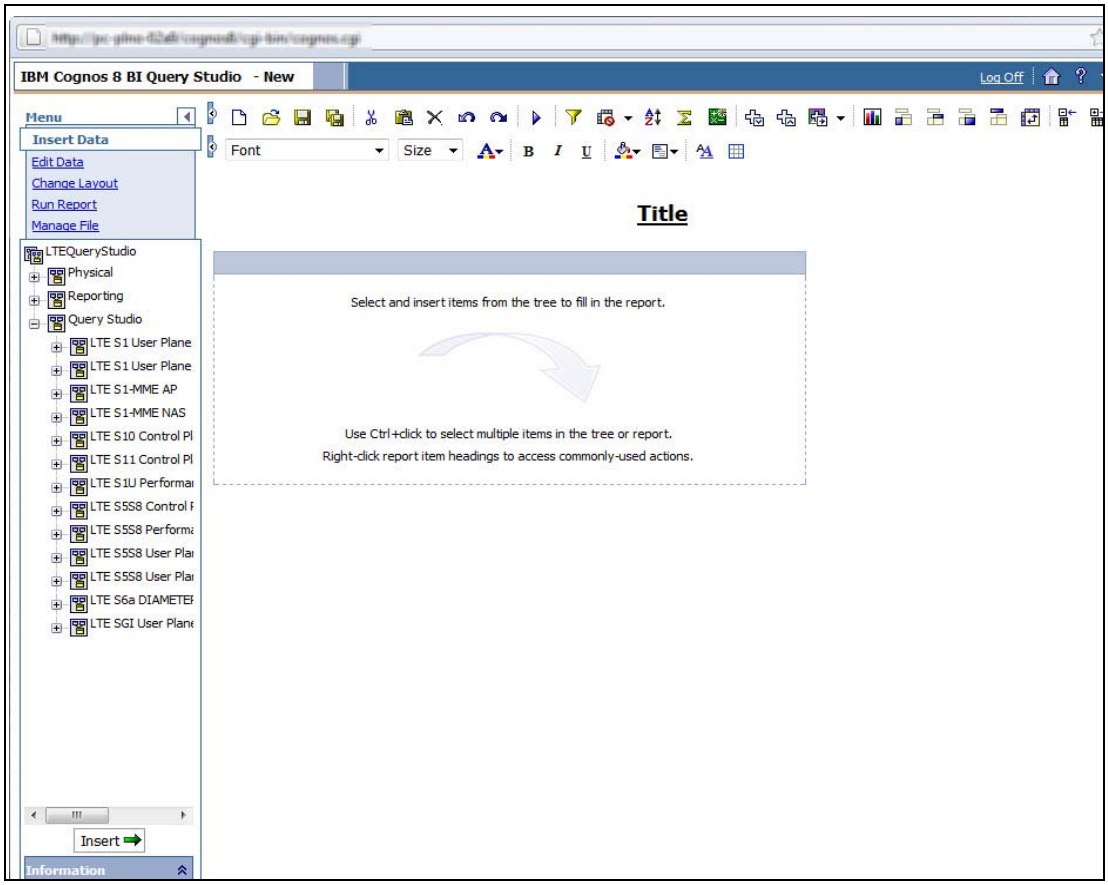

Figure 1.20 - IPI Query Reports—Query Builder Area

Query Reports Workflow

The following steps describe a typical workflow for generating a Query Report on demand. For details, see Iris Reports Online Help and Query Studio Online Help. For a list of available parameters, see ***IPI Query Reports*** document in the IPI Online Help.

Step	Action
1.	Click the **Historical Reports** button in the Iris toolbar to open the Management Reports main window.
2.	Click the **Links** accordion tab in the navigation pane to display the Query Reports folder, as shown in **Figure 1.18**.
3.	Click the **Query Reports** folder to display a packet selection dialog box, and then select one of the packets.
4.	Expand the IPI packets tree and navigate to the KPIs and dimensions you want to use in your query.
5.	Keep data collection OFF until you are ready to run the report.
6.	Drag and drop the elements you want to include in the report into the query builder area on the right.
7.	Format the report, define equations for KPIs, and group data as needed.
8.	When you are finished building and formatting the report, run the report with data collection ON.
9.	Save the report to the My Folders directory. You can also send an email with a link to the report.

IPI Query Report Example

See **Figure 1.21** for an example IPI query report. For a list of available KPIs and dimensions, see IPI Query Reports document in the IPI Online Help.

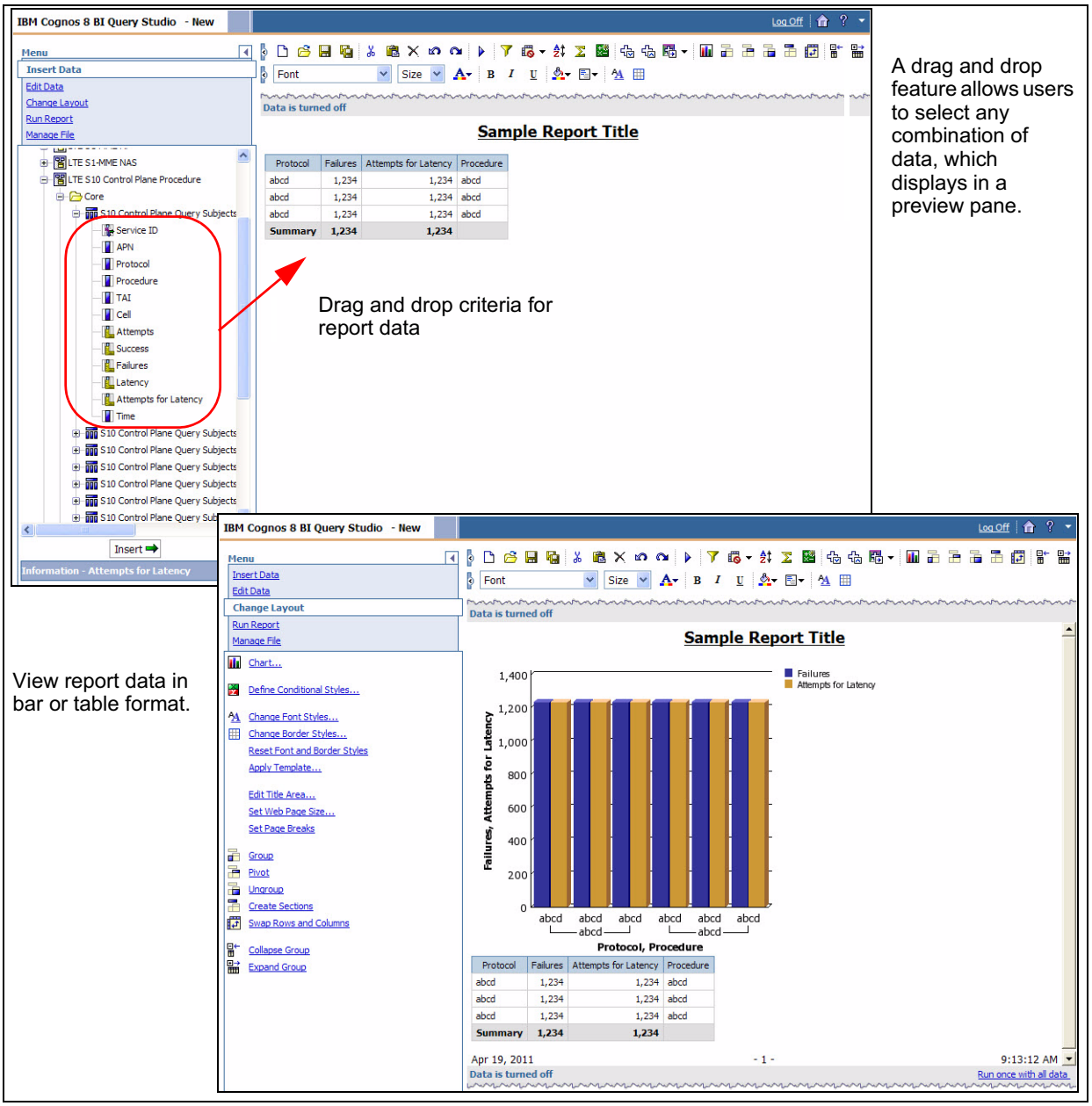

Figure 1.21 - IPI Output Report Example

ALARMS POLICY MANAGEMENT OVERVIEW

IPI alarms are managed through the IrisView Policy Management application, which uses policies to provide critical information to carriers on the performance of provisioned network elements. Alarm policies enable carriers to establish a set of guiding principles to manage KPI threshold configuration in order to optimize the performance of network elements.

Use the Alarm Dashboard to monitor alarms that will be triggered when the policy threshold is breached. IPI alarms of all types are visible in the dashboard.

Use FastPath to monitor and analyze alarms triggered by violations of service-based policies; all types of alarms, including Relative and Aggregate service-based alarms, are visible in FastPath.

Alarm Policy Functionality

Alarm policies are defined in the Policy Management user interface to provide the following functions:

- Evaluate threshold violations on complex combinations of KPIs and KQIs:
  - Users can define thresholds as fixed values (different thresholds for the same KPI) or relative to a point in time (negative or positive variation); they can also modify the alarm aggregation window
  - KPIs and KQIs can be combined in mathematical expressions as well in logical expressions
- Generate notifications:
  - Generate alarms to display in the Alarm dashboard; all types of service-based alarms, including relative threshold and aggregation window alarms, are also displayed in FastPath
  - Forward alarms to an external alarm management system via Simple Network Management Protocol (SNMP)
  - Generate email notification of the alarm
  - All uncleared IPI alarms are also visible in Iris Network Maps; from Network Maps you can drill down to the Alarms Dashboard.
- Profile Support
  - Users with the appropriate privileges can create alarm profiles to which you can assign alarm policies, schedules, actions, and users.
  - Users with the appropriate privileges can view users and their assigned profiles, and modify profile assignments per user.

Policy Management User Interface

All dimensions available for a specific KPI or KQI can be used to trigger an alarm. **Figure 1.22** shows the Alarms Policy Management user interface components.

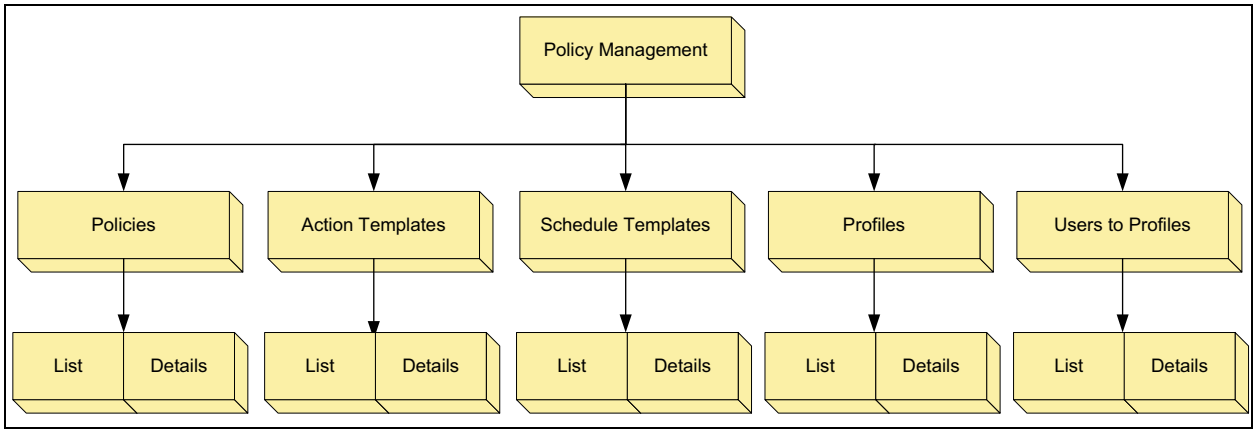

Figure 1.22 - Alarms Policy Management

Alarm Policies

The Policy window allows you to create new policies by defining conditions such as KPIs and dimensions, assigning them actions and schedules, and enabling them. For details, see Alarms Online Help.

Figure 1.23 shows an Alarm Policy example.

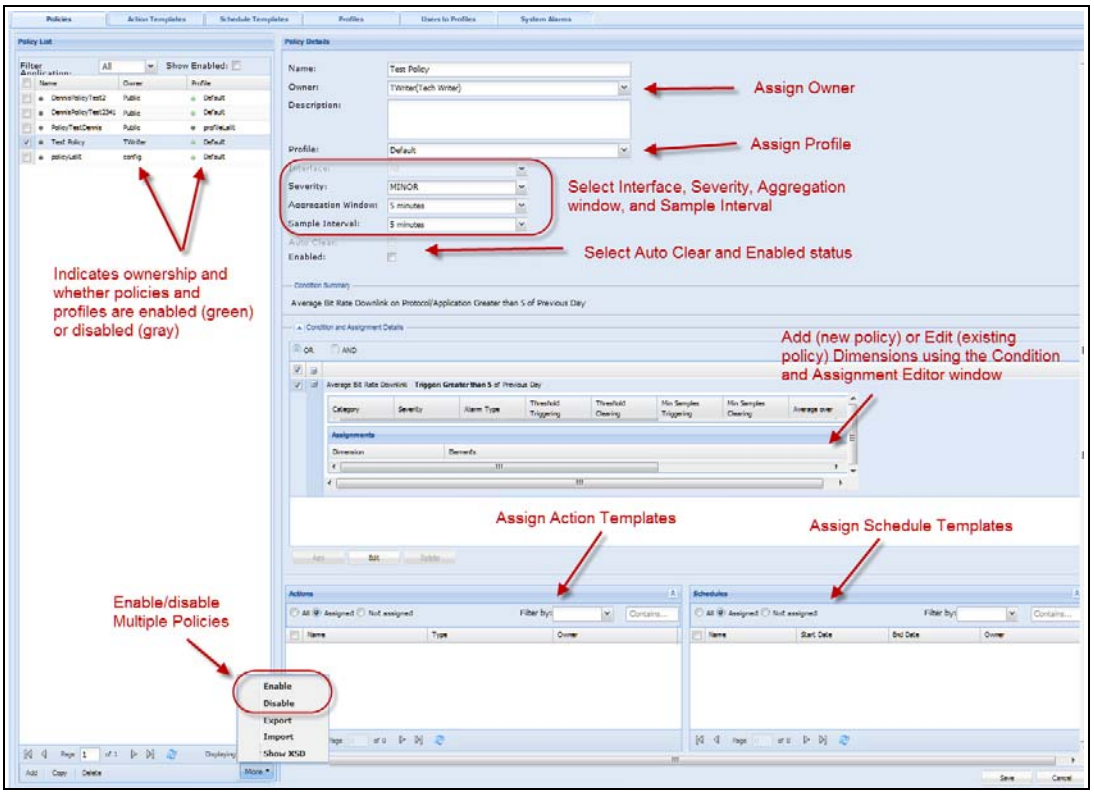

Figure 1.23 - Alarms Policy Example

A policy has a specific severity, interface, and conditions associated with it. When you create a new policy you give it a name and description to fully define it. You can view or edit the policy definition in the Policy Details pane. The Policies window includes options that enable you to perform the following functions:

- Status—Enable or disable an alarm policy. You can select the Show Enabled check box to display only active policies in the list.
- Conditions and Assignments—Using the Conditions and Assignment Editor window, you can define KPIs and thresholds and assign specific dimensions to a policy.
- Action—Configure the actions to take when an alarm is raised, based on a given policy. You can associate a policy with one or more actions: send an email, forward alarms using SNMP, or assign an Automated Controller Engine (ACE) action if you are using ACE. You define these actions in templates that you configure in the Action Templates window.
- Schedule—Assign schedule templates. You can create schedule templates to define specific time frames that you want alarm policies and alarm profiles to generate alarms. If a policy or profile is assigned a schedule template, its associated alarms are not generated for a threshold violation unless the violation occurs within the defined schedule times.

Policy Management Workflow

The following steps describe a typical workflow for creating and enabling alarm policies, and monitoring alarms triggered when policies are violated. For detailed instructions, see the Alarms and IPI Online Help.

Step	Action
1.	From the Iris toolbar open the Policy Management dashboard.
2.	Create a policy using the Policies tab and select IPI as the application. Provide a name, description, severity, aggregation window, and sample interval.
3.	Define an Interface or Service to associate with the policy; this setting will determine where you are able to monitor resulting alarms. You must choose "Service" for those alarms that you want to display in FastPath. Both Interface and Service alarms are visible in the Alarm Dashboard.
4.	Place a checkmark next to Enabled to enable the policy upon saving.
5.	Open the Conditions and Assignments Editor window by clicking the Add button. Create one or more conditions using IPI KPIs; make it a relative or absolute alarm type, assign logical operators and thresholds, and assign dimensions.
6.	For relative alarms, you can also specify averaging by indicating the number of periods to use in the calculation.
7.	When you are finished adding all KPIs and dimensions, click Save to return to the Policy page.
8.	If you want to assign actions to be taken when an alarm is raised, including sending an email, forwarding to SNMP, or performing an ACE action, you can configure these actions in the Actions template. In the Actions area, select to display All of the Action templates, only the Assigned Action templates, or only the Unassigned Action templates.
9.	Select the Action template you want to assign to this policy.
10.	In the Schedules area, select to display All of the Schedule templates, only the Assigned Schedule templates, or only the Unassigned Schedule templates.
11.	Select the Schedule template you want to assign to this policy.
12.	Save the policy.

2 IPI Best Practices

This chapter includes use cases targeted at specific organizations. The procedures in this chapter provide a high-level view of how to use the IPI application for analyzing and troubleshooting certain network scenarios; refer to the Iris Online Help for detailed procedures for using the IPI application components.

IPI Use Cases

This section includes use cases targeted at specific organizations: Engineering / Planning and Operations.

Engineering/Planning Use Cases

The following use cases show how IPI can help the Engineering / Planning organization analyze their network.

- Improve Network Optimization and Expansion
- Manage User Predictability

Improve Network Optimization and Expansion

Engineering and Planning teams can use IPI to improve forecast accuracy in the context of network optimization and expansion. IPI can help them anticipate the changes required to a network to support traffic growth patterns and new differentiated services. Engineers can refine network configuration over time based on changes in demand and traffic patterns.

Step	Action
1.	Monitor and analyze network traffic KPIs in dashboards and analysis reports, looking for trends in network traffic increases over weeks and months.
2.	Configure policies on specific network traffic KPIs of interest, setting maximum thresholds and different severity.

Manage User Predictability

User mobility affects quality of service and makes capacity planning more difficult. IPI applications can help Engineering and Planning teams improve in the following areas when managing wireless networks:

- Understand user mobility patterns
- Understand network traffic usage characterization
- Analyze application usage and KPIs to understand which applications users are accessing most often and when.

Operations Use Cases

The following use cases show how IPI can help the Operations organization troubleshoot and monitor issues within their network.

- Troubleshoot Incorrect APN Configuration
- Resolve MMS Transmission Issues
- Monitor Call Setup Failure
- Monitor Calls Dropped
- Troubleshoot Incorrect DNS Configuration
- Monitor Issues with New Handset
- Monitor Quality of Voice Calls

Troubleshoot Incorrect APN Configuration

Incorrect APN configuration can cause performance issues resulting in high PDP Ctx creation failures. Operations would like to be notified of such failing Access Point Networks (APN) in order to troubleshoot the issue.

Step	Action
1.	Configure a policy on Create PDP Ctx Failure rate on APN dimension in the Network base service.
2.	Monitor the status of the alarms in FastPath.
3.	Drill down on the alarms to see which APNs are problematic.
4.	Drill down to data record (DR) log and Iris Session Analyzer (ISA) to identify the issue.

Resolve MMS Transmission Issues

When Multimedia Messaging Service (MMS) cannot be sent by some handsets, Operations need to resolve the issue because it impacts revenue.

Step	Action
1.	Configure a policy on MMS Submit Failure Rate on Handset dimension for MMS.
2.	Monitor the status of the alarms in FastPath.
3.	Drill down on the alarms to see which handsets are problematic.
4.	Drill to DR log and ISA to further isolate the issue.

Monitor Call Setup Failure

Voice calls failing to setup is a big revenue-impacting issue. Operations need to monitor where the issues are occurring most often in order to quickly resolve them.

Step	Action
1.	Configure a policy on Call Setup Failure Rate on Source Node dimension for Network service.
2.	Monitor the status of the alarms in FastPath.
3.	Drill down on the alarms to see which Nodes are problematic.
4.	Drill to DR log and ISA to identify the issue.

Monitor Calls Dropped

Voice calls being dropped is a big revenue-impacting issue. Operations need to monitor where the issues are occurring most often in order to quickly resolve them.

Step	Action
1.	Configure a policy on Call Drop Rate on Source Node and Destination dimensions for Network service.
2.	Monitor the status of the alarms in FastPath.
3.	Drill down on the alarms to see which Nodes are problematic.
4.	Drill to DR log and ISA to identify the issue.

Troubleshoot Incorrect DNS Configuration

When incorrect DNS configuration impacts the users experience, Operations needs to resolve the issue because it impacts revenue.

Step	Action
1.	Configure a policy on DNS Query Failure Rate on AppServer dimension for Network service.
2.	Monitor the status of the alarms in FastPath.
3.	Drill down on the alarms to see which Handsets are problematic.
4.	Drill down to DR log and ISA to identify the issue.

Monitor Issues with New Handset

When a new handset has been delivered, Operations needs to monitor the usage and any issues related to the new handset.

Step	Action
1.	You can either create a policy on the “Network” service for handset types or create a new service for handset types focusing on a subset of interfaces and KPIs. Contact your administrator regarding creating a new service.
2.	Configure policies using the following KPIs: ▪ PDP Context Create Success Rate ▪ TCP Connection Success Rate ▪ E2E Delay

- Throughput

3. Monitor the status of the alarms in FastPath.

Monitor Quality of Voice Calls

Poor voice call quality can cause users to terminate the call earlier than needed, which can cause an increase in churn. Poor call quality and churn are both revenue-impacting issues. Operations needs to monitor where the issues are occurring most often in order to quickly resolve them.

Step	Action
1.	Configure a policy on MOS and R-Factor KPIs on Source Node dimension for Network service.
2.	Monitor the status of the alarms in FastPath.
3.	Drill down on the alarms to see which Nodes are problematic.
4.	Drill to DR log and ISA to nail down the issue.