



Service Control Application Suite for Broadband

User Guide

VER. 2.5.5

OL-138635

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-138635=
Text Part Number: OL-138635-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

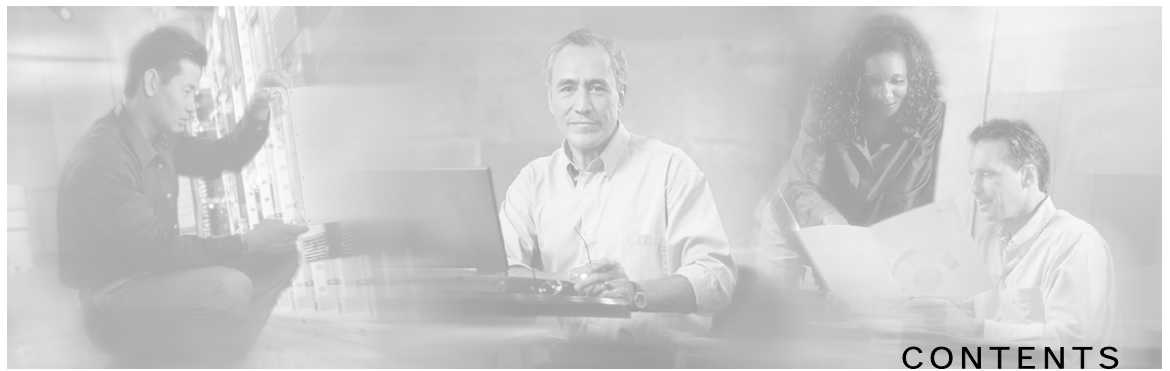
CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

Service Control Application Suite for Broadband User Guide ver. 2.5.5

Copyright © 2002-2005 Cisco Systems, Inc.
All rights reserved.



Introduction xi

- Audience xi
- Purpose xi
- Document Content xii
- Document Conventions xii
- Related Publications xiii
- Obtaining Technical Assistance xiii
 - Cisco TAC Website xiii
 - Opening a TAC Case xiv
 - TAC Case Priority Definitions xiv

Overview 1-1

- The Cisco Service Control Concept 1-1
 - Service Control Application Suite for Broadband - Service Control for Broadband Service Providers 1-2
- Service Control Capabilities 1-2
- The SCE Platform 1-3
- Management and Collection 1-4
 - Network Management 1-5
 - Subscriber Management 1-6
 - Collection 1-6
- Service Configuration Management 1-6

System Overview 2-1

- System Components 2-1
- Subscribers and Subscriber-Modes 2-3
 - Subscriber-less mode 2-3
 - Anonymous subscriber-mode 2-4
 - Static Subscriber Mode 2-4
 - Subscriber-aware mode – Dynamic Subscribers 2-4

- Subscriber Modes – Summary 2-5
- Service Configuration 2-5
 - SCAS BB Console 2-6
 - Service Configuration Utility 2-6
 - Service Configuration API 2-7

Running the SCAS BB Console 3-1

- The SCAS BB Console 3-2
 - Menu Bar and Toolbar 3-2
 - Network Traffic/Services Band 3-5
 - Message Band 3-9
 - Status Bar 3-9
- Opening the SCAS BB Console 3-10
- Closing the SCAS BB Console 3-11

Managing Service Configurations 4-1

- Applying and Retrieving Service Configurations 4-1
 - Applying a Service Configuration 4-2
 - Retrieving the Current Service Configuration 4-3
 - Using the Service Configuration Utility 4-4
- Creating a New Service Configuration 4-6
- Saving the Current Service Configuration 4-8
- Validating the Current Service Configuration 4-9
- Opening an Existing Service Configuration 4-10
- Exporting Packages, Services, Protocols and Lists 4-11
- Importing Packages, Services, Protocols or Lists 4-12
- Accessing the SCAS Reporter 4-13
- Accessing the SCAS BB SM GUI 4-13
- SCAS BB Licenses 4-13

Constructing Service Configurations 5-1

- Service Configuration Overview 5-2
 - The Service Hierarchy 5-2
 - The Package Hierarchy 5-3
 - Packages and Services 5-5

Traffic Classification	5-6
Constructing and Modifying Services	5-6
Defining Service Elements for Services	5-11
Managing Protocols	5-17
Managing Lists	5-26
Traffic Control	5-30
Overview of Bandwidth Control	5-30
Global Control	5-30
Subscriber Bandwidth Control	5-31
Defining the Global Controllers	5-33
Packages	5-40
Constructing Packages	5-41
Assigning Services to Packages	5-53
Unknown Subscribers Traffic	5-67
Weekly Time-Frames	5-68
Managing Calendars	5-68
Configuring Weekly Time-Frames	5-70
Bandwidth Control Revisited	5-72
Managing RDR Settings	5-75
Using the Usage RDRs Tab (RDR Settings)	5-76
Using the Transaction Usage RDRs Tab (RDR Settings)	5-78
Using the Log RDRs Tab (RDR Settings)	5-79
Using the Traffic Discovery Tab (RDR Settings)	5-81
Using the Quota RDRs Tab (RDR Settings)	5-82
Using the Realtime RDRs Tab (RDR Settings)	5-84
Subscriber Notification	5-85
Filtering the Traffic Flows	5-89
Constructing a Filter Rule	5-89
Adding a Filter Rule	5-89
Editing a Filter Rule	5-95
Removing a Filter Rule	5-96
Activating a Filter Rule	5-97
Deactivating a Filter Rule	5-97

Managing the System Settings 6-1

- Understanding the System Settings 6-1
 - Configuring the System Mode Parameter 6-1
 - Setting Redirection Parameters 6-3
 - Setting Ongoing Policy Check Parameters 6-7
 - Setting P2P Detection Parameters 6-8
 - Setting BW Management Parameters 6-9
- Dynamic Signature Management 6-10
- Attack Filtering and Subscriber Notification 6-13
 - Subscriber Notification on Network Attack 6-13

Managing Subscribers 7-1

- Introducing the SCAS BB SM GUI 7-2
 - Accessing the SCAS BB SM GUI 7-2
 - Connecting and Disconnecting 7-4
 - Exiting the SCAS BB SM GUI 7-5
 - The SM GUI Main Window 7-5
- Working with Individual Subscribers 7-8
 - Locating and Selecting Subscribers 7-8
 - Adding a Subscriber 7-9
 - Editing Subscribers 7-12
 - Removing Subscribers 7-15
- Working with Subscriber csv Files 7-15
 - Importing Subscriber Files 7-15
 - Exporting Subscriber Files 7-17
- Managing Subscribers via Other System Components 7-18
 - Anonymous-Subscriber Mode 7-18
 - Subscriber-Aware Mode 7-19
 - Managing Real-time Subscriber Usage RDRs 7-21
 - Managing csv Files 7-23

Generating Reports 8-1

- Introducing the SCAS Reporter 8-1
 - Accessing the SCAS Reporter 8-2
 - Exiting the Reporter 8-3

- The Reporter Main Screen 8-4
- The Reports Wizard 8-5
- Defining the Report 8-6
 - Creating a New Report Definition 8-7
 - Generating a Report 8-17
 - Duplicating an Existing Report Definition 8-17
 - Modifying an Existing Report Definition 8-17
 - Renaming an Existing Report Definition 8-18
 - Deleting a Report Definition 8-18
- Working with Reports 8-19
 - Report Options 8-19
 - Viewing Reports 8-20
 - Editing a Chart 8-21
 - Generating a New Report 8-22
 - Refreshing the Report 8-23
 - Printing Reports 8-23
 - Exporting Reports 8-23

SCAS Reporter Templates A-1

- Overview of Report Templates A-1
 - Monitoring Reports A-3
 - Traffic Discovery Reports A-6
- Global Monitoring A-7
 - Global Bandwidth per Service A-8
 - Global Hourly Usage Sessions per Service A-8
 - Global Daily Usage Sessions per Service A-8
 - Global Hourly Usage Volume per Service A-9
 - Global Daily Usage Volume per Service A-9
 - Global Aggregated Usage Volume per Service A-9
 - Daily Peak BW for All Packages A-10
 - Global Hourly Aggregated Minutes per Service A-10
 - Global Concurrent Session per Service A-10
- Package Monitoring A-11
 - Package Bandwidth per Service A-11

- Package Hourly Usage Sessions per Service A-11
- Package Daily Usage Sessions per Service A-11
- Package Hourly Usage Volume per Service A-12
- Package Daily Usage Volume per Service A-12
- Daily Peak BW per Package A-12
- Package Aggregated Usage Volume per Service A-13
- Package Hourly Aggregated Minutes per Service A-13
- Package Concurrent Session per Service A-13
- Subscriber Monitoring A-14
 - Subscriber Bandwidth per Service Counter A-14
 - Subscriber Hourly Usage Volume per Service A-14
 - Subscriber Daily Usage Volume per Service A-14
 - Top Subscribers A-15
 - Subscriber Hourly Usage Sessions per Service A-15
 - Subscriber Daily Usage Sessions per Service A-16
 - Subscriber Aggregated Usage Volume per Service A-16
 - Daily Peak BW for Specific Subscriber A-16
 - Subscriber Hourly Aggregated Minutes per Service A-17
- Traffic Discovery - Statistics A-17
 - Top IP Protocol A-17
 - Top Servers A-18
 - Top Servers TCP Ports A-18
 - Top Servers UDP Ports A-19
 - Top Client A-19
 - Top Client IP To Server TCP Port A-20
 - Top Client IP To Server UDP Port A-20
 - Top Client IP to Server IP A-21
 - Top Server IP and Server TCP Port A-21
 - Top Client IP and Server UDP Port A-22
 - Top Client IP to Server IP and Server TCP Port A-22
 - Top Client IP to Server IP and Server UDP Port A-23
 - Top Signature-Based Protocols A-23
 - Top Service TCP Ports A-24
 - Top Service UDP Ports A-25

Web and Streaming Reports A-25
Top Web Hosts A-25
Top HTTP Streaming Hosts A-26
Top RTSP Hosts A-27
Top MMS Servers A-27
Top FTP Servers A-28
Top Service Servers A-28
Streaming Host Distribution by Subscriber Packages A-29
RTSP Host Distribution by Subscriber Packages A-29
MMS Server Distribution by Subscriber Packages A-30
FTP Server Distribution by Subscriber Packages A-30
Service Distribution by Subscriber Packages A-31
Email and News Reports A-31
Top SMTP Servers A-32
Top POP3 Servers A-32
Top NNTP Servers A-33
Top E-mail Senders A-33
Top E-mail Recipients A-34
Top E-mail Account Owners A-34
Top Newsgroups A-35
Top Subscriber to Newsgroup A-35
Top NNTP Consumers A-36
SMTP Server Distribution by Subscriber Packages A-36
POP3 Server Distribution by Subscriber Packages A-37
NNTP Server Distribution by Subscriber Packages A-37
P2P Reports A-38
Top P2P Consumers A-38
Top P2P Downloaders A-38
Top P2P Uploaders A-39
Top P2P Protocols A-39
Top P2P Protocols A-40
VoIP Reports A-40
Global Bandwidth per VoIP Service A-40
Global Hourly Call Minutes per VoIP Service A-41

- Package Bandwidth per VoIP Service A-41
- Package Hourly Call Minutes per VoIP Service A-41
- Subscriber Bandwidth per VoIP Service A-42
- Subscriber Hourly Call Minutes per VoIP Service A-42
- Global Concurrent Calls per VoIP Service A-42
- Packet Concurrent Calls per VoIP Service A-43
- Top SIP Domains A-43
- Top Talkers A-44

Demographic Data and Service Popularity Reports A-44

- Global Active Subscriber per Service A-44
- Service Popularity among Subscribers A-45
- Package Active Subscriber per Service A-45
- Service Popularity among Subscribers of a Specific Package A-46
- Service Popularity among Subscribers of a Specific Package A-46
- Service Popularity among Subscribers of a Specific Package A-47
- Relative Consumption Consumptions of Top Subscribers A-47

Malicious Traffic Reports A-47

- Global Scan/Attack Rate A-48
- Global DoS Rate A-48
- Top Scanning/Attacking Hosts A-48
- Top Scanning/Attacking Hosts A-48
- Top DoS Attacked Hosts A-49
- Top Scanning/Attacking Hosts A-49
- Infected Subscribers A-49
- DoS Attacked Subscribers A-49

Protocol Reference Tables B-1

- Generic Protocols B-1
- Signature-based Protocols B-1
- IP Protocols B-3
- Port-Based Protocols B-7

RDR Format and Field Content C-1

- Universal RDR Fields C-1
- Transaction RDR C-2

Transaction Usage RDR C-4
VoIP Transaction Usage RDR C-5
Subscriber Usage RDR C-8
Real-time Subscriber Usage RDR C-9
Link Usage RDR C-11
Package Usage RDR C-13
Blocking RDR C-15
Quota Provision RDR C-16
Remaining Quota RDR C-17
Threshold Breach RDR C-18
DHCP RDR C-19
QOS Request RDR C-20
QOS Delete RDR C-21
Malicious Traffic Periodic RDR C-22
RDR Enumeration Fields C-23
Block Reason (uint8) C-23
PROTOCOL_ID (int16) C-24
Aggregation Period (uint8) C-25
Time Frames (uint16) C-26
RDR Tag Assignment Summary C-26
Periodic RDR Zero Adjustment Mechanism C-27

Database Tables D-1

Overview D-1
Database Tables D-1
Table RPT_SUR D-2
Table RPT_PUR D-2
Table RPT_LUR D-3
Table RPT_TR D-3
Table RPT_MALUR D-4
Table RPT_TOPS_PERIOD0 D-5
Table RPT_TOPS_PERIOD1 D-5
Table VALUES_INI_ENG D-6
Table INI_VALUES D-6

Glossary of Terms 1

Index 1



Introduction

This guide contains comprehensive instructions for using the Service Control Application Suite for Broadband solution, including the three **SCAS BB** front ends:

- SCAS BB Console
- **SCAS BB** Subscriber Manager GUI
- SCAS Reporter

This guide assumes a basic familiarity with the concept of the Service Control solution, the SCE Platforms, and related components.

Audience

This guide is intended for the administrator who will be responsible for daily operation of the solution, utilizing the many features of the SCAS BB Console, **SCAS BB** Subscriber Manager, and SCAS Reporter front ends to gain visibility into, and control over, the distribution of network resources.

Purpose

The *Service Control Application Suite for Broadband User Guide* documents all features of the application in detail. It describes all three front ends. It also explains which features of the system are only available to **SCAS BB** Capacity Control or **SCAS BB** Tiered Control users.

Document Content

Chapter 1: *Overview* provides a brief overview of the Service Control solution in general, as well as an introduction to the Service Control Application Suite for Broadband solution.

Chapter 2: *System Overview* describes the components of the system and explains some basic concepts.

Chapter 3: *Running the SCAS BB Console* describes the main features of the SCAS BB Console. It also explains how to access the SCAS BB Console.

Chapter 4: *Managing Service Configurations* describes how to apply and retrieve a Service Configuration using either the SCAS BB Console or the Service Configuration Utility, as well as how to open, create, and save a Service Configuration. It also explains how to export package, service, protocol, or list definitions.

Chapter 5: *Constructing Service Configurations* explains how to construct a Service Configuration that will give you the network visibility and control that you need.

Chapter 6: *Managing the System Settings* provides detailed explanations and procedures for the configuring the System Settings, importing dynamic signatures, and configuring attack filtering settings.

Chapter 7: *Managing Subscribers* describes the **SCAS BB** Subscriber Manager GUI, as well as other interfaces for managing subscribers via the SCE Platform or the smartSUB Manager.

Chapter 8: *Generating Reports* describes the SCAS Reporter and options available for this front end.

Appendix A: *SCAS Reporter Templates* describes the template groups and query fields for the different categories of Reporter Templates.

Appendix B: *Protocol Reference Tables* presents tables of protocols that are supported by **SCAS BB** traffic classification.

Appendix C: *RDR Format and Field Content* lists the various RDRs produced by the SCE Platform and gives their structure, describes the columns and fields of each RDR, and states under what conditions each kind of RDR is generated. It also provides field-content information for fields generated by Service Control components (such as tags), and a description of the Periodic RDR Zero Adjustment Mechanism.





Appendix D: *Database Tables* presents the different database tables used for storing RDRs (after their conversion by an Adapter), and a description of the table columns (field names and types).

Glossary: Brief description of terms used throughout this guide.

Document Conventions

The following typographic conventions are used in this guide:

Typeface or Symbol	Meaning
<i>Italics</i>	References, new terms, field names, and placeholders.
Bold	Names of menus, options, and command buttons.
Courier	System output shown on the computer screen in the Telnet session.

Typeface or Symbol	Meaning
Courier Bold	CLI code typed in by the user in examples.
<i>Courier Italic</i>	Required parameters for CLI code.
[<i>italic in brackets</i>]	Optional parameters for CLI code.
	Note.
	Notes contain important information.
	Warning.
	Warning means danger of bodily injury or of damage to equipment.

The CLI commands are written in the following format:

command *RequiredParameter* **constant** [*optional-parameter*]

[no] is an optional parameter that may appear before the command name.

When typing commands, you may enclose parameters in double-quote marks, and you *must* do so when there is a space or a question mark within a parameter name.

Examples are shown in courier style. **Bold courier** is used to show the commands as you type them and regular courier is used for system prompts and responses.

Related Publications

The Service Control Application Suite for Broadband *User Guide* should be used in conjunction with the *Service Control Application Suite for Broadband Installation Guide*. The *Service Control Application Suite for Broadband API Programmer's Guide*, the SCE Platform user guides (*SCE 1000/SCE 2000 User Guides*), the *smartSUB Manager User Guide* and the *Collection Manager User Guide* may also be useful.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac> (<http://www.cisco.com/tac>)) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do> (<http://tools.cisco.com/RPF/register/register.do>)

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution.

If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

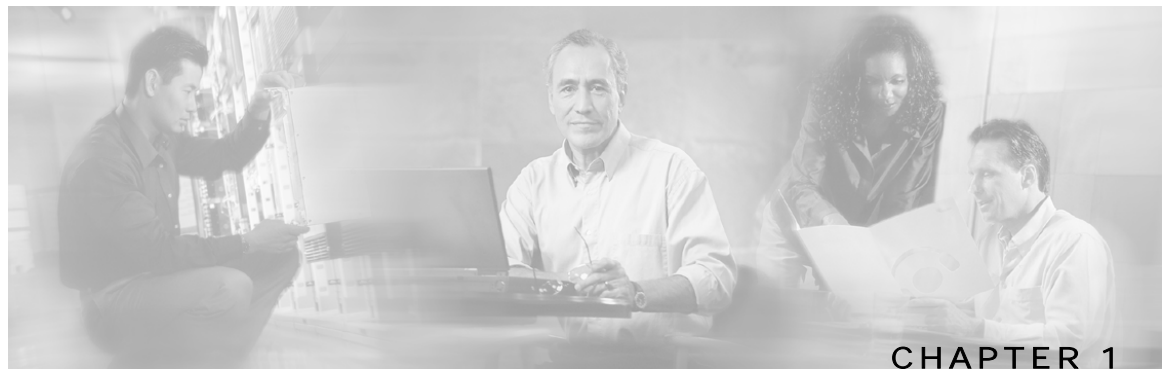
For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
(<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>)

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

- **Priority 1 (P1)**—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
- **Priority 2 (P2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- **Priority 3 (P3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
- **Priority 4 (P4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.



Overview

This chapter provides a general overview of the Cisco Service Control solution. It introduces the Cisco Service Control concept and the Service Control capabilities. It also briefly describes the hardware capabilities of the SCE Platform, as well as the Cisco specific applications that together compose the total Cisco Service Control solution.

This chapter contains the following sections:

- [The Cisco Service Control Concept](#) 1-1
- [Service Control Capabilities](#) 1-2
- [The SCE Platform](#) 1-3
- [Management and Collection](#) 1-4
- [Service Configuration Management](#) 1-6

The Cisco Service Control Concept

The Cisco Service Control concept is delivered through a combination of purpose-built hardware and specific software solutions that address various Service Control challenges faced by service providers. The SCE Platform is designed to support observation, analysis, and control of Internet/IP traffic.

Service Control enables service providers to create profitable new revenue streams while capitalizing on their existing infrastructure. With the power of Service Control, service providers have the ability to analyze, charge for, and control IP network traffic at multi-Gigabit wire line speeds. The Cisco Service Control solution also gives service providers the tools they need to identify and target high-margin, content-based services.

As the downturn in the telecommunications industry has shown, IP service provider business models need to be reworked in order to make them profitable. Having spent billions of dollars to build ever larger data links, providers have incurred massive debts and rising costs. During the same time, access and bandwidth became a commodity where prices continually fell and profits disappeared. Service providers now realize that they must offer value-added services to derive more revenue from the traffic and services running on their networks. However, capturing real profits from IP services requires more than simply running those services over data links; it requires detailed monitoring and precision, real-time control and awareness of services as they are delivered. Cisco provides Service Control solutions that allow the service provider to bridge this gap.

Service Control Application Suite for Broadband - Service Control for Broadband Service Providers

Service providers of wireline broadband access (DSL, Cable) targeting residential and business consumers must find new ways to get maximum leverage from their existing infrastructures, while differentiating their offerings with enhanced IP services.

Service Control Application Suite for Broadband adds a new layer of service intelligence and control to existing networks that can:

- Report and analyze network traffic at subscriber and aggregate level for capacity planning
- Provide customer-intuitive tiered application services and guarantee application SLAs
- Implement different service levels for different types of customers, content, or applications
- Identify network abusers who are violating the Acceptable Use Policy
- Identify and manage peer-to-peer, NNTP (news) traffic, and spam abusers
- Enforce the Acceptable Use Policy (AUP)
- Integrate Service Control solutions easily with existing network elements and BSS/ OSS systems

Service Control Capabilities

At the core of the Cisco Service Control Platform stands the purpose-built network hardware device: the Service Control Engine (SCE). Implementing a complete Service Control solution requires that the Service Control Engine provide certain functionalities and capabilities. The following are the core capabilities of the Cisco Service Control Engine, which support a wide range of applications for delivering Service Control solutions:

- Subscriber and application awareness: Application-level drilling into IP traffic for real-time understanding and controlling of usage and content at the granularity of a specific subscriber.
 - Subscriber awareness: The ability to map between IP flows and a specific subscriber for maintaining the state of each subscriber transmitting traffic through the platform, and enforcing the appropriate policy on this subscriber traffic.

Subscriber awareness is achieved using dedicated integrations with subscriber management repositories, such as a DHCP or a Radius server.

- Application awareness: The ability to understand and analyze traffic up to the application protocol layer (Layer 7).

For an application protocol that is implemented using bundled flows (such as FTP, which is implemented using Control and Data flows), the SCE Platform understands the bundling connection between the flows and treats them accordingly.

- Stateful, real time traffic control: The ability to perform advanced control functions, including granular BW metering and shaping, quota management and redirection, utilizing stateful real-time traffic transaction processing. This requires highly adaptive protocol and application level intelligence.
- Programmability: The ability to quickly add new protocols and easily adapt to new services and applications in the ever-changing service provider environment. Programmability is achieved using the SML language.

Programmability means that new services can be deployed quickly and provides an easy upgrade path for network, application, or service growth.

- **Robust and flexible back office integration:** The ability to integrate with existing 3rd party systems at the Service Provider, such as provisioning systems, subscriber repositories, billing systems, and OSS systems. The Service Control Engine provides a set of open and well-documented APIs that allows a quick and robust integration process.
- **Scalable High-Performance Service Engines:** The ability to execute all operations described above at wire speed.

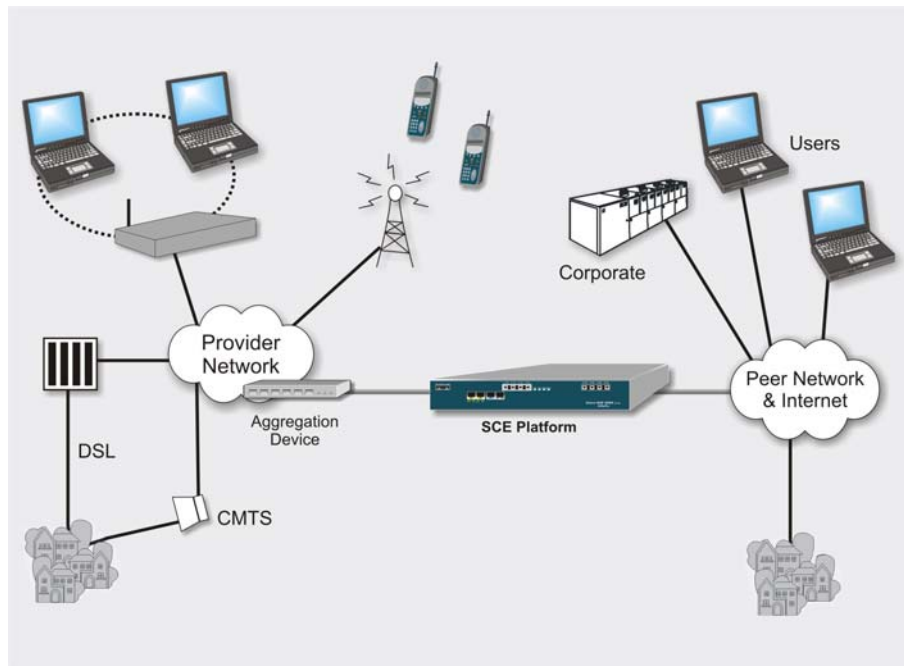
The SCE Platform

The Service Control Engine family of programmable network devices is capable of performing stateful flow inspection of IP traffic, and controlling that traffic based on configurable rules. The Service Control Engine is a purpose-built network device making use of ASIC components and RISC processors to go beyond packet counting and delve deeper into the contents of network traffic. Providing programmable, stateful inspection of bi-direction traffic flows and mapping these flows with user ownership, the Service Control Engine platforms provide a real-time classification of network usage. This information provides the basis of the Service Control Engine advanced traffic control and bandwidth shaping functionality. Where most bandwidth shaper functionality ends, the Service Control Engine provides more control and shaping options including:

- Layer 7-3 stateful wire-speed packet inspection and classification
- Robust support for over 600 protocol/applications including:
 - General: HTTP, HTTPS, FTP, TELNET, NNTP, SMTP, POP3, IMAP, WAP, and others
 - P2P: FastTrack-KazaA, Gnutella, WinMX, Winny, Hotline, eDonkey, DirectConnect, Piolet, and others
- Streaming & Multimedia: RTSP, SIP, HTTP-STREAMING, RTP/RTCP, and others
- Programmable system core for flexible reporting and bandwidth control
- Transparent network and BSS/OSS integration into existing networks
- Subscriber awareness for relating traffic and usage to specific customers

The following diagram demonstrates a deployment of an SCE Platform in the network.

Figure 1-1: SCE Platform in the Network



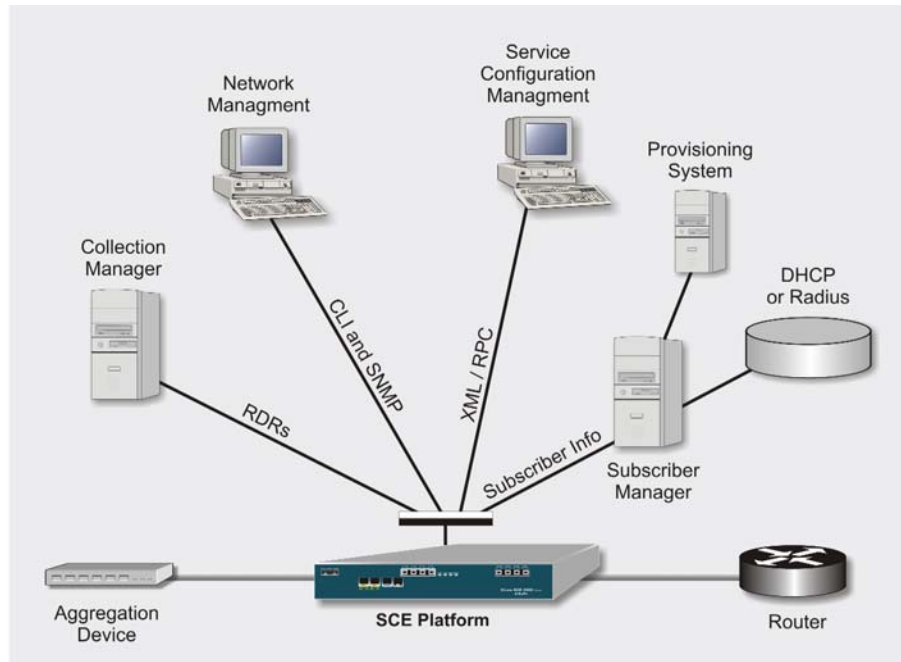
Management and Collection

The Service Control solution includes a complete management infrastructure that provides the following management components to manage all aspects of the Service Control solutions:

- Network management
- Subscriber management
- Service Control Management

These management interfaces are designed to comply with common management standards and to easily integrate with existing OSS infrastructure.

Figure 1-2: Service Control Management Infrastructure



Network Management

Cisco provides complete network FCAPS Management (Fault, Configuration, Accounting, Performance, Security).

Two interfaces are provided for network management:

- **CLI** (Command Line Interface). The CLI is accessible through the Console port or through a Telnet connection.

CLI is used for configuration and security functions.

- **SNMP** (Simple Network Management Protocol).

SNMP provides fault management via SNMP traps, as well as performance monitoring functionality.

Subscriber Management

In cases where Service Control Application Suite for Broadband is used to enforce different policies on different subscribers, and tracks usage on an individual subscriber basis, the smartSUB Manager (SM) component is required to function as middleware software used to bridge between the OSS and the SCE Platform(s). Subscriber information is stored in the SM database and can then be distributed between multiple devices according to actual subscriber placement.

The SM provides subscriber awareness, mapping network IDs to subscriber IDs. It obtains subscriber information using dedicated integration modules, which integrate with AAA devices like Radius or DHCP servers.

Subscriber information may be obtained in one of two ways:

- Push Mode: The SM pushes subscriber information to the SCE Platform automatically upon logon of a subscriber.
- Pull Mode: On-demand, in response to a query from the SCE Platform to the SM.

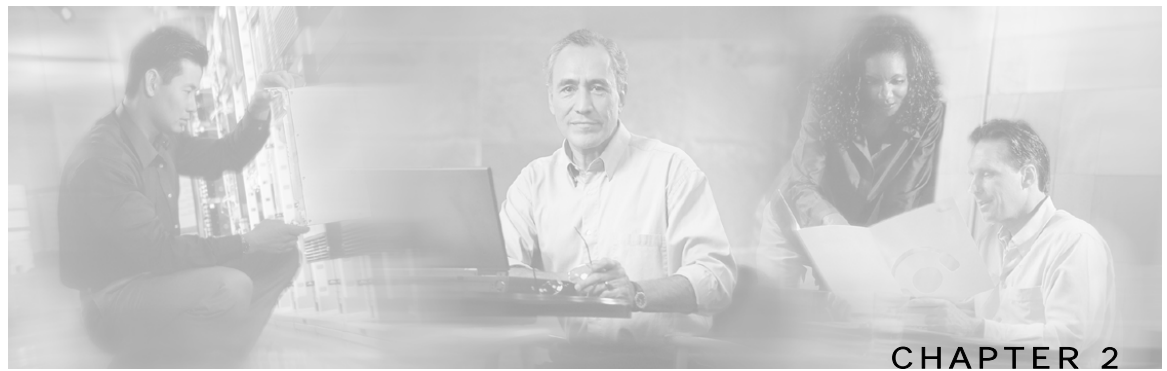
Collection

The Service Control Application Suite for Broadband solution generates usage data and statistics from the SCE Platform and forwards them as Raw Data Records (RDRs), using a simple TCP based protocol (RDR-Protocol). The Service Control solution provides the Collection Manager software as an implementation of a collection system, listening in on RDRs from one or more SCE Platforms, and processing them on the local machine. The data is then stored for analysis and reporting functions, as well as simple collection and presentation of data to additional OSS systems such as billing.

Service Configuration Management

Service configuration management is the ability to configure the general service definitions of a Service Control application. Service Configuration is performed by creating an XML configuration file and applying it to an SCE device. Service Control Application Suite for Broadband provides tools to automate the distribution of these configuration files to SCE Platforms, and this simple, standards-based approach makes it easy to manage multiple devices in a large network.

Service Control provides a simple to use GUI to edit and create these files, as well as a complete set of APIs to automate their creation.



System Overview

Service Control Application Suite for Broadband is the Service Control solution that allows broadband service providers to gain visibility into and control over the distribution of network resources, and thereby to optimize traffic in accordance with their business strategies. It enables service providers to reduce network costs, improve network performance and customer experience, and create new service-offerings and packages.

This chapter contains the following sections:

- [System Components](#) 2-1
- [Subscribers and Subscriber-Modes](#) 2-3
- [Service Configuration](#) 2-5

System Components

The Service Control Application Suite for Broadband solution consists of three main components:

- The SCE Platform: A flexible and powerful dedicated network usage monitor that is purpose-built to analyze and report on network transactions at the application level.

For complete information regarding the installation and operation of the SCE Platform, refer to the *SCE 1000/SCE 2000 User Guides*.

- The Service Control smartSUB Manager (SM): A middleware software component used in cases where dynamic binding of subscriber information and policies is required. The SM manages subscriber information and provisions it in real time to multiple SCE Platforms. The SM can store subscriber policy information internally, and act as a state-full bridge between the AAA system (e.g. RADIUS, DHCP) and the SCE Platforms

For complete information regarding the installation and operation of the smartSUB Manager, refer to the *smartSUB Manager User Guide*.

- The Service Control Collection Manager (CM): An implementation of a collection system, listening in on RDRs from one or more SCE Platforms. It collects usage information and statistics, stores them in a bundled database, and provides a set of insightful reports from this data. The CM also converts subscriber usage information and statistics into simple text-based files for further processing and collection by external systems.

For complete information regarding the installation and operation of the Collection Manager, refer to the *Collection Manager User Guide*.

Together, the SCE Platform, the Collection Manager, and the smartSUB Manager are designed to support detailed observation, analysis, reporting, and control of IP network traffic. Note that the Collection Manager and smartSUB Manager are optional components, and are not required in all deployments of the solution. Sites that employ third party collection and reporting applications and/or do not require dynamic subscriber-aware processing may not require these components.

The following figure illustrates the flow of information within the Service Control Application Suite for Broadband solution.

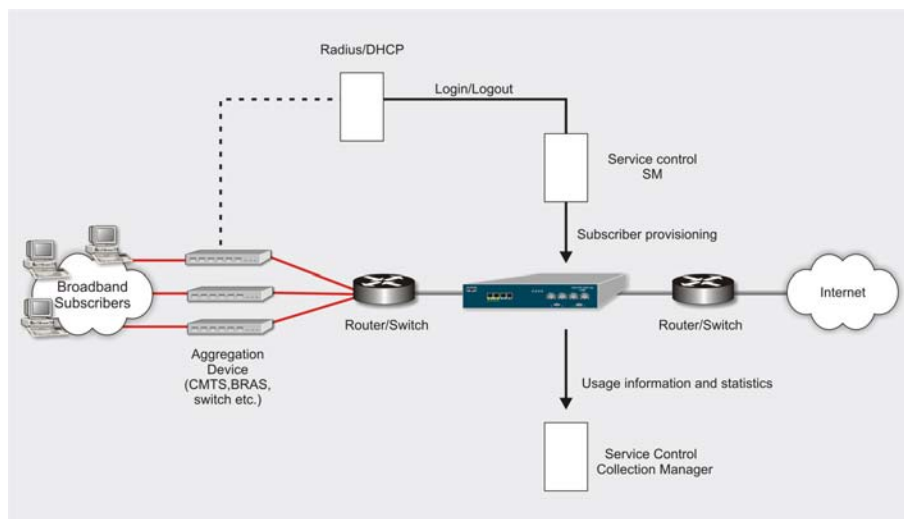
- Horizontal flow: Represents traffic between subscribers and IP network.

The SCE Platform monitors traffic flow.

- Vertical flow: Represents transmission of the Raw Data Records (RDRs) from the SCE Platform to the Collection Manager.

The *smartSUB Manager* may be added to the control flow to provide subscriber data. This enables the Service Control Application Suite for Broadband to conduct subscriber level analysis and control.

Figure 2-1: Flow of Information in Service Control Application Suite for Broadband



Subscribers and Subscriber-Modes

One of the fundamental entities in the Service Control Application Suite for Broadband solution is a *subscriber*. A subscriber is the most-granular entity that the Service Control solution can individually monitor, account and enforce a policy on. In the most granular instance of the **SCAS BB** system a subscriber is an actual customer of the service-provider on whom an individual policy is implemented. However, it is also possible to use the Service Control Application Suite for Broadband solution to monitor and control traffic at a higher granularity, such as when monitoring controlling traffic by subnets or aggregation devices.

One of the most important decisions to be made when designing an **SCAS BB** solution is what will be defined as a subscriber in the system. This determines what subscriber-mode will be used, which in turn determines what (if any) integrations are required, as well as what actual policy to define. The following section describes the different subscriber-modes supported, what functions are supported for each and what are the prerequisites and required components needed.

Service Control Application Suite for Broadband supports the following four subscriber modes:

- **Subscriber-less mode:** no subscribers are defined
- **Anonymous subscriber-mode:** IP addresses are controlled and monitored individually. The SCE Platform automatically identifies IP addresses as they are used and assigns them a package
- **Static Subscriber Mode:** incoming IP addresses are bound and grouped statically into 'subscribers', as configured by the system operator
- **Subscriber-aware mode – Dynamic Subscribers:** subscriber information is dynamically bound to the IP address currently in use by the subscriber through an integration with the system that assigns IP addresses to subscribers (RADIUS, DHCP). Policy information is either administered to the **SCAS BB** solution directly, or is also provisioned dynamically through an integration

Subscriber-less mode

Subscriber-less mode is the choice for sites where control and - analysis functions are required only at a global device resolution. It can be used, for example, to monitor and control the total amount of P2P traffic over the link.

Since subscriber-less mode requires no integration, the smartSUB Manager component is not required. Note that, since subscriber-less mode is not influenced by the number of subscribers or inbound IP addresses, the total amount of subscribers utilizing the monitored link is unlimited from the perspective of the SCE device.

Anonymous subscriber-mode

Anonymous subscriber mode provides the means to analyze and control network traffic at a subscriber-inbound IP address granularity. Use this mode when no subscriber-differentiated control or subscriber-level quota tracking is required, when analysis on an IP level is sufficient, or when offline IP-address/subscriber binding can be performed. For example, it is possible to identify which subscribers generate the most P2P traffic by identifying the top IP addresses and correlating them to individual subscribers manually/offline via RADIUS/DHCP logs. The total bandwidth of P2P traffic allowed for each subscriber can be limited as well.

Since anonymous mode requires no integration or static configuration of the IP addresses used, the smartSUB Manager component is not required. Rather, ranges of IP addresses are configured directly on the SCE device, for which the system will dynamically create ‘anonymous’ subscribers, using the IP address as the subscriber-name. Note that the total number of concurrently-active anonymous subscribers supported by the SCE Platform is the same as the total number of concurrently-active subscribers.

Static Subscriber Mode

Static subscriber mode binds together incoming IP addresses into groups, so that traffic from/to a defined subscriber can be controlled as a group. For example, with this mode, all traffic from/to a particular network subnet (used by multiple subscribers concurrently) can be defined as a ‘virtual subscriber’ and controlled/viewed as a group.

Static subscriber mode supports cases in which the entity controlled by the Service Control solution uses a constant IP address or address-range that does not change dynamically, such as:

- Environments where the subscriber IP address(es) do not change dynamically via DHCP, RADIUS, etc.
- Deployments in which a group of subscribers using a common pool of IP addresses, such as all those served by a particular CMTS, BRAS, etc., are to be managed together to provide a shared bandwidth to the entire group.

The system supports the definition of static subscribers directly on a SCE device, and does not require external management software (smartSUB Manager). This is achieved by using the SCE device CLI to define the list of subscribers, their IP addresses and associated package.

Subscriber-aware mode – Dynamic Subscribers

Dynamic-subscriber-aware mode, the Service-Engine is populated by subscriber information (OSS ID & policy) that is dynamically bound to the (IP) address currently in use by the subscribers. This provides differentiated and dynamic control per subscriber and subscriber-level analysis, regardless of IP address in use. This mode is used to control/analyze traffic on a subscriber level and monitor subscriber-usage, regardless of IP addresses. It also enables assigning and enforcing different control-policies (packages) for different subscribers.

In this mode the smartSUB Manager (SM) needs to be used to perform device provisioning with subscriber information. The SM is a server application that maintains the above association, and provisions it to SCE devices in real-time.

Subscriber Modes – Summary

The following table summarizes the different subscriber modes supported by the system.

Mode	Features Supported	Main Advantages	When to Use
Subscriber-less mode	Global (device-level) analysis & control	No subscriber-configuration required	Global control solution or subscriber level analysis. Examples: Control P2P uploads at peering points Limit total amount of P2P to xx%
Anonymous-mode	Global analysis & control Individual IP address level analysis & control	No subscriber-configuration required. Only need to define subscriber IP address ranges used Provides subscriber-level control w/o integration	IP level analysis or control that is not differentiated per subscriber, and where offline IP-address/subscriber binding is sufficient. Examples: Limit per subscriber P2P to 64Kbps Identify top subscribers by identifying top IP addresses and correlating manually/offline with RADIUS/DHCP logs
Static Subscriber mode	Global Analysis & Control Control based on individual IP addresses/groups as configured statically to the SCE device	On-time Static subscriber configuration, with no integration requirements Manage subscriber traffic in logical groups	Control of traffic of groups of subscribers. Example: Assign a 5Mbps limit of P2P traffic for each group of subscribers using a single CMTS device
Dynamic Subscriber mode	Full system functionality	Differentiated and dynamic control per subscriber Subscriber-level analysis, regardless of IP address in use	To control/analyze traffic on a subscriber level. Monitor subscriber-usage, regardless of IP addresses Assign different control-policies (packages) to different subscribers, and change packages dynamically

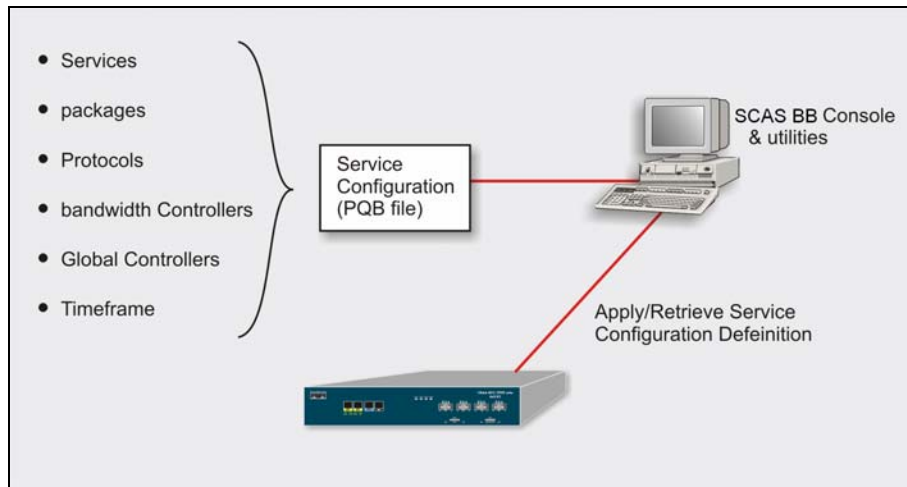
Service Configuration

Service configuration defines the way an SCE device analyses and controls traffic. In very general terms, Service Configuration defines the following:

- protocol and service classification
- packages and policies
- bandwidth controllers

- global controllers

Figure 2-2: Service Configuration



Service configuration is accomplished using one of the following:

- SCAS BB Console
- Service Configuration Utility
- **SCAS BB** API

SCAS BB Console

The SCAS BB Console is the Service Control Application Suite for Broadband GUI used to create, modify, and apply the service configuration. The SCAS BB Console lets you define services, packages, protocols, bandwidth control and other entities in the configuration. The SCAS BB Console creates a policy configuration file (*.pqb*), which can then be saved and/or applied to the SCE device(s).

You can also access the **SCAS BB** Subscriber Manager from the SCAS BB Console to manage subscribers. In addition, you can access the Reporter feature of the Collection Manager to create and output reports.

The SCAS BB Console is fully documented in the remainder of this guide.

Service Configuration Utility

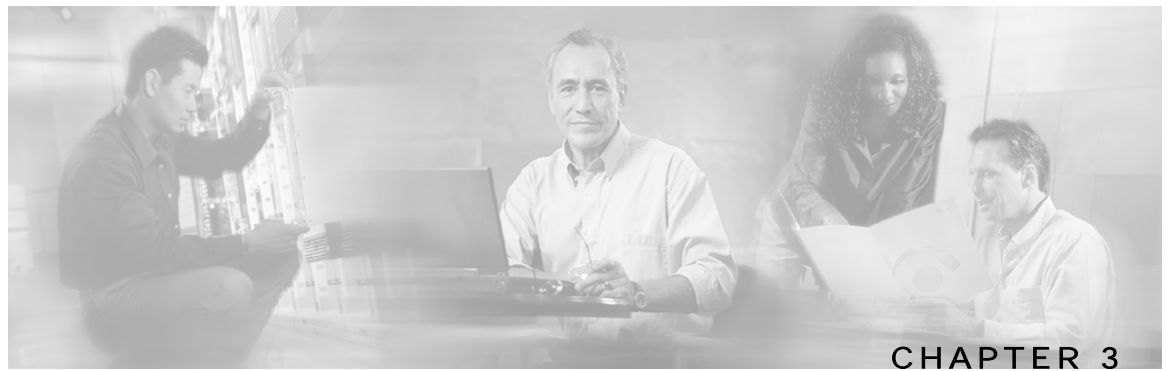
The Service Configuration Utility is a simple command line tool that can be used to apply *.pqb* configuration files onto SCE devices, or retrieve the current configuration from an SCE Platform and save as a *pqb* file. The tool can be installed and executed on either Windows or Solaris environments, and configures SCE devices with the policy-configuration in a *.pqb* file.

For additional information regarding the Service Configuration Utility, see *Using the Service Configuration Utility* (on page 4-4).

Service Configuration API

The Service Configuration API is a set of Java classes used to program and manage Service Configurations, and to apply these Service Configurations to the SCE Platforms. In addition, applications using the Service Configuration API can be integrated with third-party systems, allowing service providers to automate and simplify management and operational tasks

See the Service Control Application Suite for Broadband *API Programmer's Guide* for more information regarding the **SCAS BB** API.



Running the SCAS BB Console

The SCAS BB Console is the front-end of the <fullproduct. It is used to configure the services that the SP offers its clients.

This book contains four chapters that explain how to use the SCAS BB Console:

- This chapter describes the SCAS BB Console itself
- The next chapter, *Managing Service Configurations* (on page 4-1), describes how to manage the service configurations, for example, how to save or retrieve a configuration
- The chapter *Constructing Service Configurations* (on page 5-1) guides you through the basic tasks of configuring traffic classification, traffic control and RDR settings
- The chapter *Managing the System Settings* (on page 6-1) presents the advanced system settings

This chapter contains the following sections:

- [The SCAS BB Console](#) 3-2
- [Opening the SCAS BB Console](#) 3-10
- [Closing the SCAS BB Console](#) 3-11

The SCAS BB Console

The following figure shows the SCAS BB Console main screen and the various elements that appear on it:

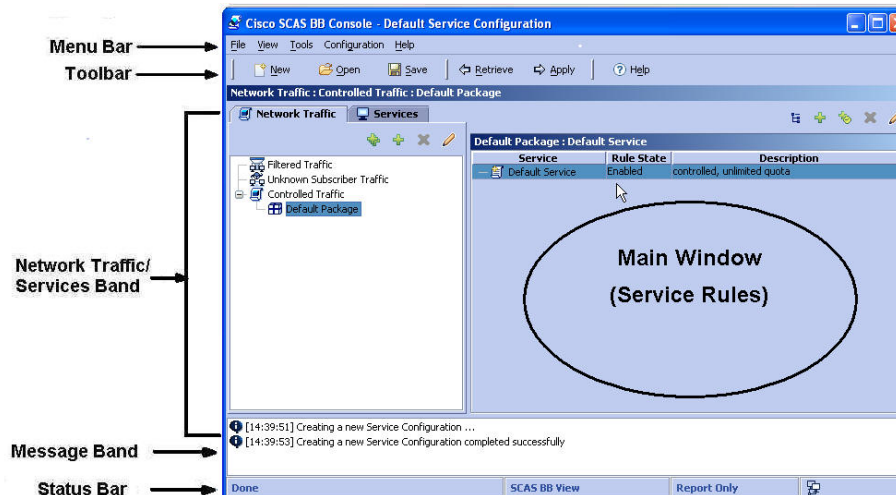











Figure 3-1: SCAS BB Console: Main Screen


Menu Bar and Toolbar

The following table describes the toolbar and various menus and sub-menus found when navigating through the SCAS BB Console menu bar. A black line in the table delineates between menus and a gray line indicates a command separator in the menu list.

Table 3-1 SCAS BB Console Menu and Toolbar

Menu	Sub-Menu	Description	Comments
File	Apply	Transfers the current Service Configuration to the SCE Platforms and activates it.	Keyboard shortcut: Alt+A
			
	Retrieve	Transfers the Service Configuration from the SCE Platform to the SCAS BB Console.	Keyboard shortcut: Alt+R
			
	Validate	Checks that the current Service Configuration is valid.	
			
	New	Creates a new Service Configuration.	Keyboard shortcut: Alt+N
			
	Open	Opens an archived Service Configuration.	Keyboard shortcut: Alt+O
			

Menu	Sub-Menu	Description	Comments
	Save 	Saves the current Service Configuration to the open .pqb file.	Keyboard shortcut: Alt+S
	Save As	Allows you to save the current Service Configuration to a selected .pqb file.	
	Import 	Imports any of the following from an existing *.csv file: <ul style="list-style-type: none"> • Packages • Services • Protocols • Lists 	
	Export 	Exports any of the following to a *.csv file: <ul style="list-style-type: none"> • Packages • Services • Protocols • Lists 	
	Exit	Closes the SCAS BB Console.	Keyboard shortcut: Ctrl+Q
View	View Status	When enabled, the SCAS BB Console output appears in the Message band.	Default: enabled
Tools	Subscribers Manager	Starts the <i>SCAS BB</i> SM GUI.	
	Reporter 	Starts the SCAS Reporter.	
Configuration	Network Traffic	Brings the Network Traffic band to the front in the main window. Allows you to edit packages, rules, and filtered traffic settings.	
	Services	Brings the Services band to front in the main window. Allows you to add, remove, or edit Services.	
	Global Controllers	Allows you to add, remove, or edit Global Controllers.	
	Protocols	Allows you to add, remove, or edit Protocols.	
	Lists	Allows you to add, remove, or edit Network Address Lists.	

Menu	Sub-Menu	Description	Comments
	Weekly Time Frames	Allows you to define four time-frames and their scope.	Based on dividing a week into 24x7 hours and assigning each hour to one of four time-frames
	RDR Settings	Use to control the generation of various types of RDRs	<p>Opens a multi-tab dialog box:</p> <ul style="list-style-type: none"> • Usage RDRs • Traffic Discovery • Quota RDRs • Transaction Usage RDRs • Log RDRs • Realtime RDRs
	Subscriber Notifications	Allows you to add, remove or edit subscriber notifications.	
	Signatures	Allows you to import dynamic signatures.	
	System Settings	Use to specify system mode and various advanced settings.	<p>Opens a multi-tab dialog box:</p> <ul style="list-style-type: none"> • System Mode • P2P Detection • Redirection URLs • Ongoing Policy Check • BW Management
Help	Help Contents	Accesses help information by topic.	
	License Manager	Allows you to activate SCAS BB Capacity Control and SCAS BB Tiered Control licenses.	
	About	Shows the current version of the SCAS BB Console and the current environment settings.	

Network Traffic/Services Band

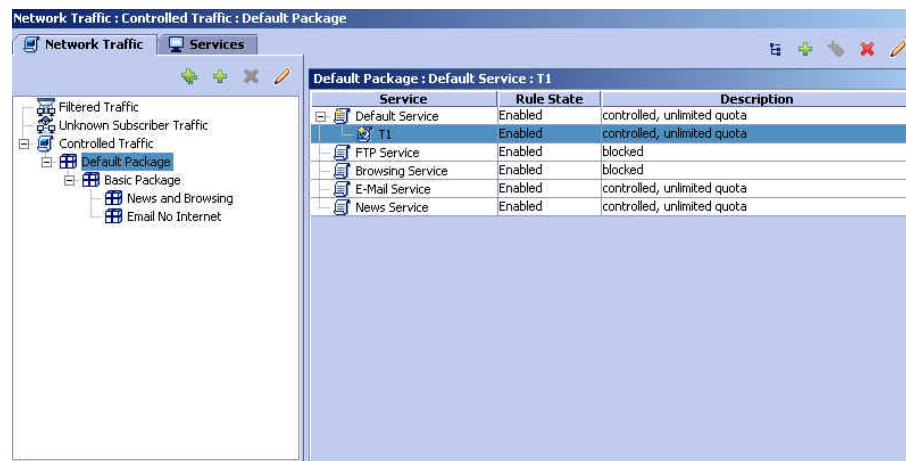
The *Network Traffic/Services band* is the left-hand pane of this screen. This band has two tabs, Network Traffic and Services, which appear below the band. This band displays Network Traffic or Services, depending on the active tab. Further details concerning each Network Traffic/Services can be found in the right-hand pane, the *Main Window*.

The *Main Window* is the right-hand pane of this screen. The contents of this screen depend on the active band in the Network Traffic/Services band.

Network Traffic Band

When the Network Traffic band is active, the information that appears in the Main Window depends upon the selected category or Package in the left-hand pane of this screen (see the following figure).

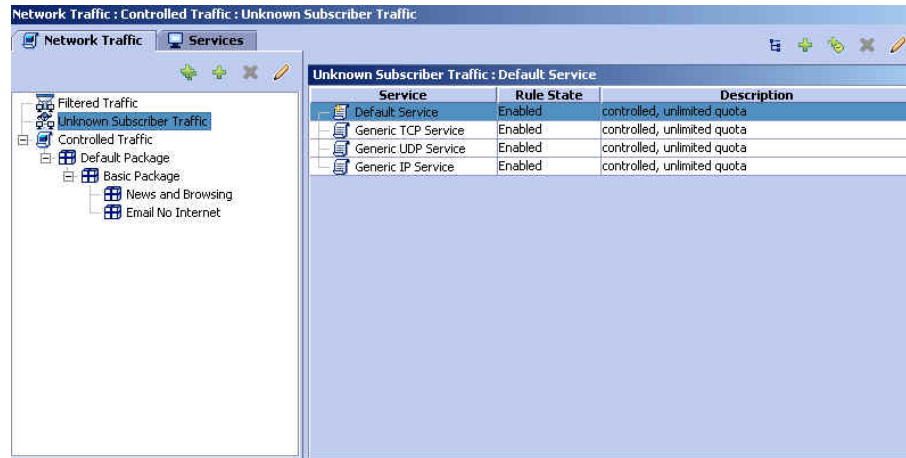
Figure 3-2: Network Traffic Band



The following are the Network Traffic categories:

- **Filtered Traffic:** A traffic flow that is filtered out of the SCE Platform, so that the traffic flow will not be affected by Service Configuration definitions. The Filter Rules are displayed in the Main Window.

Figure 3-3: Network Traffic: Unknown Subscribers



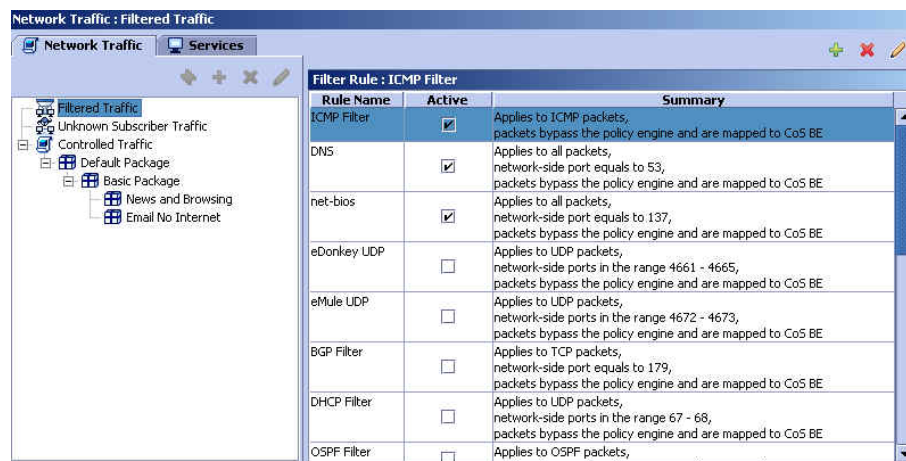
The Filter Rules are listed in a table that has the following columns:

- **Rule name:** The name of the Filtered Traffic Rule.
- **Active:** The operational state of the rule.
- **Summary:** A summary of the rule settings.

From the Main Window, you can add a new Filtered Traffic Rule, or remove or edit a selected Filtered Traffic Rule.

- **Unknown Subscribers Traffic:** A traffic flow belongs to this category when it was not mapped to a Filtered Traffic rule, and its IP address or VLAN ID did not match the IP address or VLAN ID of a subscriber in the SCE Platform internal database.

Figure 3-4: Network Traffic: Filtered Traffic Rule



By default, the Unknown subscriber traffic contains rules for the three generic services:

- Generic TCP Service
- Generic UDP Service
- Generic IP Service

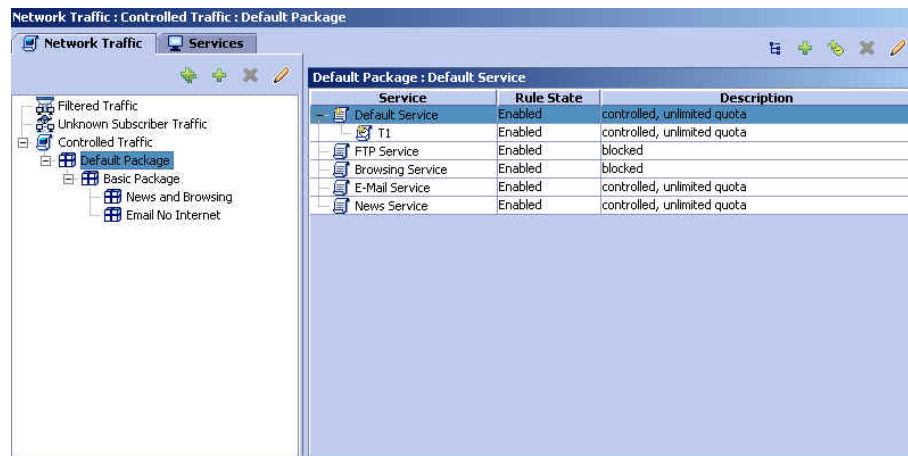
No packages can be added to the Unknown Subscriber Traffic package in the Network Traffic pane:

From the Main Window, a new service rule or a new time based service rule can be added to the Unknown Subscriber Traffic package, or a selected service rule can be removed or edited.

Available functions in Main Window:

- Add Rule
- Add
- Delete Rule
- Edit Rule
- **Controlled Traffic:** A traffic flow is mapped to Controlled Traffic when the IP address or VLAN ID does correspond to the IP address or VLAN ID of a subscriber in the database, and no Filtered Traffic Rule applies.

Figure 3-5: Network Traffic: Controlled Traffic



When a Package is selected in the Network Traffic tab, the list of Rules defined for the package appears in the Main Window on the right.

The Rules are listed in a table with the following columns:

- **Service:** The name of the Service for which the Rule applies.
- **Rule State:** The operational state of the rule.
- **Description:** The rule action.

From the Network Traffic pane, a new package can be added, or a selected package can be duplicated, removed or edited.

Available functions in Network Traffic pane:

- Duplicate Package (duplicate package is added at the same level in the hierarchy as the selected package)

- Add Package (by default, package is added as descendant to currently selected package)
- Delete Package
- Edit Package

From the Main Window, a new service rule or a new time based service rule can be added to the selected package, or a selected service rule can be removed or edited.

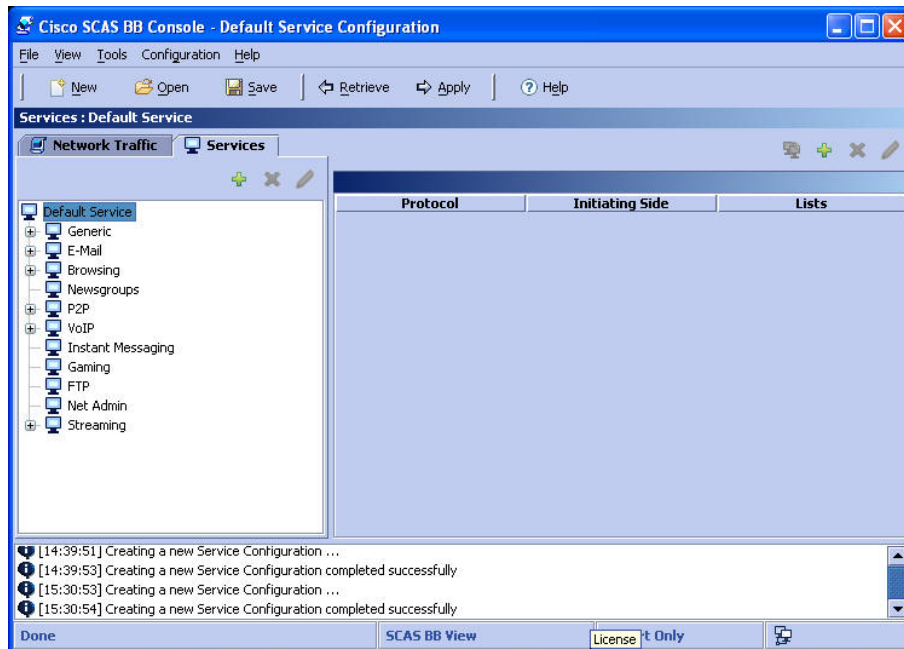
Available functions in Main Window:

- Add Rule
- Add Time Based Rule (the time-based rule will apply only to the selected service rule)
- Delete Rule
- Edit Rule

Services Band

When the Services band is active, the Service Element per Service information appears in the Main Window (see the following figure).

Figure 3-6: Services Band



The Service Element information is listed in a table that has the following columns:

- **Protocol:** The transaction protocol. For example, FTP, HTTP Browsing, or SMTP.
- **Classification Direction:** The initiating side of the transaction. (Network-Initiated, Subscriber-Initiated).
- **Lists:** The network-side IP addresses or host names of the transaction.

Available functions in the Service pane:

- Add Service

- Delete Service
- Edit Service

Available functions in Main Window:

- Move Service Element to another Service
- Add Service Element
- Delete Service Element
- Edit Service Element

Message Band

Below the Network Traffic/Services band and the Main Window is the *Message band* (see the following figure). This band shows system messages and events as they happen.



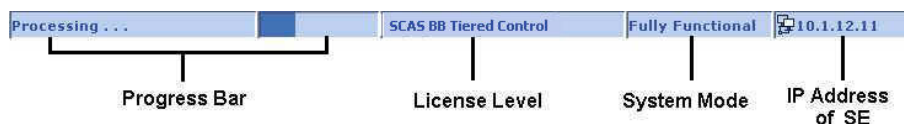
You can enlarge the Network Traffic/Services band and Main Window areas by hiding the Message band. Alternatively, you can open the Message band when you want to see the messages and process notifications.

Status Bar

The *Status Bar* (illustrated below) shows you the following information:

- **Progress Bar:** Indicates processing is taking place.
- **Current License Level:** The license level at which the SCAS BB Console is operating (see *SCAS BB Licenses* (on page 4-13)):
 - *SCAS BB* View
 - *SCAS BB* Capacity Control
 - *SCAS BB* Tiered Control
- **Current System Mode:** The current operational state of the system (see *Configuring the System Mode Parameter* (on page 6-1)):
 - Fully Functional: Reporting and active actions both enabled
 - Report Only: Reporting enabled, active actions disabled
 - Transparent: Reporting and active actions both disabled
- **IP Address of the SCE:** Available only when connected to an SCE Platform to apply or retrieve a Service Configuration

Figure 3-7: The Status Bar



Opening the SCAS BB Console

The procedure for opening the SCAS BB Console varies slightly, depending on whether it is necessary to connect to the SCE device. When simply opening an existing Service Configuration or creating a new one, it is not necessary to connect to the SCE device. However, retrieving the current Service Configuration from an SCE device does require connecting to the device.

Connecting to the SCE device requires the following information:

- password
- IP address of the SCE Platform

To open the SCAS BB Console and open an existing Service Configuration or create a new one:

Step 1 Select **Start > Programs > Cisco SCAS > SCAS BB x.x.x > SCAS BB Console**.

The following dialog opens.



Step 2 Click the appropriate radio button to either open an existing Service Configuration or create a new one.

Step 3 Click **OK**.

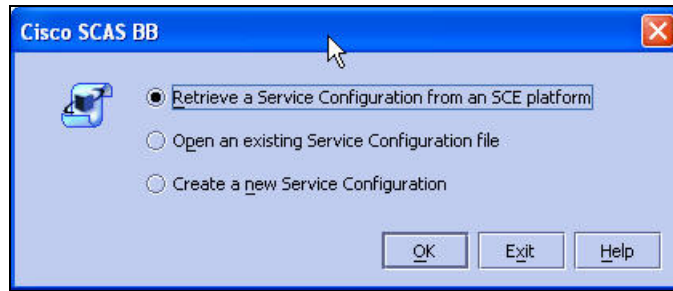
The system responds, depending on the selected choice:

- Open an existing Service Configuration: The *Open a Service Configuration* dialog opens.
- Create an new Service Configuration: A message appears indicating that a new Service Configuration file is being opened.

To open to the SCAS BB Console and retrieve a Service Configuration:

Step 1 Select **Start > Programs > Cisco SCAS > SCAS BB x.x.x > SCAS BB Console**

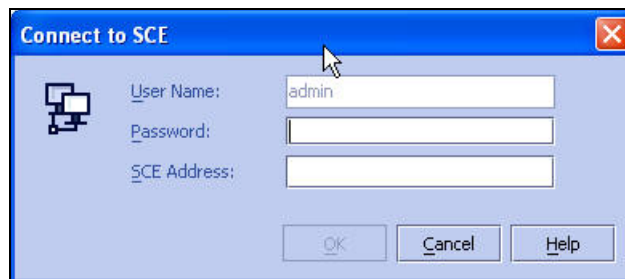
The following dialog opens.



Step 2 Click the appropriate radio button to retrieve a Service Configuration from an SCE device.

Step 3 Click **OK**.

The *Connect to SCE* dialog opens.



Step 4 Type in the Password, and address of the SCE device.

Step 5 Click **OK**.

The SCAS BB Console is connected to the specified SCE Platform, and the Service Configuration of that device is displayed in the SCAS BB Console.

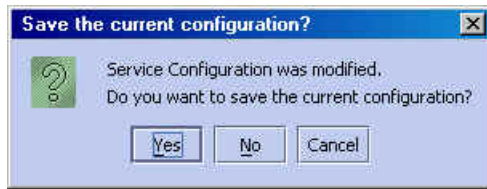
Once the Service Configuration has been retrieved, the SCE device is disconnected from the SCAS BB Console.

Closing the SCAS BB Console

To exit the SCAS BB Console:

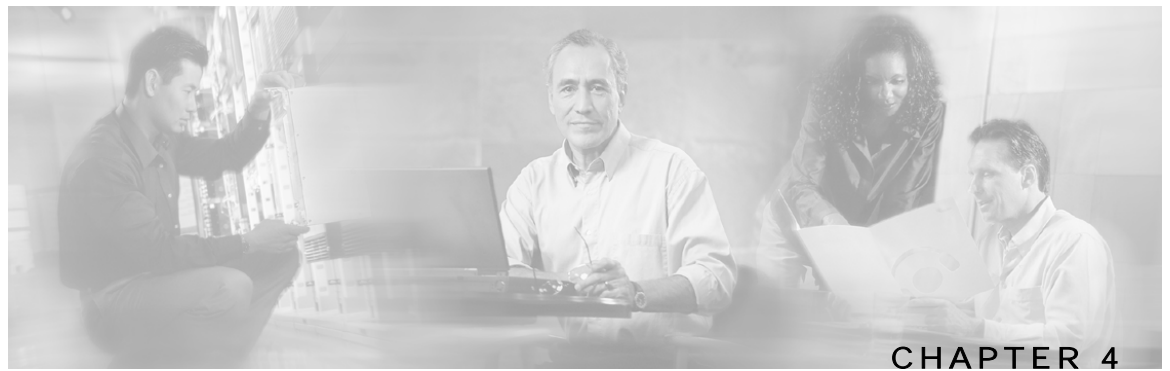
Step 1 From the **File** menu, click **Exit**.

If the Service Configuration was edited, a **Save state confirmation** message appears.



If you wish to save the current configuration, click **Yes**.

The Service Configuration changes are saved and the SCAS BB Console closes.



Managing Service Configurations

This section presents instructions for managing the Service Configurations, such as, applying Service Configurations to and retrieving them from the SCE Platform, or saving and opening Service Configurations.

This chapter contains the following sections:

- [Applying and Retrieving Service Configurations](#) 4-1
- [Creating a New Service Configuration](#) 4-6
- [Saving the Current Service Configuration](#) 4-8
- [Validating the Current Service Configuration](#) 4-9
- [Opening an Existing Service Configuration](#) 4-10
- [Exporting Packages, Services, Protocols and Lists](#) 4-11
- [Importing Packages, Services, Protocols or Lists](#) 4-12
- [Accessing the SCAS Reporter](#) 4-13
- [Accessing the SCAS BB SM GUI](#) 4-13
- [SCAS BB Licenses](#) 4-13

Applying and Retrieving Service Configurations

A Service Configuration must be applied to the SCE Platform. If you do not apply the Service Configuration, the new or edited Service Configuration will not take effect, and the previous Service Configuration will continue to be enforced by the SCE Platform.

It is also possible to retrieve the current Service Configuration from a specified SCE Platform. This Service Configuration will then be displayed in the SCAS BB Console.

In order to apply or retrieve a Service Configuration, the SCAS BB Console must be connected to the SCE Platform. The system will require the following information in order to connect to the SCE device before validating and applying the configuration:

- password: for each console session, the password is only required on the first connection to the system

- Address of the SCE Platform: after the first connection per console session, the IP address of the last SCE device connected to is displayed

You can also apply or retrieve a Service Configuration using the Service Configuration Utility. This utility provides a command-line interface for performing these operations. This is an easy method for automating applying/retrieving service configurations.

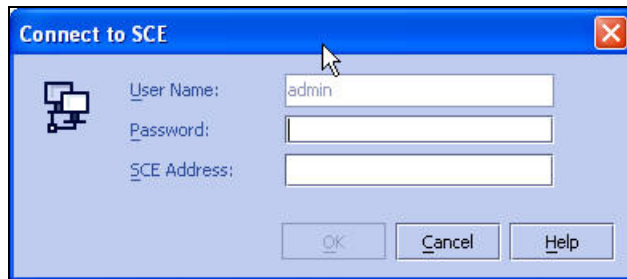
Applying a Service Configuration

When you click **Apply**, the Service Configuration is validated. If there is a problem and the validation process ends with a warning or error, the *Service Configuration Validation* screen appears, supplying the validation results. It is possible to select to **Apply Anyway** or to correct the problem prior to applying the Service Configuration. Use the **Validation** menu command to manually validate a Service Configuration at any time.

To apply the currently open Service Configuration to an SCE Platform:

- Step 1** From the toolbar, click **Apply** 

The following dialog box appears. If you have previously connected to the system during this console session, some information may not be required.



- Step 2** Fill in the necessary fields.

- Step 3** Click **OK**.

The SCAS BB Console is connected to the specified SCE Platform.

The Service Configuration undergoes the validation process. If the Service Configuration is validated, skip step 4. If the validation process ended with a warning or error status, the *Service Configuration Validation* dialog box, illustrated below, appears.



Figure 4-1: Service Configuration Validation Dialog Box (Warning/Error Status)

- Step 4** It is possible to keep this dialog box open and edit the Service Configuration.
- See the section *Validating the Current Service Configuration* (on page 4-9) for additional information on this feature. If you decide to ignore the warning messages, continue this procedure.
 - Click **Cancel** to call off the *Apply* operation.
- Step 5** Click **Apply Anyway** to continue with the *Apply Service Configuration* procedure. The Message band indicates that the Service Configuration is being applied to the SCE Platform. SCAS BB Console disconnects from the SCE device after the Service Configuration has been applied.

Retrieving the Current Service Configuration

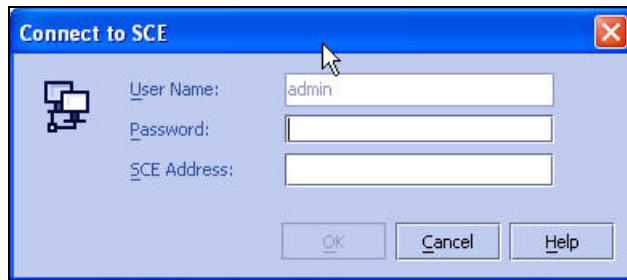
Use the **Retrieve** option to retrieve the current Service Configuration for review or edit. Remember that if you edit the retrieved Service Configuration, you must apply it to the SCE device again in order for the changes to take effect.

To retrieve the current Service Configuration from an SCE Platform:

- Step 1** From the toolbar, click **Retrieve** .

Applying and Retrieving Service Configurations

The following dialog box appears. If you have previously connected to the system during this console session, some information may not be required.



Step 2 Fill in the necessary fields.

Step 3 Click **OK**.

The message *Retrieving Service Configuration ...* appears, as the SCAS BB Console transfers the configuration from the SCE.

The Service Configuration components seen in the SCAS BB Console will change to the new Service Configuration components.

SCAS BB Console disconnects from the SCE device after the Service Configuration has been retrieved.

Using the Service Configuration Utility

The service configuration utility (`servconf`) is a command-line interface for applying/retrieving service configurations. Use it in a scripting environment to automate service configuration tasks. Note that when applying a Service Configuration, you can specify multiple SCE devices in one command.

The service configuration utility can be used in both Windows and Solaris environments.

The command-line syntax is:

```
servconf [CONNECTION] <OPERATION> [LICENSE] [FILE] [REFER-SE]
```

The following tables list the `servconf` operations and options.

Table 4-1 `servconf` Operations

Operation	Abbreviation (if applicable)	Description
--apply	-a	Copies the specified service configuration file to the specified SCE device(s) and activates it.
--retrieve	-r	Retrieves the currently active service configuration.
--update-dc	-u	Updates a Collection Manager with the service configuration values.
--status		Show the service configuration status on the SCE Platform.
--help		Prints this help, then exits.

Operation	Abbreviation (if applicable)	Description
--version		Prints the program version number, then exits.

Table 4-2 servconf File Option

File Option	Abbreviation	Description
--file=FILE	-f	Specifies service configuration FILE.

Table 4-3 servconf Connection Options

File Option	Abbreviation	Description
--se=ADDRESS	-S	Specifies the ADDRESS of the destination SCE Platform. To specify multiple SCE devices, list the IP addresses separated by a semicolon. (See Example 1 below) Note that when using a semicolon in a Unix command line, the command line argument should be enclosed in quotation marks.
--dc=ADDRESS	-D	Specifies the ADDRESS of the destination CM Platform (required only for --update-dc operation).
--password=PASSWORD	-P	Specifies the PASSWORD for connecting to the SCE Platform.
--dc-update-method		Specifies the METHOD (SQL or RPC) for updating the CM. Default = SQL

Table 4-4 servconf License Options

File Option	Abbreviation	Description
--customer-id=ID	-c	Specifies the ID of the customer, needed for activating the license.
--license=KEY	-l	Specifies the KEY for activating the license of the specified customer (16 characters string).

Table 4-5 servconf Reference SCE Option

File Option	Description
--refer-se=SCE	Specifies the ADDRESS of the SCE Platform to which the service configuration values refer (required only for --update-dc operation).

Table 4-6 servconf Apply Option

File Option	Description
--no-dc	An optional flag that specifies that the --apply operation should not automatically update the CM with service configuration values.

EXAMPLE 1:

The following example shows how to copy the service configuration file *config.pqb* from the local machine to two SCE Platforms (at 63.111.106.7 and 63.111.106.12), and activate this configuration:

```
servconf --"se 63.111.106.7;63.111.106.12" --password pcube --apply --file
config.pqb
```

EXAMPLE 2:

The following example shows how to retrieve the currently active service configuration from the SCE Platform at 63.111.106.7, and save it in file *my_files/config.pqb* on the local machine.

```
servconf -S 63.111.106.7 -P pcube --retrieve --file my_files/config.pqb
```

EXAMPLE 3:

The following example shows how to update the CM at 63.121.116.17 with service configuration values from file *config.pqb*, as if they were applied to the SCE Platform at 63.111.106.7 (but without actually applying them to the SCE Platform):

```
servconf -D 63.121.116.17 -P pcube --update-dc --refer-se 63.111.106.7
--file config.pqb
```

Creating a New Service Configuration

Use this procedure to create a new Service Configuration.

To create a new Service Configuration:

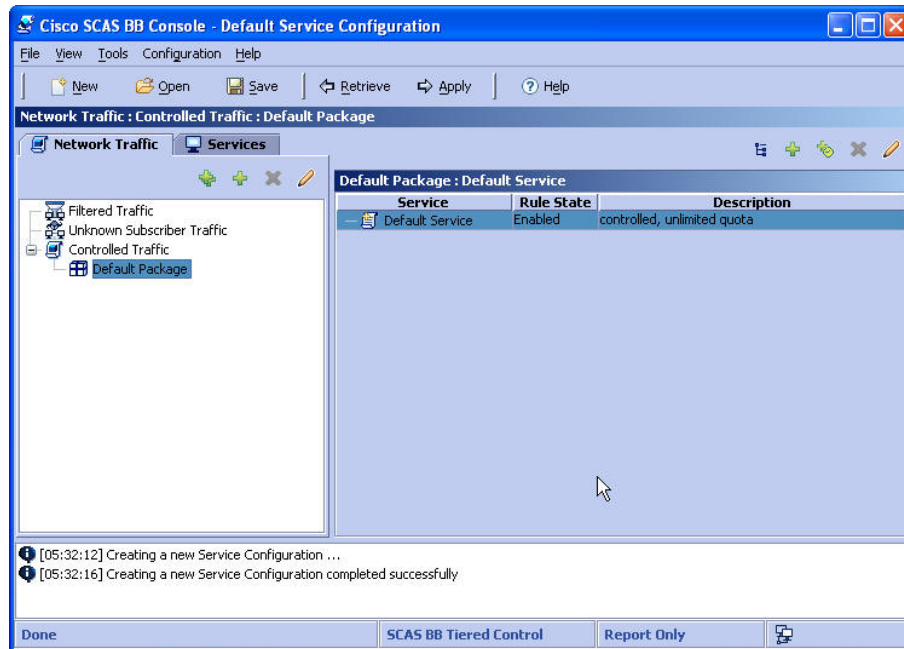
Step 1 In the toolbar, click **New** .

The message *Creating a new Service Configuration...* appears as the SCAS BB Console loads the information necessary for creating a new Service Configuration.



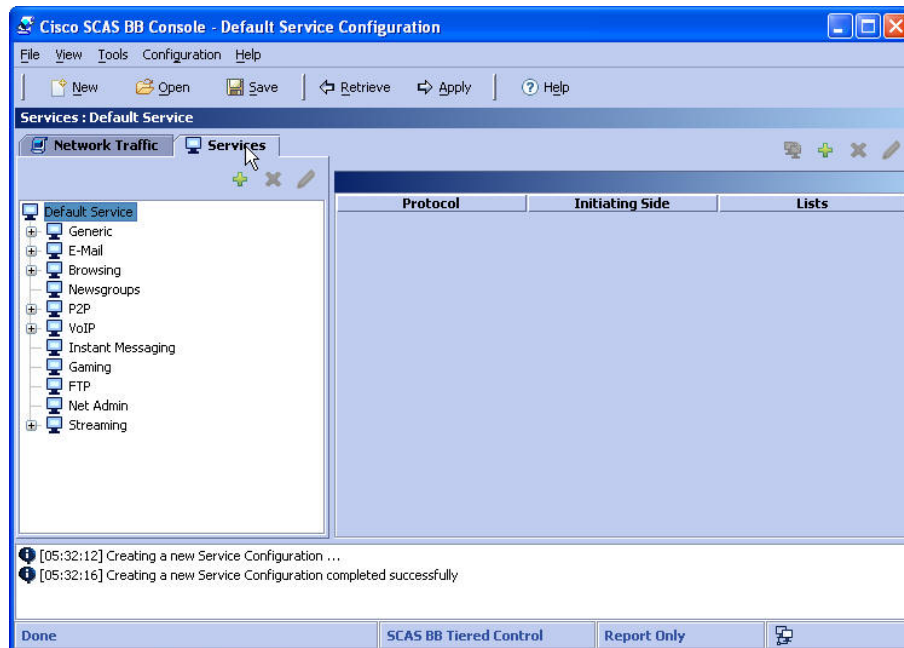
When a new Service Configuration opens, it contains the default configuration supplied with the Service Control Application Suite for Broadband.

Figure 4-2: New Service Default Configuration



The **Services** Band lists the predefined services supplied with the Service Control Application Suite for Broadband, and an associated transaction table appears in the *Main Window*.

Figure 4-3: New Service: Services Band



Saving the Current Service Configuration

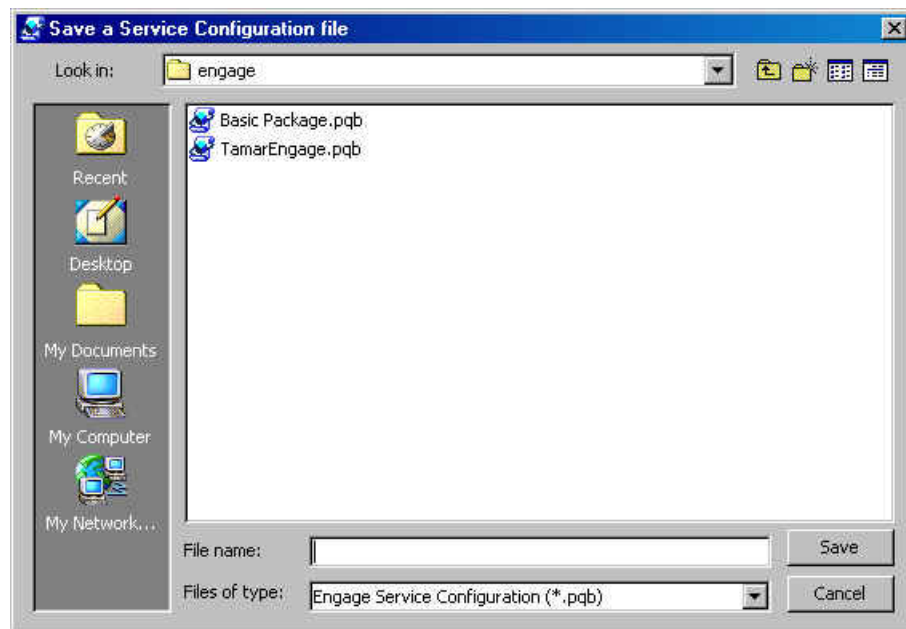
Use this procedure to save the Service Configuration currently open in the SCAS BB Console. All Packages, Services, and Lists that have been defined as part of the Service Configuration are also saved.

To save the current Service Configuration to a Service Configuration file:

Step 1 From the **File** menu, click **Save As**.

The *Save a Service Configuration* browser window appears.

Figure 4-4: Save Service Configuration Dialog



Step 2 From the *Files of Type* drop-down list, select **Service Configuration (*.pqb)**

Step 3 In the *File name* text box, type a new or existing filename, or use the browser to locate an existing pqb file.

Step 4 Click **Save** to save the Service Configuration to the selected file. If it is an existing file, this Service Configuration will overwrite the contents of the file.

During processing a *Saving Service Configuration File* message appears, and a confirmation message appears in the Message band when the process is complete.

To save the current Service Configuration to the currently open Service Configuration file:

Step 1 In the toolbar, click **Save** .

A confirmation message appears in the Message band when the process is complete.

Validating the Current Service Configuration

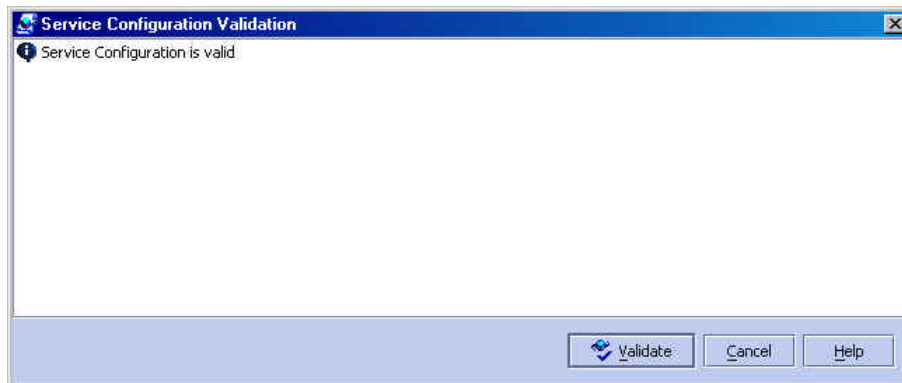
Use the **Validate** option to validate the new or updated Service Configuration currently presented on screen. The validation process checks for overall Service Configuration coherence, and points out possible pitfalls within the Service Configuration.

The **Validate** process is activated automatically by the **Apply** operation. The Service Configuration is validated and the *Service Configuration Validation* dialog box appears if the procedure found errors and/or issued warnings regarding the current Service Configuration.

To validate the current Service Configuration:

Step 1 From the **File** menu, click **Validate**.

The *Service Configuration Validation* dialog box appears.



The *Service Configuration Validation* dialog box can remain open while you use the validation messages to guide you as you fix the Service Configuration. You can move the screen aside and edit the Service Configuration.

Step 2 Click **Validate** to run the validation procedure after editing the Service Configuration.

The validation messages are updated.

Step 3 Click **Cancel**.

The *Service Configuration Validation* dialog box is closed.

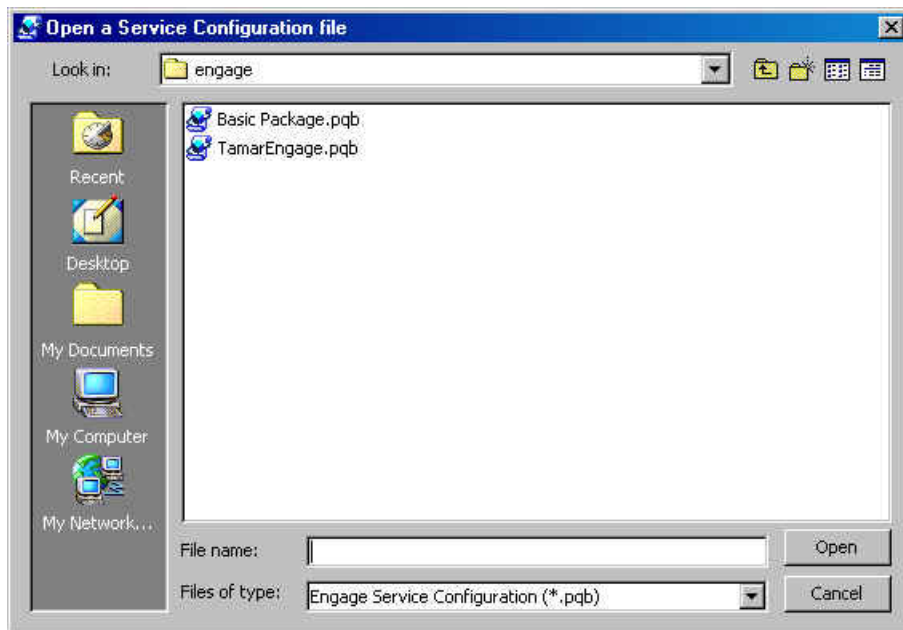
Opening an Existing Service Configuration

Use this operation to open a previously archived Service Configuration for viewing or editing.

To open a Service Configuration file:

- Step 1** From the toolbar, click **Open** .

The *Open a Service Configuration File* browser window appears.



- Step 2** From the *Files of Type* drop-down list, select **Service Configuration (*.pqb)**.
- Step 3** In the *File name* text box, type a *pqb* file name, or browse to retrieve the file.
- Step 4** Click **Open**.

A message entitled *Please Wait* containing the message "Opening Service Configuration File" appears. The Packages and Services that were stored in this Service Configuration file become available when the loading process is complete.

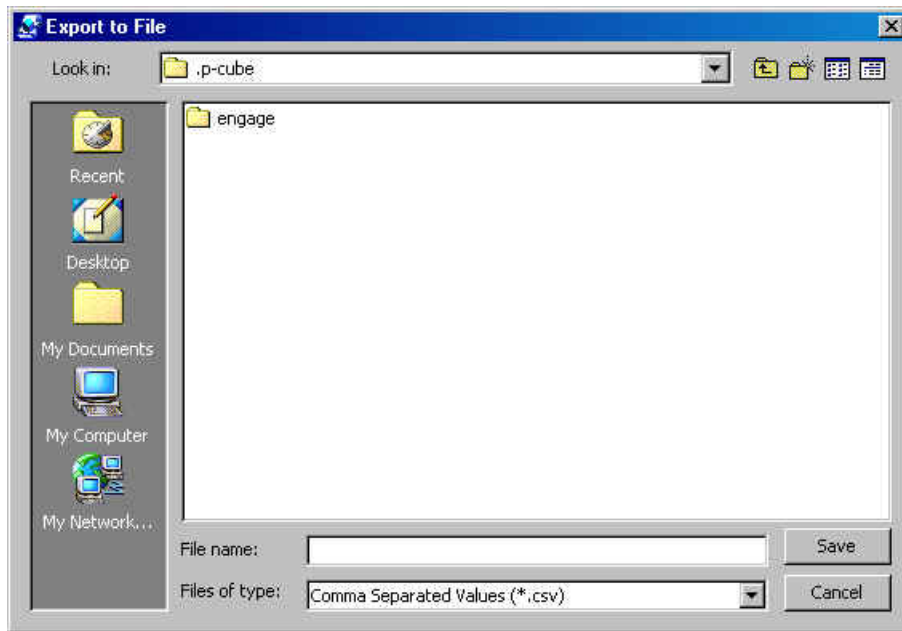
Exporting Packages, Services, Protocols and Lists

Use this option to export Packages, Services, Protocols and Lists to a *csv* file of your choice. You can create a new file or overwrite an existing one. The *csv* file formats are described in Exporting Policy Building Blocks to CSV File.

To export Packages, Services, Protocols or Lists:

Step 1 From the **File** menu, select **Export** and then click **Packages, Services, Protocols or Lists**.

The *Export to File* browser window appears.



Step 2 From the *Files of Type* drop-down list, select **Comma Separated Values (*.csv)**.

Step 3 Use the browser to select the file you want to overwrite

or

In the *File name* text box, type the name of the export file.

Step 4 Click **Save**.

The Packages, Services, Protocols or Lists are saved to a *.csv file.

Importing Packages, Services, Protocols or Lists

Use this option to import Packages, Services, Protocols or Lists from *csv* files into the current Service Configuration. (See *Exporting Policy Building Blocks to CSV File*, for information about *csv* import file formats.)

To import Packages, Services, Protocols or Lists:

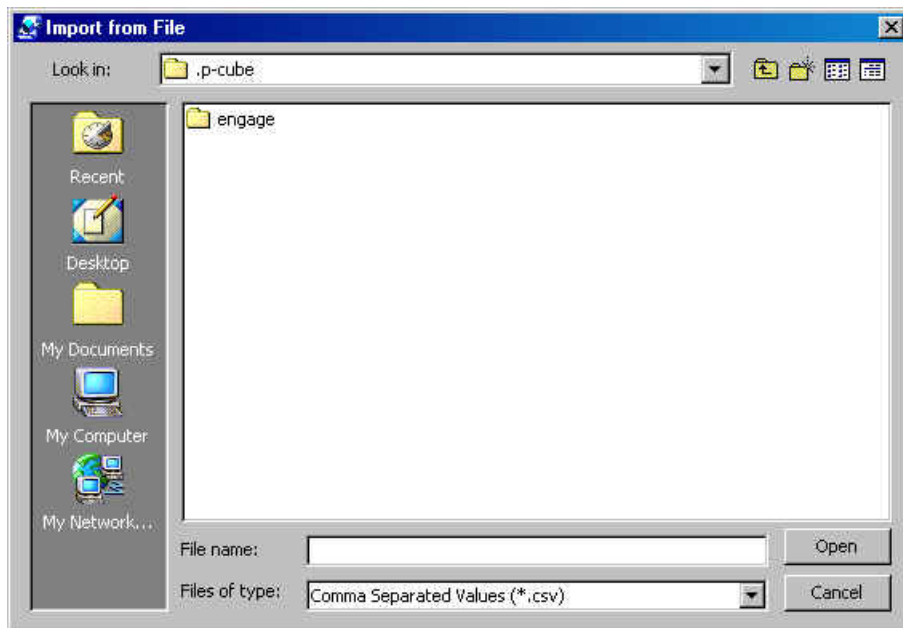
Step 1 From the **File** menu, select **Import** and then click **Packages, Services, Protocols or Lists**.

An *Import Warning* message appears.



Step 2 Click **Yes**.

The *Import from File* browser window appears.



Step 3 From the *Files of Type* drop-down list, select **Comma Separated Values (*.csv)**.

Step 4 Use the browser to find the file you want to import

or

In the *File name* text box, type the name of the file to import.

Step 5 Click **Open**.

The Packages, Services, Protocols or Lists are imported into the current Service Configuration domain.

Accessing the SCAS Reporter

The SCAS Reporter allows you to query the Collection Manager RDR database, and present the results in a chart or a table. This is a valuable tool for understanding the habits and resource consumption of the applications and subscribers that occupy your network. It can also be used for judging the efficacy of various Rules and the possible impact of their implementation on the network. You can view the reports in both tabular and chart formats, export them, save them, and edit their appearance. For more information, see *Generating Reports*.

The Reporter application must be installed on the same workstation as the SCAS BB Console.

To access the SCAS Reporter:

Step 1 From the **Tools** menu, click **Reporter**.

The SCAS Reporter application opens with the *Connect to Collection Manager* dialog box.

Accessing the SCAS BB SM GUI

The *SCAS BB* SM GUI lets you manage subscribers, assign packages to subscribers, edit subscriber parameters and manually add subscribers when dealing with a small number of subscribers.

For more information, see *Managing Subscribers* (on page 7-1).

To access the *SCAS BB* Subscriber Manager GUI:

Step 1 From the **Tools** menu, click **Subscribers Manager**.

The *SCAS BB* SM GUI application opens to the *Connect to SM* dialog box.

SCAS BB Licenses

Service Control Application Suite for Broadband offers three different levels of licensing to suit the needs of different sites:

- **SCAS BB View**: This is the basic form of *SCAS BB*. It has the following capabilities:
 - Monitoring and Reporting

- No control capabilities
- **SCAS BB Capacity Control:** This license adds traffic control functionality. It has the following capabilities:
 - Monitoring and Reporting
 - Capacity Control, for example by assigning traffic of different applications to different Global Controllers
 - One package only (default package) - no differentiation between subscribers.
 - requires a key
- **SCAS BB Tiered Control:** This license permits the differential control of traffic flows based on package. It has the following capabilities:
 - Monitoring and Reporting
 - Capacity Control
 - Multiple packages - allows differentiation between subscribers, for example by allowing greater BW or greater daily volume quota to subscribers of a certain package
 - requires a key

To register for a higher-level license:

Step 1 From the **Help** menu, click **License Manager**.

The *License Manager* dialog box appears.



Step 2 Check the **Enter new license key** checkbox.

The **Customer ID** and **Key** fields become available.

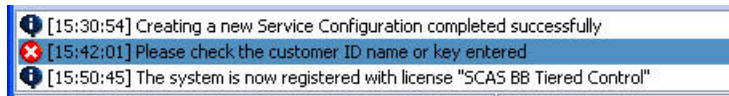


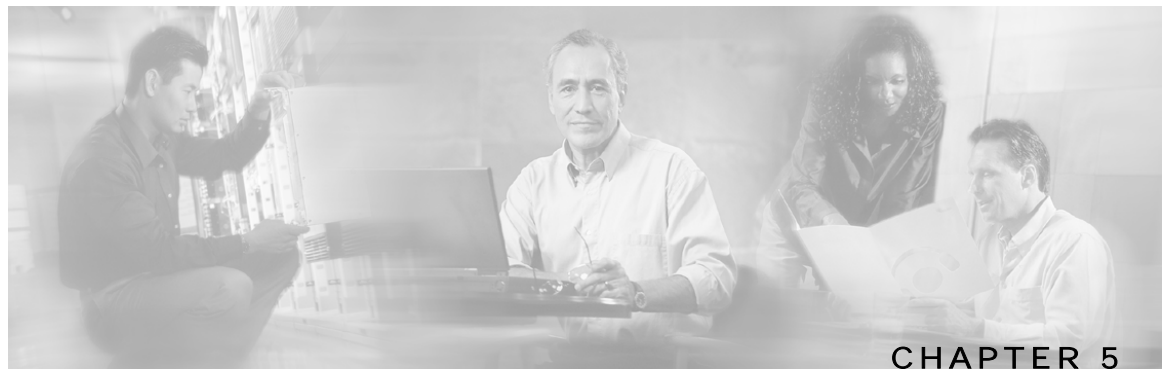
Step 3 Type your Customer ID and Key in the appropriate fields.

Step 4 Click **OK**.

The new license is displayed in the message band and status bar.

Figure 4-5: Displaying the New License





Constructing Service Configurations

A Service Configuration defines the behavior of the SCE Platform for the various traffic flows that it encounters. There are two general levels of processing:

- **Analysis and monitoring:** When using the *SCAS BB* Basic license (*SCAS BB* View), the Service Configuration defines the generation of RDRs for analysis and monitoring purposes.
- **Analysis, monitoring, and control:** When using *SCAS BB* Capacity Control or *SCAS BB* Tiered Control, the Service Configuration also translates the conditions of the various packages offered to the subscribers by the SP into rules that will be enforced on subscriber traffic by the SCE Platform. (See *SCAS BB Licenses* (on page 4-13).)

This chapter contains the following sections:

- [Service Configuration Overview](#) 5-2
- [Traffic Classification](#) 5-6
- [Traffic Control](#) 5-30
- [Packages](#) 5-40
- [Unknown Subscribers Traffic](#) 5-67
- [Weekly Time-Frames](#) 5-68
- [Bandwidth Control Revisited](#) 5-72
- [Managing RDR Settings](#) 5-75
- [Subscriber Notification](#) 5-85
- [Filtering the Traffic Flows](#) 5-89

Service Configuration Overview

A Service Configuration defines how the SCE Platform analyzes network traffic, what rules apply to the traffic, and what actions the SCE Platform should take in order to enforce these rules. Service Configurations are stored as PQB files.

A *Service Configuration* is a data structure that tells the SCE Platform how it should classify network transactions and how it should act upon these classified transactions. A Service Configuration is composed of the following two main elements:

- *Services*: define the categories to which transactions are classified
- *Packages*: define how the SCE Platform should act upon transactions from different Services.

Each subscriber must be assigned a package.

In addition, the following elements, which are the components of the service and package definitions, must be defined:

- *Protocols*: each Protocol is defined by the port and the transport type.
- *Lists*: lists of IP addresses or destination URLs
- *Global Controllers*: virtual queues that provide constraints for large, global, volumes of traffic, such as "Total P2P Traffic". Each global controller represents the percentage of total system bandwidth to be allotted to all traffic of a particular type.
- *Weekly Time Frames*: Up to ten *Calendars* can be defined, each with four different time frames, such as weekend, peak, or off-peak. This can be used, for example, to define different calendars for different time zones.

The Service Hierarchy

A *Service* is a basic entity that is provisioned and monitored by the SCE Platform. Service Control Application Suite for Broadband supports a maximum of 500 different defined services. A Service is a category of transactions that is defined by the following parameters of the transaction:

- *Protocol*
- Initiating side
- *List of IP address or destination URLs (optional)*

For example, an email service could be defined by protocol (POP and/or SMTP protocols), while specialized browsing services might be defined by protocol and destination URL list.

Services are arranged in a hierarchal tree. A single "Default Service" is at the root, and each new Service can be placed anywhere in the tree.

Services inherit the rule of their ancestors. When a rule is defined for a particular Service (in a specific Package) all its child services are controlled by the same rule for that package, unless explicitly specified.

Service Counters

Service hierarchy provides a way to share usage counters, as well as to organize services according to their semantics. Services are accounted in groups, through the hierarchy. Each service is assigned usage counters.

There are two categories of usage counters for services:

- Global (Link and Package RDRs & reports): maximum of 64 different exclusive global counters can be defined
- Subscriber (Subscriber RDRs & reports): maximum of 32 different exclusive subscriber counters can be defined

A global counter and a subscriber counter are assigned to each service. The usage of a Service can either be accounted exclusively for traffic classified to it, or in conjunction with traffic of its parent service. For example, if a Service “Premium Browsing” is defined as a child of “Browsing”, the operator can either define a special usage counter for Premium Browsing or configure it to use the same counter as “Browsing”. The two counters are independent, in other words, for the same service, one counter may be the same as the parent service, while the other is exclusive to the child.

The Package Hierarchy

A *Package* is a collection of settings that pertain to a specific group of subscribers (for example, "Gold Subscribers"). These settings are *Rules* that tell the SCE Platform how to act upon transactions of these subscribers, according to the transaction service. Separate rules may be assigned to different *Weekly Time Frames*, as defined in the *Calendar* assigned to the package. The package rules might be defined to permit access to only certain types of services, or to permit access to certain services on the weekend, but not during the week. A package might also permit access to a particular service, but put a limit on the volume that the subscriber may consume.

Service Control Application Suite for Broadband supports a maximum of 5,000 defined packages.

Packages are arranged in a hierarchal tree. A single “Default Package” is the root of the tree, and each new Package can be placed anywhere in the tree.

Each package can be assigned both upstream and downstream *Subscriber Bandwidth Controllers*. The BWCs limit the bandwidth of transactions, and can also prioritize transactions. In addition, they link services to specific *Global Controllers*, which limit total bandwidth of specific services or protocols, such as P2P protocols, in the total data traffic.

Each package is also assigned up to 16 quota buckets. Each bucket can be defined as either a volume bucket or a number of sessions bucket, and assigned a maximum capacity.

Finally, each package can be assigned a calendar with time frames appropriate to the package.

Package Counters

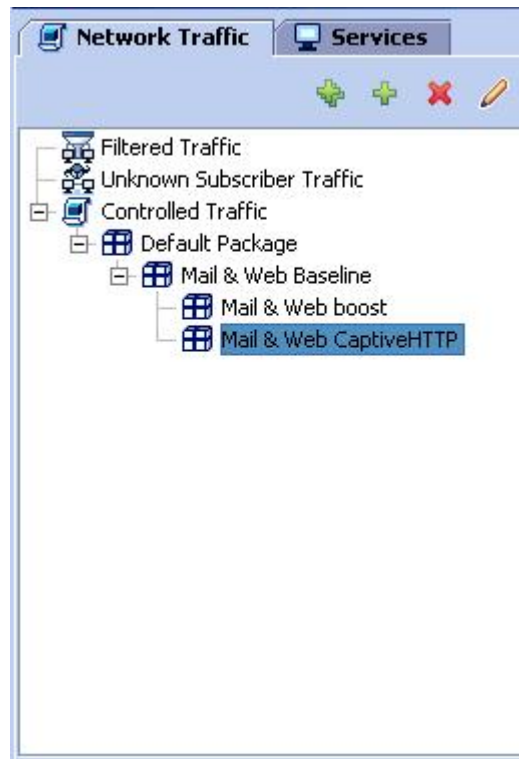
As with the service hierarchy, the package hierarchy provides a way to share package usage counters, as well as to organize services according to their semantics. A maximum of 64 different exclusive package counters can be defined, one of which is defined for the Unmapped Subscriber Traffic package.

Usage Reporting at a Package level is grouped as follows:

- Package assigned an exclusive package counter: all traffic associated with this package will be accounted separately in the assigned counter (along with any children that are not assigned exclusive counters).
- Package NOT assigned an exclusive package counter: all traffic associated with this package will be accounted together with its parent package.

For example, in the sample Package Hierarchy below, if “Mail & Web Baseline” is allocated an exclusive counter, but none of its child packages are, then all Package Usage Records and the derived reports (such as “Package Bandwidth per Service”) would group together usage of subscribers assigned to all three packages.

On the other hand, if, say the Mail & Web Boost package also had an exclusive counter, the traffic for Main & Web Baseline and Mail & Web Captive HTTP would be accounted together, while traffic for Mail & Web Boost would be accounted separately. (This is instructive as an illustration, but in general is not efficient as an actual configuration, since the hierarchical structure should be used to group packages that can use the same counter.)



Packages and Services

Following is a very general guideline to constructing a service configuration.

To construct a service configuration:

Step 1 Define all the basic elements of the configuration:

- protocols
- lists
- calendars
- global controllers

Step 2 Select the **Services** tab.

- Add new services to the Services hierarchy.
- Add new service elements (protocols) or edit existing elements.

Step 3 Select the **Network Traffic** tab.

- a) Add new packages to the Packages hierarchy.

Be sure to configure the proper range/number of the following elements for the package, so that appropriate specific elements are available for defining the service rules:

- Subscriber bandwidth controllers for each type of upstream and/or downstream traffic that you want to limit.
 - Quota buckets (volume and/or number of sessions).
 - Calendar with appropriate Time frame configuration.
- b) Add new rules (services) or edit existing rules.

Each package supports a maximum of 32 service rules. However, more than 32 services can be defined for a package if some services are children of others, since services inherit the rule of the parent service, unless explicitly defined otherwise.

For each service rule, assign the following:

- Subscriber bandwidth controllers
- Quota buckets
- Time frame (time-based rule only)

Step 4 From the **Configuration** menu, select **RDR Settings** to define all types of RDRs.

Traffic Classification

Traffic classification is the first step in constructing an Service Control Application Suite for Broadband service configuration. Traffic is classified according to services.

For each commercial service the providers offer to their subscribers, a corresponding service is defined in the *SCAS BB* solution for classifying and identifying the service, reporting on its usage, and controlling its traffic as required.

Services are classified on the basis of the following:

- **Protocol:** Utilizing the SCE Platform application-protocol awareness, the system classifies network traffic according to the protocol
- **Initiating side (optional):** Transactions can be classified to different services according to whether or not they were initiated by subscribers
- **Lists of network-side addresses (optional):** IP addresses or hostnames of the network-side host of the transaction.

Constructing and Modifying Services

It is recommended that you first define a variety of Services and only afterwards generate relevant Packages. The instructions in this section are independent of those in the section on constructing Packages.

Adding a New Service

Adding a new Service to the Services hierarchy is the first step in constructing a new Service.

When adding a Service, you will have to supply the following details:


- **Service name:** (*Services Settings Dialog Box - General Tab*). A unique name of your choice.
- **Description:** (*Services Settings Dialog Box - General Tab*). It is recommended that you use this box to record useful information about the Service.
- **Parent Service:** (*Services Settings Dialog Box - Hierarchy Tab*). By default, the parent is the Service currently selected. However, any other service may be selected from the drop-down list.
- **Service Usage Counters:** (*Services Settings Dialog Box - Hierarchy Tab*). Indicate whether the service will be assigned exclusive global and subscriber usage counters, or will use the counters of the parent service.

If exclusive counters are defined, the counter is automatically named the same name as the service, but you can define an index number for each exclusive counter.

- **Service Index:** (*Service Settings Dialog Box - Advanced Tab*). An identification number for a particular Service. There can be a maximum of 500 Services in the system. A specific Service can be governed by Service Rules in more than one Package. The SCE Platform recognizes Services by their index number, therefore, changing the Service name does not have an impact on the SCE Platform activity. The value of the Service Index is supplied automatically by the system and it is recommended that you do not modify this field.

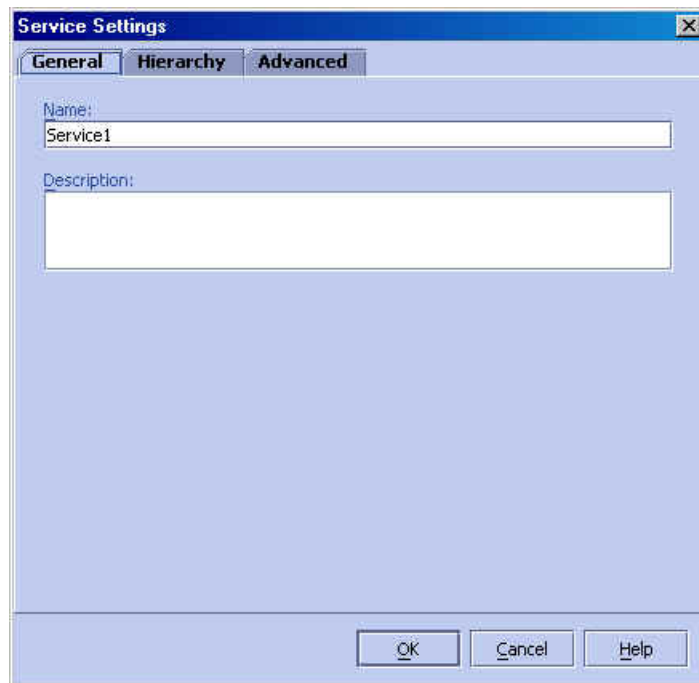
Adding a New Service Name and Description

To add a new Service name and description:

- Step 1** In the Services hierarchy, select the Service that will be the parent of the new service and click  (**Add**).

The *Service Settings* dialog box appears.

Figure 5-1: Service Management Dialog: General Tab



- Step 2** In the *Name* text box, type a unique and relevant Service name.

- Step 3** In the *Description* text box, type a meaningful and useful description of the Service.

If you want to define exclusive usage counters for this service, or if you did not select the proper parent service before clicking **Add**, skip to the instructions in the next section *Defining the Service Usage Counters* (on page 5-8).

- Step 4** Click **OK**.

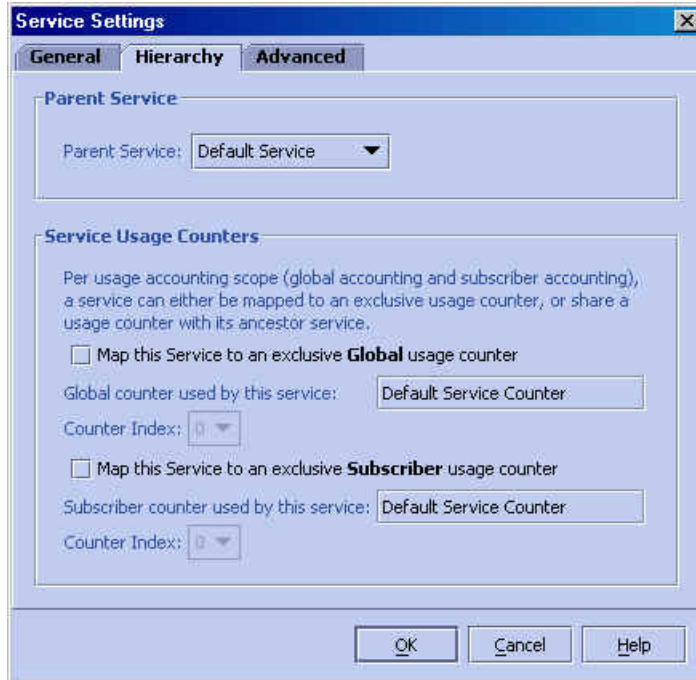
The Service is added to the Services band as a child to the service selected in the band.

Defining the Service Usage Counters

To define the Parent Service and the Service Usage Counters:

- Step 1** In the *Service Settings dialog box*, click the **Hierarchy** tab.
The *Service Settings Dialog Box - Hierarchy Tab* appears.

Figure 5-2: Service Settings Dialog Box - Hierarchy Tab



- Step 2** To define the Parent Service, select the desired service from the drop-down list.

- Step 3** To define the service usage counters:

- To share usage counter(s) with the parent service: Uncheck the "**Map this Service to an exclusive usage counter**" checkbox.

The counter name of the parent service appears in the usage counter name field

- To define exclusive usage counters: Check the "**Map this Service to an exclusive usage counter**" checkbox.

The name of this service appears in the usage counter name field.

If desired, select a counter index from the Counter Index drop-down list.

If you want to specify an index for this service, skip to the instructions in the next section *Setting the Service Advanced Options* (on page 5-9).

- Step 4** Click **OK**.

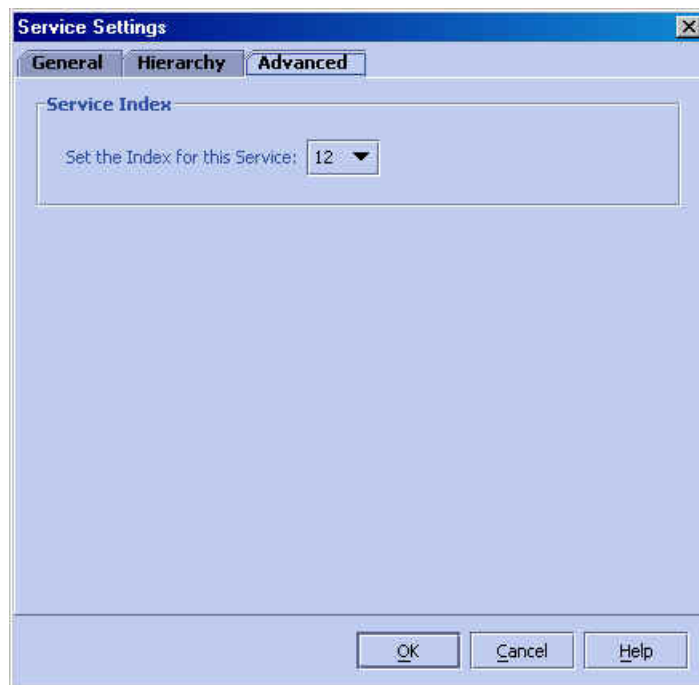
The Service is added to the Services band as a child to the selected parent service.

Setting the Service Advanced Options

To set the Service advanced options:

- Step 1** In the *Service Settings dialog box*, click the **Advanced** tab.
The *Service Settings Dialog Box - Advanced Tab* appears.

Figure 5-3: Service Settings Dialog Box - Advanced Tab



- Step 2** From the *Set the Index for this Service* drop-down list, select a Service Index.
The maximum value is 499.



Note The system automatically assigns a free number for a newly created Service. You should modify this number only in cases where a specific index value must be assigned to a specific Service.

- Step 1** Click **OK**.
The Service is added to the Services band as a child to the selected parent service.

You have now completed the first stage towards defining a new Service. The name of the new Service appears in the Services hierarchy. Go to the section *Defining Transaction Mapping for Services* ("[Defining Service Elements for Services](#)" on page 5-11) for instructions on how to add Service Elements to a service.

Editing Service Parameters

You can edit a Service parameter.

To edit a Service parameter:

Step 1 In the **Services** hierarchy, click the name of the Service you want to edit.

Step 2 From the Services band, click  (**Edit**).

The *Service Settings Dialog box - General Tab* appears, see *Adding a New Service Name and Description* (on page 5-7).

Step 3 Edit the Service definition as follows:

- Click the **General** tab to change the name or description of the Service.
- Click the **Hierarchy** tab to change the parent service or to change the usage counter configuration.
- Click the **Advanced** tab to change the Service index.

Step 4 Click **OK**.


The Service parameter(s) are changed.

Removing a Service

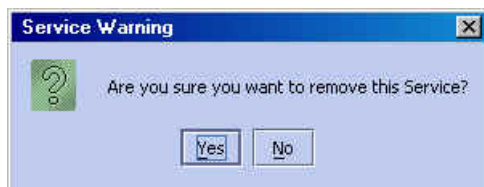
You can remove a Service.

To remove a Service:

Step 1 In the **Services** hierarchy, click the name of the Service you want to remove.

Step 2 In the Services band, click  (**Remove**).

The *Service Warning - Remove* message appears. If any Package has a Rule for this Service, an additional warning message, "All references to the service [service name] will be removed", is displayed.



Step 3 Click **Yes**.

The Service is removed from the Service hierarchy and is no longer available.

Children of the deleted service are not removed.

Defining Service Elements for Services

To complete the definition of a Service, you must define the service elements. The relevant Rule for each transaction is identified and executed based on the resolved Service and the Packages assigned to the Subscriber who generated the transaction.

A traffic flow considered an element of a specific service if it meets all three of the following criteria:

- It belongs to the specified Protocol
- It is initiated by the required side (network, subscriber, or either)
- The destination is an address that belongs to a specified List

Adding a Service Element


A Service is made up of Service Elements. A Service Element maps a specific Protocol, an initiating side, and associated Lists to the selected service.

- For more information on Protocols, see *Working with Protocols* (on page 5-20).
- For more information on Lists, see *Working with Lists* (on page 5-27).

Selecting a Protocol for a Service Element

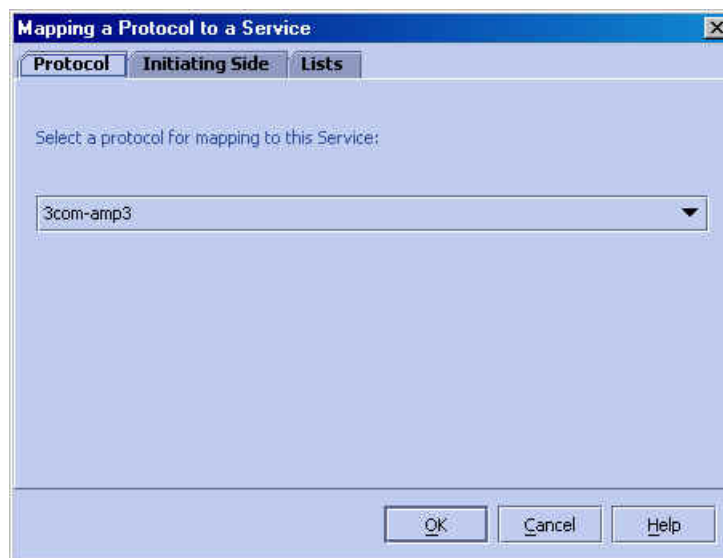
To select a protocol for a Service Element:

Step 1 In the Service hierarchy, click the Service for which you want to select a Protocol.

Step 2 In the Service Elements pane, click  (Add).

The following dialog box appears.

Figure 5-4: Mapping a Protocol to a Service



Step 3 Click the **Protocols** tab.

Step 4 From the *Select a protocol for mapping to this Service* drop-down list, select a Protocol.

If you want to define the service only for a particular initiating side, skip to the instructions in the next section *Selecting a Transaction Mapping Initiating Side* ("[Selecting an Initiating Side](#)" on page 5-12).

Step 5 Click **OK**.

A transaction mapping has been added to the Service selected in the Services band.

Selecting an Initiating Side

Use this dialog box to determine the initiating side(s) of transactions that will be mapped to this Service. The system supports the following initiating side definitions:

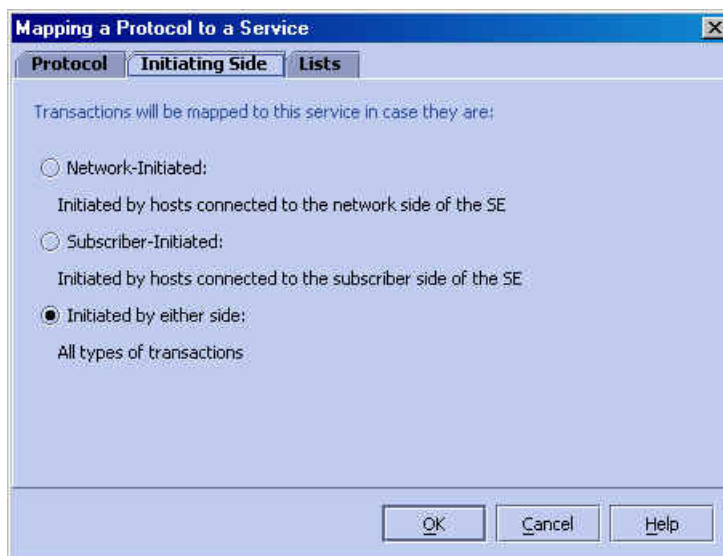
- *Network-Initiated*: transactions that are initiated at the network side towards (a server) at the subscriber side.
- *Subscriber-Initiated*: transactions that are initiated at the subscriber side towards (a server) at the network side
- *Initiated by either side*: default

To select a direction for a protocol mapped to a Service:

Step 1 From the *Mapping a Protocol to a Service* dialog box, click the **Initiating Side** tab. See *Selecting a Protocol for a Service Element* (on page [Error! Bookmark not defined.](#)).

The following dialog box appears.

Figure 5-5: Mapping a Protocol to a Service: Direction Tab



Step 2 Select one of the three options:

- Network-Initiated
- Subscriber-Initiated
- Initiated by either side

If you want to associate Lists to the Mapping, skip to the instructions in the section *Selecting Mapping Lists* ("[Selecting Lists](#)" on page 5-13).

Step 3 Click **OK**.

A initiating side has been selected for the Service Element.

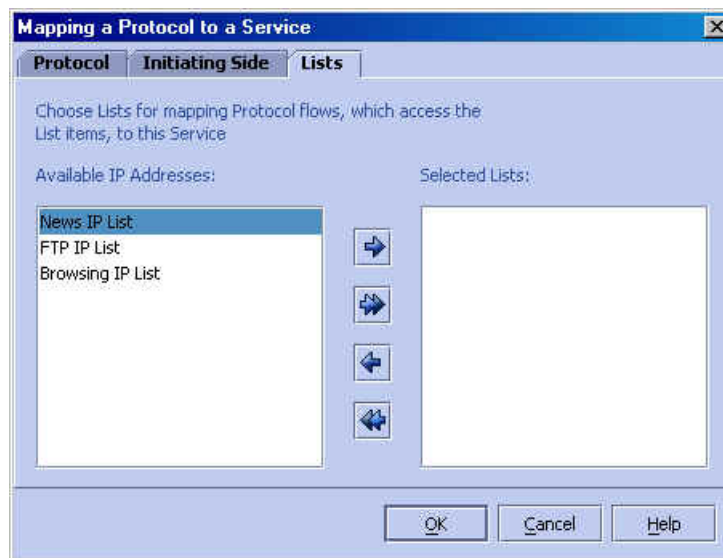
Selecting Lists

To select Lists for a specific Service transaction mapping:

Step 1 From the *Mapping a Protocol to a Service* dialog box, click the **Lists** tab. See *Selecting a Protocol for a Service Element* (on page 5-11) .

The following dialog box appears.

Figure 5-6: Mapping a Protocol to a Service: Lists Tab

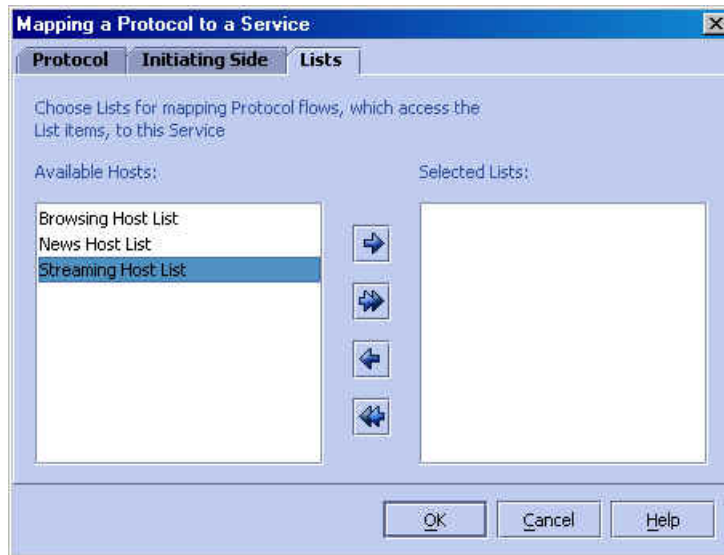


Step 2 Select a List from the *Available Hosts/Available IP Addresses* list box.

**Note**

The title and contents of the Lists that appear (in the left hand list-box of the **Lists** tab), vary depending on the protocol's supported List type.
Available Hosts is the title and content when the selected protocol is HTTP Browsing, HTTP Streaming, RTSP Streaming, or SMTP based.
Available IP Addresses is the title and content for all Protocols. For example, if you select the FTP protocol, the FTP supported list-type is IP Addresses, and the left hand list-box will show *Available IP Addresses*.

Figure 5-7: Mapping a Protocol to a Service: Lists Tab (Hosts)



- Step 3** Click / to shift the selected list(s) to the *Chosen Lists* list box.
- Step 4** Repeat the previous two steps until you have transferred all the lists that you want to transfer.

**Note**

You can use the "Shift-All" command button to shift all the lists from one list box to the other.

- Step 5** Remove a list from the **Chosen Lists** list box by selecting it and clicking / .
- Step 6** Repeat the previous two steps until you have transferred all the lists that you want to transfer.
- Step 7** Click **OK**.

You have defined the types of transactions that will be mapped to the Service selected in the Services band.



Note When a protocol is selected, the set of selected Lists is emptied. Therefore, if you select the desired lists, and then return to the **Protocol** tab to select a different protocol (if, for example, you selected the wrong one initially), there will be no lists selected for that protocol. You must return to the **Lists** tab and make your selections a second time.

Editing a Service Element

To edit a service element:


- Step 1** In the Services hierarchy, click the name of the Service you want to edit.
A list of associated service elements will appear in the SCAS BB Console Main Window.
- Step 2** Click the name of the service element that you want to edit.
- Step 3** From the SCAS BB Console Main Window, click  (**Edit**).
The *Mapping a Protocol to a Service* dialog box, illustrated in *Mapping a Protocol to a Service* (on page [Error! Bookmark not defined.](#)) appears.
- Step 4** Click the tab that contains the parameters to be edited.
Use the following reference list in the table below.
- Step 5** Click **OK**.
The changes are saved.


Table 5-1 Service Management Reference List

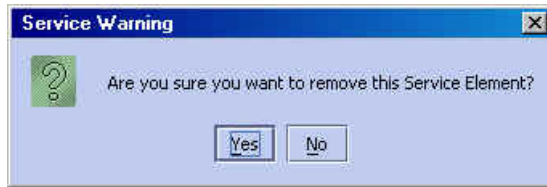
Tab Name	Instructions
Protocol	See <i>Selecting a Protocol for Mapping to a Service</i> (Selecting a Protocol for Mapping to a Service " Selecting a Protocol for a Service Element " on page 5-11).
Direction	See <i>Selecting a Transaction Mapping Initiating Side</i> (" Selecting an Initiating Side " on page 5-12).
Lists	See <i>Selecting Mapping Lists</i> (" Selecting Lists " on page 5-13).

Removing a Service Element

You can remove any service element when necessary.

To remove a service element:

-
- Step 1** In the Services hierarchy, click the name of the Service that has a service element that you want to remove.
- Step 2** In the **Service Element** table, click the name of the transaction mapping definition that you want to remove.
- Step 3** From the SCAS BB Console Main Window, click  (**Remove**).
- A *Service Warning - Remove Service Element* message appears.




- Step 4** Click **Yes**.
- The service element is removed and is no longer part of the selected Service.
-

Moving a Service Element

You can move an existing service element from one service to a different service.

To move a service element:

-
- Step 1** In the Services hierarchy, click the name of the Service you want to edit.
- A list of associated service elements will appear in the SCAS BB Console Main Window.
- Step 2** Click the name of the service element that you want to edit.
- Step 3** From the SCAS BB Console Main Window, click  (**Move Service Element**).
- The *Move Service Element* dialog box, appears.
- Step 4** From the drop-down list, select the service to which you want the element to be moved .
- Step 5** Click **OK**.
- The service element is moved to the selected service.
-

Managing Protocols

In this section you will learn about Protocols, how to set them up and how to manage them.

Protocols are used for defining Service Elements (see *Defining Transaction Mapping for Services* ("[Defining Service Elements for Services](#)" on page 5-11)).

Protocols

A Protocol is composed of an application protocol, the destination port(s), a unique name and a description (optional). The ability to define and recognize a differentiation between protocols is a powerful tool for service provisioning and billing in a subscriber-based environment.

Protocols are divided into four groups:

- **Generic Protocols:** Generic IP, Genetic TCP and Generic UDP protocols, used for transactions that were not specifically mapped to a service by one of the more specific protocol types below
- **IP Protocols:** Non TCP/UDP protocols (such as ICMP), identified according to the IP protocol number of the transaction
- **Port-based Protocols:** TCP and UDP protocols that are classified according to their well-known ports. The default configuration includes more than 600 common port-based protocols.

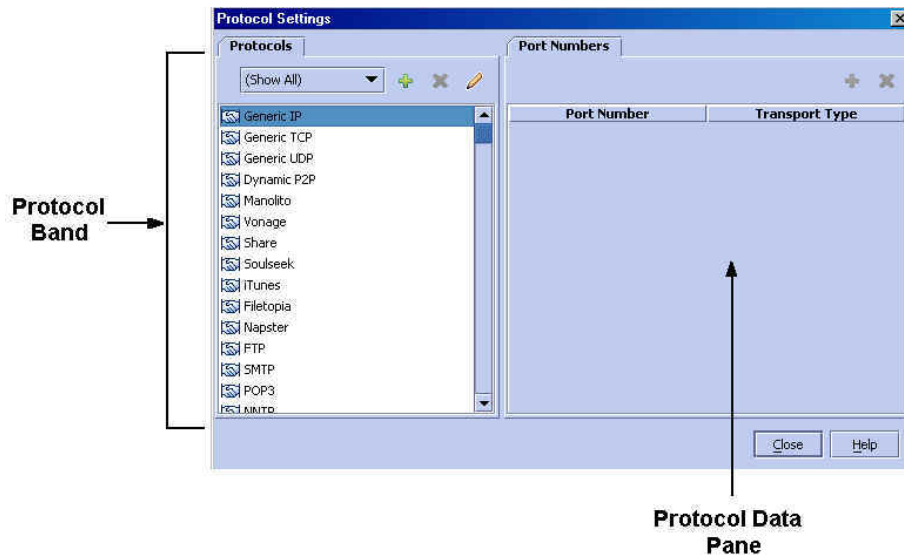
You may add new protocols (for example, to classify a certain gaming protocol that uses a specific port) and edit or remove existing ones.

- **Signature-based Protocols:** Protocols classified according to a Layer7 application signature. This group includes the most common protocols, such as HTTP and FTP, as well as a large group of popular P2P protocols.

The Service Control Application Suite for Broadband supports many commercial and common protocols. For a complete list of protocols, see *Protocol Reference Tables* (on page [B-1](#)).

Protocol Settings Screen

Figure 5-8: Protocol Settings Screen



The Protocol Settings screen is divided into two panes. The left pane is the *Protocols* band. The right pane is the *Protocol Data Window*.

The Protocols band contains the list of Protocols that were defined for the system. Located at the top right hand corner of the band, are three command buttons: **Add**, **Remove** and **Edit**.

Use these buttons to create, edit, and remove Protocols. To do so, you need to know the following information:

Table 5-2 Protocol Definition Parameters

Field	Description	Comments
Protocol name	Descriptive name for the newly created Protocol.	
Description	Descriptive information about the Protocol.	Optional
Supported List Type	List type that can be associated with this protocol when defining services using this protocol: <ul style="list-style-type: none"> • Hosts • IP addresses 	This field can only be configured in a few protocols (http browsing, http streaming, rtsp, smtp). All other protocols support only IP address lists .

Use the information in this table when constructing or editing a Protocol.

Protocol Data

The right side of the Protocol Settings screen displays the protocol data. When a Protocol is selected in the Protocols band, the configured sets of **Port Numbers** are displayed in the Protocol Data pane.

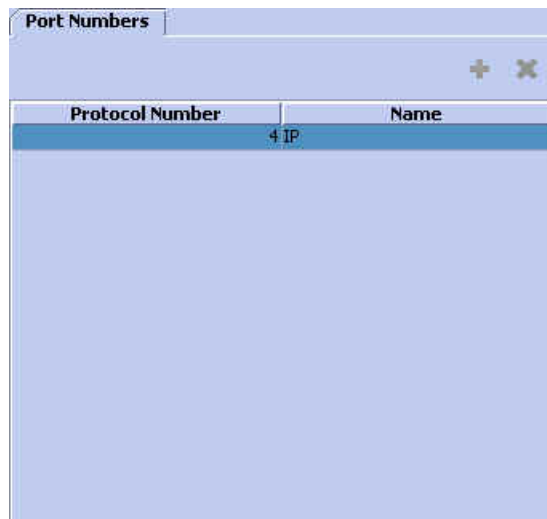
These items appear in a table with two columns:

- Port Number
- Transport Type

The Protocol Data pane for IP protocols differs from that for other protocols. The table contains the following two columns:

- Protocol Number
- Name

Figure 5-9: Protocol Settings: IP Protocols



Protocol Number	Name
4	IP

Located at the top right hand corner of this window are the command buttons, **Add** and **Remove**. Edit the contents of a field within the table by clicking on the cell you want to edit.

Use the Port Numbers feature to define additional "well-known" ports for predefined Protocols. There are two basic rules to consider when assigning a port number and type to a Protocol:

- You can assign additional port numbers to Protocols. In case of a duplicate port mapping, an error message appears preventing the requested assignment.
- Note that it is possible to remove all assignments (including the defaults) for a certain Protocol. For example, you can remove the assignment of port 80 to an HTTP type protocol.

Working with Protocols

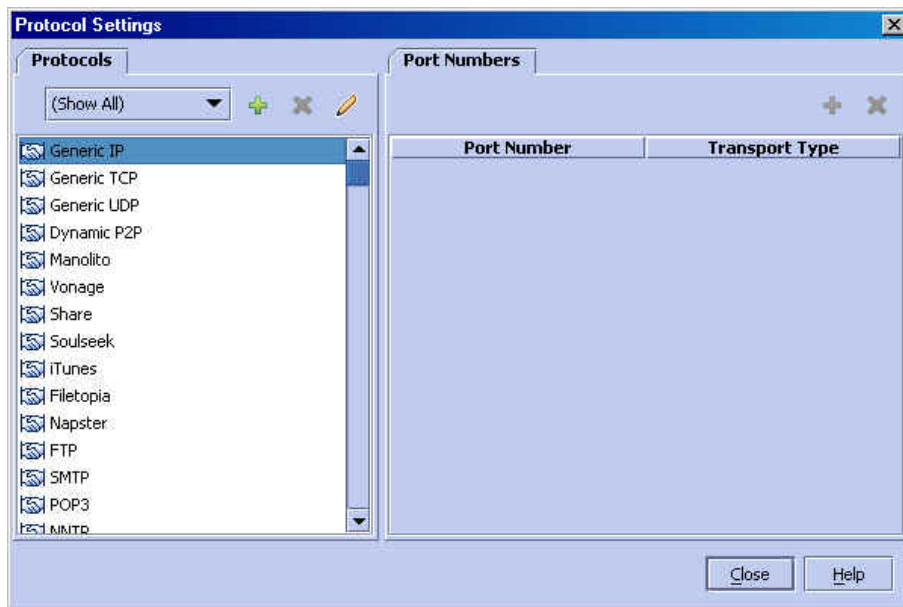
In this section you will learn the procedures for setting up a Protocol.

To access the Protocol Settings Screen:

Step 1 From the **Configuration** menu, click **Protocols**.

The *Protocol Settings* screen appears.

Figure 5-10: Protocol Settings Dialog



Using and Filtering The Protocols View

The listing of protocols is displayed according to type in the following order:

- generic protocols
- signature-based protocols: sorted by port numbers
- IP protocols: sorted by protocol number
- port-based protocols: sorted by port numbers

To quickly access a protocol, type its first letter in the protocol list. The next protocol starting with this letter is brought to view. Since protocols are displayed by type and port number, not alphabetically, you may need to press the letter again until the requested protocol is brought to view.

You can filter the protocols by type, so that the listing displays only the selected type of protocol. Display options are:

- show-all

- generic protocols
- IP protocols
- port-based protocols
- signature-based protocols

To filter the Protocol Settings Screen:


-
- Step 1** From the **Protocols** drop-down listing, select the type of protocols to be displayed. The protocols of the selected type appear in the listing.
-

Editing Protocols

You can edit the protocol name, description, and/or associated list type.

Editing the Protocol name and description

To edit a Protocol name and description

-
- Step 1** To access the Protocol Settings Screen:
Follow the procedure in the section *Working with Protocols* (on page 5-20).
- Step 2** On the Protocols band, select the Protocol you want to edit.
- Step 3** From the Protocols band, click  (**Edit**).

The *Protocol Settings Dialog Box - General Tab* appears, as illustrated in the following figure. (If the selected Protocol supports either IP addresses or host names, the *Supported List Type* tab also appears in the dialog box.)

Figure 5-11: Protocol Settings Dialog Box - General Tab



- Step 4** In the *Name* field, type a new protocol name.
- Step 5** In the *Description* field, edit the description of the Protocol.
- Step 6** Click **OK**.

The Protocol is changed.

Editing the Protocol supported list type

All protocols can be associated with lists of IP addresses. HTTP Browsing, HTTP Streaming and RTSP and SMTP protocols can be associated with Lists of IP addresses or host names.

To edit the Protocol supported list type


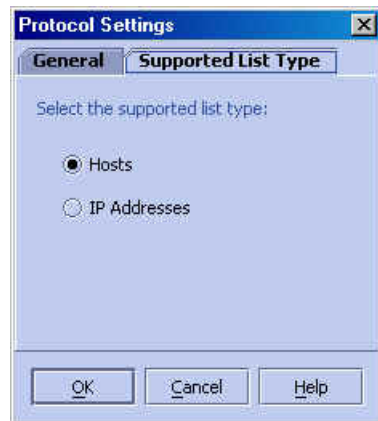
- Step 1** To access the Protocol Settings Screen:
Follow the procedure in the section *Working with Protocols* (on page 5-20).
- Step 2** On the Protocols band, select the Protocol you want to edit.
- Step 3** From the Protocols band, click  (**Edit**).
The *Protocol Settings Dialog Box – General and Supported List Type Tabs* appears, see figure below.
- Step 4** Click the **Supported List Type** tab.
The *Protocol Settings Dialog Box - Supported List Type Tab* appears.

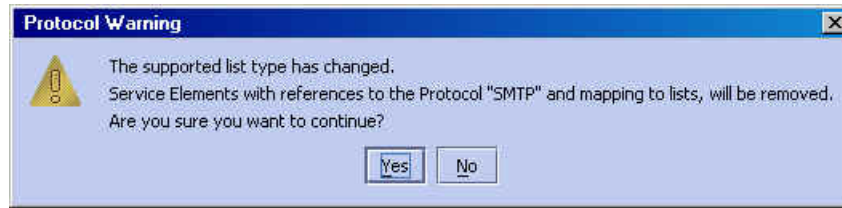
Figure 5-12: Protocol Settings - Supported List Type Tab



- Step 5** Select one of the following options:
- **Hosts:** Supports differentiation of traffic flows based on the host name of the network side of the session. Not all protocols support this option.
 - **IP Addresses:** The match is dependant on matching the prefix to receive a range of IP addresses. The match is with the network side IP address of the session.

Step 6 Click **OK**.

A *Protocol Warning - Supporting List Type* message appears.

**Step 7** Click **Yes**.

The supported list type is changed.


Removing Protocols

Only port-based protocols can be removed.

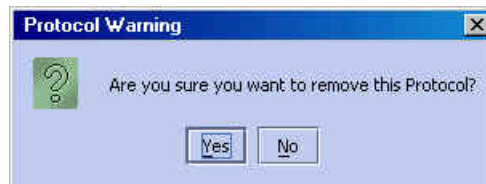
To remove a Protocol

Step 1 To access the Protocol Settings Screen:

Follow the procedure in the section *Working with Protocols* (on page 5-20).

Step 2 On the Protocols band, select the Protocol you want to remove.**Step 3** From the Protocols band, click  (**Remove**).

A *Protocol Warning - Remove Protocol* message appears.

**Step 4** Click **Yes**.

The Protocol is removed from the Protocols band.

Adding Protocols

Use this option to define Protocols.

To construct a new Protocol:

Step 1 To access the Protocol Settings Screen:

Follow the procedure in the section *Working with Protocols* (on page 5-20).

Step 2 On the Protocols band, click  (**Add**).

The *Protocol Settings Dialog Box - General Tab* appears.

Figure 5-13: Protocol Settings Dialog Box - General Tab



Step 3 In the *Name* field, type a unique name for the new Protocol.

Step 4 (Optional) In the *Description* field, type a meaningful description of the Protocol.

Step 5 Click **OK**.

The new Protocol appears in the Protocols Band. You can now add relevant port numbers, see *Adding Protocol Data* (on page 5-24).

Adding Protocol Data

Under some circumstances you can add protocol data, port numbers or protocol numbers, to the protocol. Follow these guidelines:

- You can only add port numbers to port-based and signature-based protocols
- IP protocols have defined protocol numbers, not port numbers
- For the following protocols you cannot add/edit ports directly, as they share the port configuration of the corresponding protocol (second of the pair)
 - FastTrack KaZaA File Transfer/(FastTrack KaZaA Networking)

- Gnutella File Transfer/(Gnutella File Networking)
- HTTP Streaming/(HTTP Browsing)

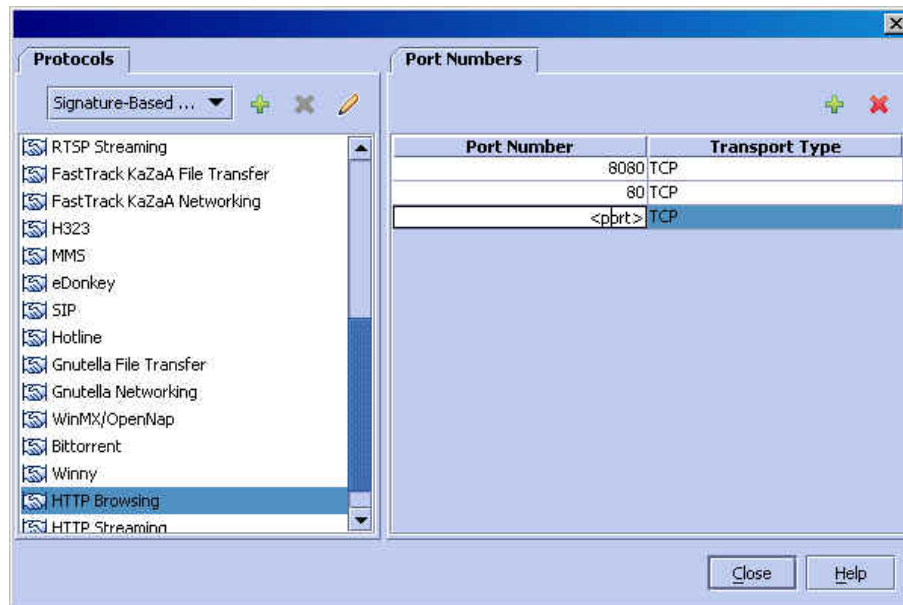
To add a port and transport type to a Protocol:

Step 1 Click on a Protocol in the Protocols band.

Step 2 In the Protocol Data pane, click  (Add).

A line is added in the Port Numbers table with <port> in the *Port Number* column and a *Type* (depends on the base communication protocol).

Figure 5-14: Protocol Settings: Adding a Port



Step 3 In the *Port Number* column, double-click in the field and type the new value.

Step 4 In the *Transport Type* column, select the *Transport Type* from the drop-down list.

The port number and transport type are added to the Port Numbers table.

Editing Protocol Data

Refer to the restrictions noted under *Adding Protocol Data* (on page 5-24).

To edit the port number and type definition of a Protocol:

Step 1 Click on a Protocol in the Protocols band.

Step 2 Click on the cell you want to change.

Step 3 In the *Port Number* column, type the new value.


Step 4 Click on the *Transport Type* cell you want to change.

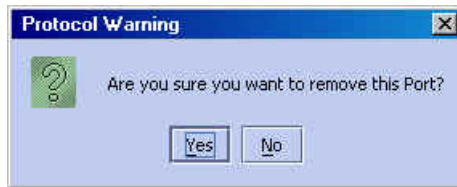
Step 5 In the *Transport Type* column, *Transport Type* from the drop-down list.

The port number and/or transport type are changed.

Removing Port Numbers

To remove a port number and type definition from a list of items:

- Step 1** Click on a Protocol in the Protocols band.
- Step 2** In the Port Numbers table, click on the line that you want to remove.
- Step 3** In the Port Numbers pane, click  (**Remove**).
A *Protocol Warning - Remove Port* message appears.



- Step 4** Click **Yes**.
The port is removed from the Port Numbers table.
-

Managing Lists

In this section you will learn about Lists, how to set them up and how to manage them.

List Types

Use Lists to classify network sessions, assigning them to distinct Services based on their destination. A List can be one of the following types of lists:

- **IP Addresses:** The List elements are IP addresses or ranges of IP addresses.
- **Hosts:** The List elements are URLs.

The URL is composed of the URL hostname and the URL path, separated by a colon, with optional wildcards, in the following format:

```
*<host-suffix>:<path-prefix>*
```

For example, the following URL:

```
*.yahoo.com:/en/*
```

would match both the following:

```
www.yahoo.com/en/index.html and image.yahoo.com/en/main.jpg
```

Working with Lists

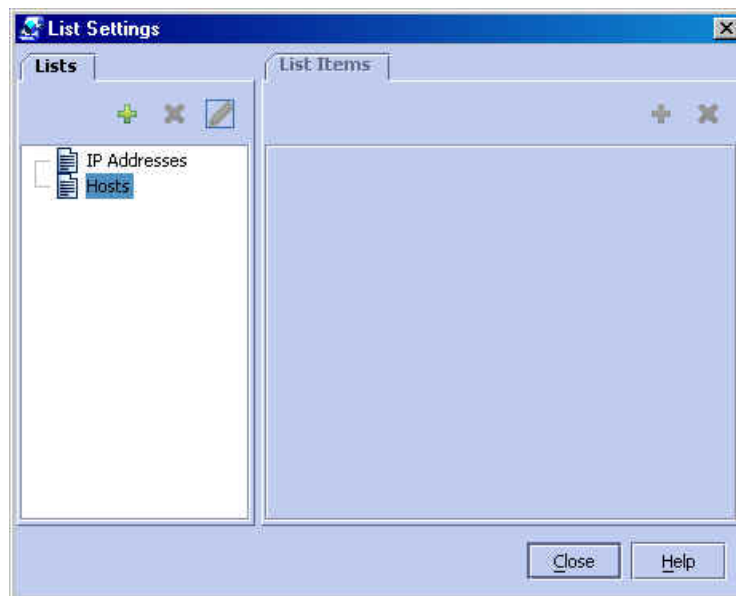
In this section you will learn how to set up a List.

To access the List Settings Screen:

Step 1 From the **Configuration** menu, click **Lists**.

The *List Settings* screen appears.

Figure 5-15: List Settings



In the example in the figure above, the *News* list is located under the *Hosts* hierarchy. The associated list items are URLs.


Adding a List

To add a new List:

Step 1 To access the List Settings Screen

Follow the procedure in the section *Working with Lists* (on page 5-27).

Step 2 In the List band, point to the selected list type.

Step 3 From the List band, click  (**Add**).

The *List Settings* dialog box appears.

Figure 5-16: List Settings: General Tab




- Step 4** In the *Name* text box, type a unique name for the new List.
- Step 5** In the *Description* text box, type a meaningful description of the List.
- Step 6** Click **OK**.

The new List appears in the Lists band under the selected List Type. You can now add relevant List Items, see *Adding a List Item* (on page 5-29).


Editing a List

To edit a List:

- Step 1** To access the List Settings Screen
Follow the procedure in the section *Working with Lists* (on page 5-27).
- Step 2** On the List band, select the List you want to edit.
- Step 3** From the List band, click  (**Edit**).
The *List Settings* dialog box appears (see *Adding a List* (on page 5-27)).
- Step 4** In the *Name* text box, type the new name.
- Step 5** In the *Description* text box, edit the description of the List.
- Step 6** Click **OK**.
The List is changed.


Removing a List

To remove a List:

- Step 1** To access the List Settings Screen
Follow the procedure in the section *Working with Lists* (on page 5-27).
- Step 2** On the List band, select the List you want to remove.
- Step 3** From the List band, click  (**Remove**).
The List is deleted and removed from the List band.
-

Adding a List Item

To add a relevant item to a List:

- Step 1** Click on a List in the List band.
- Step 2** In the List Items window, click  (**Add**).
A new line is added to the List Items table.
- Step 3** Double-click the new list item, type a new value and press **Enter**.
- Valid values for host lists are URLs (such as www.yahoo.com/en/index.html).
 - Valid values for IP lists are IP addresses (such as 63.111.106.7) or IP ranges (such as 194.90.12.0/24).
-


Editing a List Item

To edit a list item:

- Step 1** Click on a List in the List band.
- Step 2** Double-click on the **List Items** cell you want to change.
- Step 3** Type the new value and press **Enter**.
The list item is changed.
-

Removing a List Item

To remove a list item:

-
- Step 1** Click on a List in the List band.
- Step 2** Click on the line you want to remove.
- Step 3** From the List Items window, click  **(Remove)**.
The list item is removed.
-

Traffic Control

Traffic control is the more advanced functionality of the Service Control Application Suite for Broadband solution, and is available only with the *SCAS BB* Capacity Control and *SCAS BB* Tiered Control licenses. Therefore, most of the options and procedures addressed in this section are not available to the users of *SCAS BB* View.

Overview of Bandwidth Control

Bandwidth control in the Service Control Application Suite for Broadband solution is accomplished in two stages:

- Global control
- Subscriber bandwidth control

Global Control

Bandwidth is controlled in the SCE Platforms by the use of virtual queues, or Global Controllers. You can configure a maximum of 16 Global Controllers per interface (upstream/downstream). As these are global controllers, their configuration is not linked to a package, but rather they are configured for the entire system.

The purpose of the global controllers is to provide constraints for large, global, volumes of traffic, such as "Total Gold Subscriber Traffic", or "Total P2P Traffic", as opposed to controlling bandwidth at the subscriber level. Each global controller represents the percentage of total system bandwidth that you want to allot to all traffic of a particular type. P2P traffic provides a good illustration, as the volume of P2P traffic has increased to the point where it causes significant problems for many ISPs. Using the global controller, you can limit total P2P traffic in the system to any desired percentage of total traffic bandwidth, keeping the amount of total traffic bandwidth consumed by P2P traffic constant and under control.

Subscriber Bandwidth Control

A Subscriber Bandwidth Controller (BW Controller) controls the entire subscriber's traffic or some portion of it. A BW Controller is specified by the following main parameters: CIR and PIR.

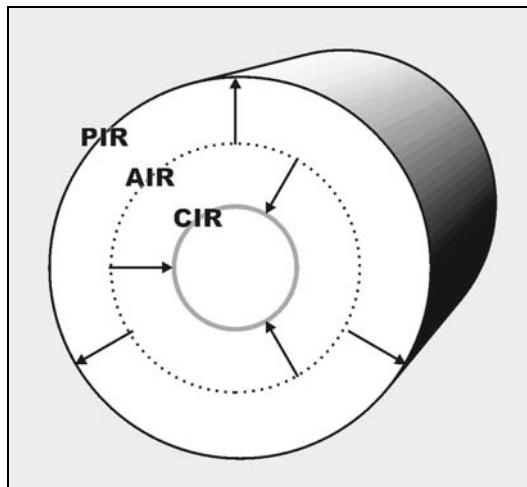
- Committed Information Rate (**CIR**): Defines the minimal bandwidth that must be granted to traffic that is controlled by the BW Controller.
- Peak Information Rate (**PIR**): Defines the maximal bandwidth allowed to that traffic.

PIR can be thought of as the "width" of the virtual pipe. To continue with this analogy, assume that the pipe is flexible and may adjust in width. CIR is therefore the minimal "width" the pipe can contract to. During network congestion, the system contracts each pipe differently to differentiate between subscribers and between their Services.

The pipe width in this analogy defines the total bandwidth (Admitted Information Rate (AIR)) allowed to cross the pipe. Therefore, AIR ranges between CIR and PIR. The consumed bandwidth (UIR) is the rate that currently flows through the BW Controller and it is always below AIR.

It might be that the traffic associated with the BW Controller does not consume much bandwidth at a certain moment. However, in case it does demand a growing amount of bandwidth, the BW Controller should ensure that at least the CIR amount will be granted, even in conditions of network congestion (PIR-congestion). Similarly, BW Controller should ensure that no matter of congestion conditions, the traffic associated with a BW Controller would always be below the PIR limit.

Figure 5-17: Bandwidth Control Levels



In the figure above, the small (green) circle indicates CIR. The big circle (red) indicates PIR. The dashed Circle indicates AIR - the maximal rate currently allowed to flow through the BW Controller, $CIR < AIR < PIR$. As specified above, UIR - the rate that currently flows through the BW Controller, can be smaller than CIR, $0 < UIR < AIR$.

The BW Controller has a third parameter that controls how AIR is determined at different congestion conditions. As indicated, when the network is not congested the system should provide PIR and when the network is highly congested the system should provide CIR. In between these two extremes, the AIR is determined by a third parameter - Assurance Level (AL). AL controls how fast AIR would decrease from PIR to CIR as congestion builds, or increase from CIR to PIR as congestion decreases. A higher AL ensures a higher AIR compared to a similar BWC with a lower AL.

Controlling Traffic in Two Levels: Total and Internal

Subscriber BW Controllers enforce bandwidth in two levels.

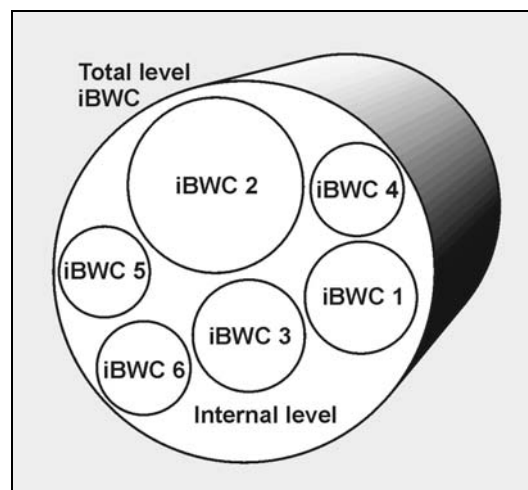
The first level, Primary BW Controller (Total) specifies bandwidth Service Configurations that the provider enforces on its subscribers.

The second level, BW Controller (Internal) specifies Service Configurations that the subscriber wishes to enforce on its Services.

Service Control Application Suite for Broadband provides each subscriber with an independent set of BW Controllers. A single BW Controller is used to control the total bandwidth of the subscriber. This BW Controller is referred as the Primary BW Controller and its corresponding parameters are referred as CIR and PIR.

The other BW Controllers control the bandwidth of some Services of that subscriber. For example, one BW Controller may control the Streaming Service, while another may control the Download and Email Services together. These BW Controllers are referred as BWCs (internal BW Controllers or iBWC) and their corresponding parameters are referred as CIR and PIR. PIR defines the upper limit for the associated Services. CIR defines a certain minimal rate for these Services. The system should ensure that this minimum is granted under certain conditions that will be described later.

Figure 5-18: Bandwidth Control on Two Levels



The primary BW Controller (tBWC) controls the entire bandwidth of the subscriber. BW Controller (iBWC) controls the bandwidth of some portion of this bandwidth that is associated with one or more Services.

BW Controllers (iBWC) are linked to traffic in the following way:

- In the Package general definitions , define a BW Controller, with its PIR, CIR, AL and CoS.
- When defining a Service Rule, assign each service to one BW Controller.

Defining the Global Controllers

There are 16 Global Controllers available per interface. By default, each interface (upstream/downstream) is assigned one default Global Controllers that controls 100% of the link traffic. You can add up to 15 more Global Controllers per link, and assign the desired percentage of the link traffic to each.

The global controllers settings window also lets you define a total link BW limit. This limits the traffic rate of each platform interface (upstream/downstream). This is useful when another device next to the SCE Platform on the IP stream has limited BW capacity, and you want this limitation to be enforced in a policy-aware manner (by the SCE Platform), instead of being arbitrarily enforced by the other device.

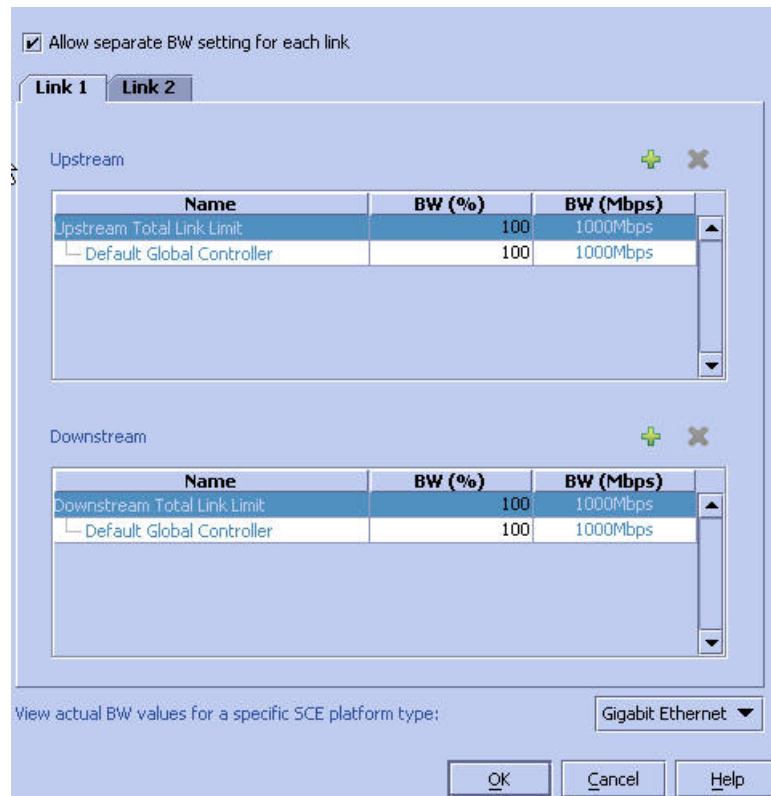
Accessing the Global Controller Settings

To access the Global Controller Settings dialog box:

-
- Step 1** From the **Configuration** menu, click **Global Controller Settings**.

The *Global Controller Settings* dialog box appears.

Figure 5-19: *Global Controller Settings*



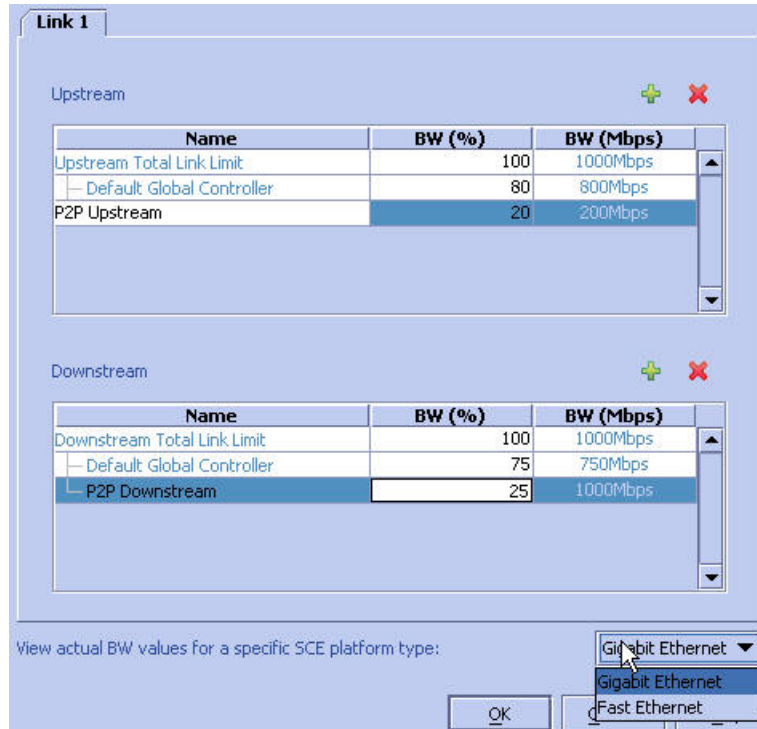
The *Global Controller Settings* dialog box has one listing for upstream Global Controllers and one for downstream. Each one has three columns:

- **Name:** A unique name assigned to the Global Controller. The system automatically assigns the names Controller1, Controller2, and so on. You may edit the name as you like.
- **BW (%):** The maximum percentage of the link traffic permitted to this Global Controller.
- **BW (Mbps):** The actual size of the band width in Mbps. This figure is calculated automatically by the system based on the SCE type (Fast Ethernet or Gigabit Ethernet), the controller bandwidth percentage and the total link BW percentage.

Step 2 To view the actual BW values in the "BW (Mbps)" column, select the type of SCE Platform:

Select the desired SCE platform type from the drop-down listing in the lower right-hand corner of the dialog box.

Figure 5-20: Global Settings: Selecting the SCE Platform



The "BW (Mbps)" column values change to reflect the choice.

Figure 5-21: Global Settings: Bandwidth Amounts for Fast Ethernet

Link 1

Upstream + ✖

Name	BW (%)	BW (Mbps)
Upstream Total Link Limit	100	100Mbps
Default Global Controller	80	80Mbps
P2P Upstream	20	20Mbps

Downstream + ✖

Name	BW (%)	BW (Mbps)
Downstream Total Link Limit	100	100Mbps
Default Global Controller	75	75Mbps
P2P Downstream	25	100Mbps

View actual BW values for a specific SCE platform type: Fast Ethernet ▼

Editing the Upstream/Downstream Total Link Limit

To edit the Upstream/Downstream Total Link Limit:

- Step 1** To access the Global Controller Settings dialog box:
Follow the procedure in the section *Accessing the Global Controller Settings* (on page 5-33).
- Step 2** Click in the **Upstream/Downstream Total Link Limit** listing field, and type in the desired bandwidth percentage.
- Step 3** Click **OK**.

Adding a Global Controller

You can add up to 15 global controllers, in addition to the default.

To add a global controller:

- Step 1** To access the Global Controller Settings dialog box:

Follow the procedure in the section *Accessing the Global Controller Settings* (on page 5-33).

Step 2 Above the listing for the desired interface (upstream/downstream), click  (**Add**).

A new global controller is added to the list with a bandwidth percentage of 100%.

To edit the name of the global controller, or the percentage of bandwidth, proceed to the next section, *Editing a Global Controller* (on page 5-37).

Removing a Global Controller

The Default Controller and the Total Link Limit cannot be removed. Note also, that if the specified global controller is being used by a subscriber BW controller, it will not be removed and an error message will appear.

To remove a global controller:

Step 1 To access the Global Controller Settings dialog box:

Follow the procedure in the section *Accessing the Global Controller Settings* (on page 5-33).

Step 2 Select the global controller to be removed.

Step 3 Click  (**Remove**).

Step 4 Click **OK**.

Editing a Global Controller

To edit a global controller:

Step 1 To access the Global Controller Settings dialog box:

Follow the procedure in the section *Accessing the Global Controller Settings* (on page 5-33).

Step 2 Click in the desired global controller listing field, and type in the desired name and/or bandwidth percentage.

Step 3 Click **OK**.

Defining Global Controllers for a Dual Link System

For a dual link system, you may define global controllers separately for each link.

To define global controllers for a dual link system:

- Step 1** Check the **Allow separate BW setting for each link** checkbox.

The dialog box now displays two tabs:

- Link 1
- Link 2

Figure 5-22: Global Controller Settings

Allow separate BW setting for each link

Link 1 **Link 2**

Upstream

Name	BW (%)	BW (Mbps)
Upstream Total Link Limit	100	1000Mbps
Default Global Controller	100	1000Mbps

Downstream

Name	BW (%)	BW (Mbps)
Downstream Total Link Limit	100	1000Mbps
Default Global Controller	100	1000Mbps

View actual BW values for a specific SCE platform type: Gigabit Ethernet

OK Cancel Help

Step 2 In the Link 1 tab, define the global controllers as explained in the previous sections.

Figure 5-23: Global Controller Settings Link 1

Allow separate BW setting for each link

Link 1 Link 2

Upstream + -

Name	BW (%)	BW (Mbps)
Upstream Total Link Limit	100	1000Mbps
Default Global Controller	60	600Mbps
P2P Upstream	15	150Mbps
Streaming Upstream	25	1000Mbps

Downstream + -

Name	BW (%)	BW (Mbps)
Downstream Total Link Limit	100	1000Mbps
Default Global Controller	60	600Mbps
P2P Downstream	15	150Mbps
Streaming Downstream	25	1000Mbps

View actual BW values for a specific SCE platform type: Gigabit Ethernet ▾

OK Cancel Help

Global controllers can only be added, renamed, or deleted in the Link 1 tab. All such changes in the Link 1 tab are automatically copied to the Link 2 tab.

Step 3 Define the bandwidth percentages (BW %) for the controllers for link 1.

Bandwidth percentages are not copied to the Link 2 tab.

Figure 5-24: Global Controller Settings Link 2

Allow separate BW setting for each link

Link 1 Link 2

Upstream + X

Name	BW (%)	BW (Mbps)
Upstream Total Link Limit	100	1000Mbps
Default Global Controller	80	800Mbps
P2P Upstream	20	200Mbps
Streaming Upstream	100	1000Mbps

Downstream + X

Name	BW (%)	BW (Mbps)
Downstream Total Link Limit	100	1000Mbps
Default Global Controller	75	750Mbps
P2P Downstream	25	250Mbps
Streaming Downstream	100	1000Mbps

View actual BW values for a specific SCE platform type: Gigabit Ethernet ▼

OK Cancel Help

Step 4 In the Link 2 tab, define the bandwidth percentages (BW %) for the controllers for link 2.

Packages

The package is the identification of the subscriber policy. It determines how each network transaction is controlled.

SCAS BB Service Configuration contains "Default Package", which is the root package and cannot be removed. The default package rule is as follows:

- Enable reporting/control (depending on license).
- Admit (do not block) traffic.
- Map traffic to the default BW controller.
- Unlimited quota bucket (volume) for both upstream and downstream traffic.

A subscriber will be mapped to the default package if no other package was specifically assigned, or if a non-existing package was assigned.

In **SCAS BB** View and **SCAS BB** Capacity Control, the default package is the only available package.

Constructing Packages

Packages are collections of Rules that define the system reaction when it encounters flows that are mapped to the Service to which the Rule is related. It is recommended that you first construct Services and only then construct Packages

Each Package contains the following information:

- **Package name:** Appears in the *Package Settings Dialog Box - General Tab*. A unique name of your choice.
- **Description:** Appears in the *Package Settings Dialog Box - General Tab*. It is recommended that you use this box to record information that is meaningful and useful.
- **Quota Management:** Appears in the *Package Settings Dialog Box - Quota Management Tab*. Specifies whether subscriber quotas are managed by an external quota manager or periodically replenished by the Service Control Application Suite for Broadband, and defines the aggregation period, when applicable.
- **Quota Buckets:** Appears in the *Package Settings Dialog Box - Quota Management Tab*. Defines up to 16 quota buckets associated with the package.
- **Subscriber Bandwidth Controller:** Appears in the *Package Settings Dialog Box - Bandwidth Controller Tab*. Used to limit subscriber BW consumption and to prioritize between subscribers at times of network congestion. Also used for linking between services and global controllers.
- **Package Index:** Appears in the *Package Settings Dialog Box - Advanced Tab*. An identification number for a particular Package. There can be a maximum of 64 Packages in the system. The SCE Platform recognizes Packages by their index number, therefore, you can change the Package name without impacting on the network's activity. The system automatically supplies a Package Index and it is recommended that you do not modify it.
- **Hierarchy:** Appears in the *Package Settings Dialog Box - Advanced Tab*. Specifies the parent package.
- **Package Usage Counters:** Appears in the *Package Settings Dialog Box - Advanced Tab*. Specifies whether an exclusive usage counter is defined for this package.
- **Calendar:** Appears in the *Package Settings Dialog Box - Advanced Tab*. Specifies the calendar that is used as the basis for time-based rules associated with this package.

Activating the Network Traffic Band

The Network Traffic/Services band is located on the left hand side of the SCAS BB Console. In order to add, edit, or remove Packages the Network Traffic tab must be active.

To activate the Network Traffic tab:

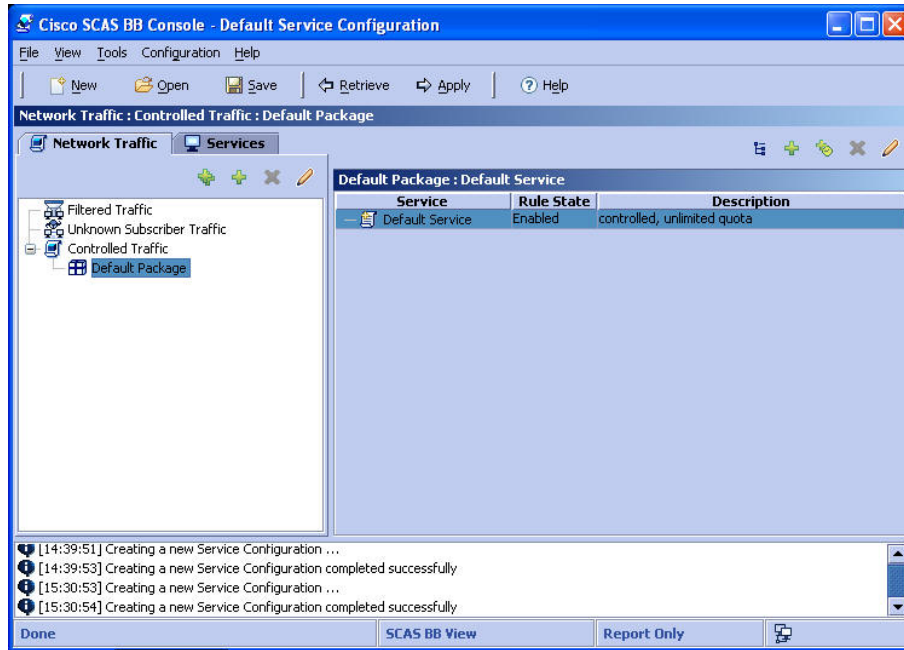
Step 1 From the **Configuration** menu, click **Network Traffic**

or

In the Network Traffic/Services band, click the **Network Traffic** tab and select the *Controlled Traffic* category.

The *SCAS BB Console - Network Traffic Tab* appears. The Network Traffic tab is now the active tab. Use the features associated with the Network Traffic tab to add new Packages, edit existing ones, and remove Packages.

Figure 5-25: SCAS BB Console - Network Traffic Tab




Adding a New Package

Adding a new Package is permitted only to *SCAS BB* Tiered Control users.

When generating a new Package, the Default Service rule is assigned by default. See *Packages* (on page 5-40).

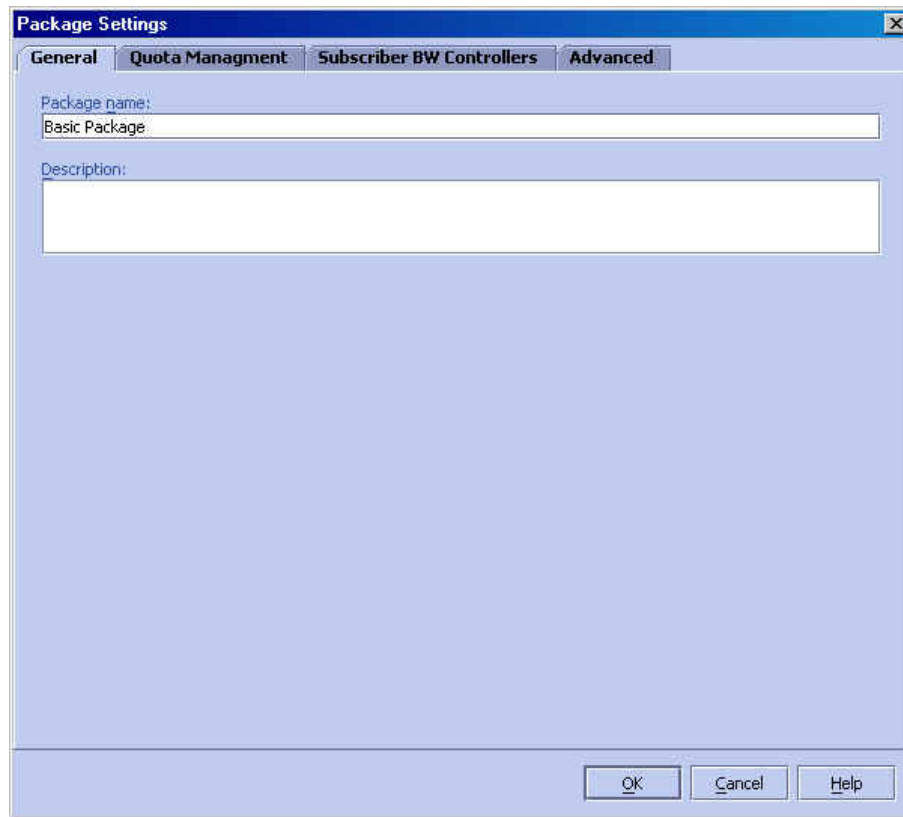
Using the General Tab (Packages)

To add a new Package:

- Step 1** To activate the Network Traffic Band:
Follow the procedure in the section *Activating the Network Traffic Band* (on page 5-41).
- Step 2** In the Packages hierarchy, select the package that you want to be the parent of the new package and click  (**Add**).

The *Packages Settings* dialog box appears.

Figure 5-26: Package Settings: General Tab



Step 3 Click the **General** tab.

Step 4 In the *Package Name* text box, type a unique and relevant Package name.

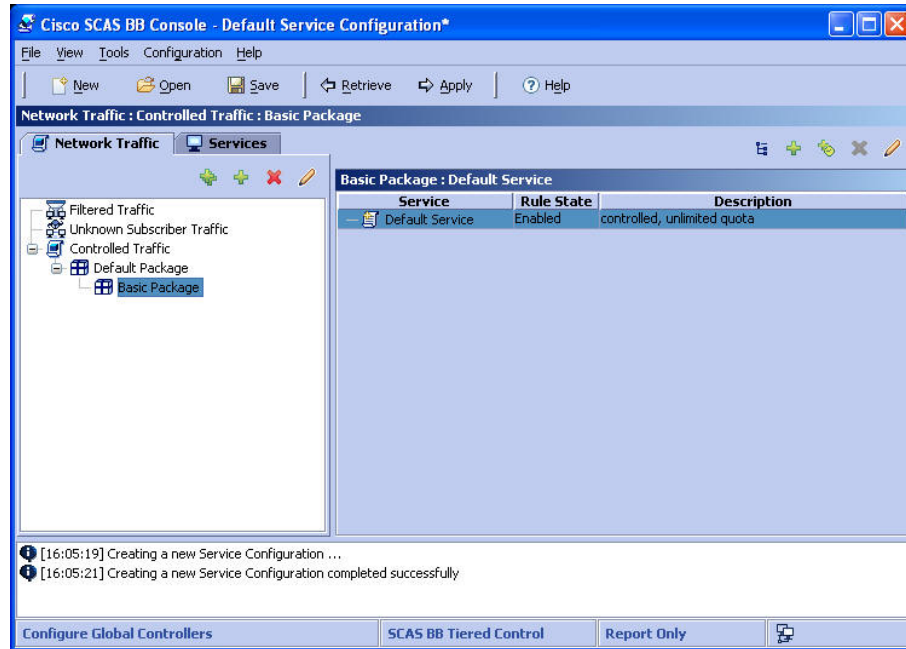
Step 5 (Recommended) In the *Description* text box, type a meaningful and useful description of the Package.

If you want define the quota management mode and quota buckets, skip to the instructions in the section *Using the Quota Management Tab (Packages)* (on page 5-44).

Step 6 Click **OK**.

The new Package is added as a child to the package selected in the Package hierarchy, and the Default Service rule appears, as shown in the figure below.

Figure 5-27: Network Traffic Band: New Package



To edit the default Rule and to add new Rules for Services that can be assigned to the Packages you created, see *Constructing and Modifying Services* (on page 5-6).

Using the Quota Management Tab (Packages)

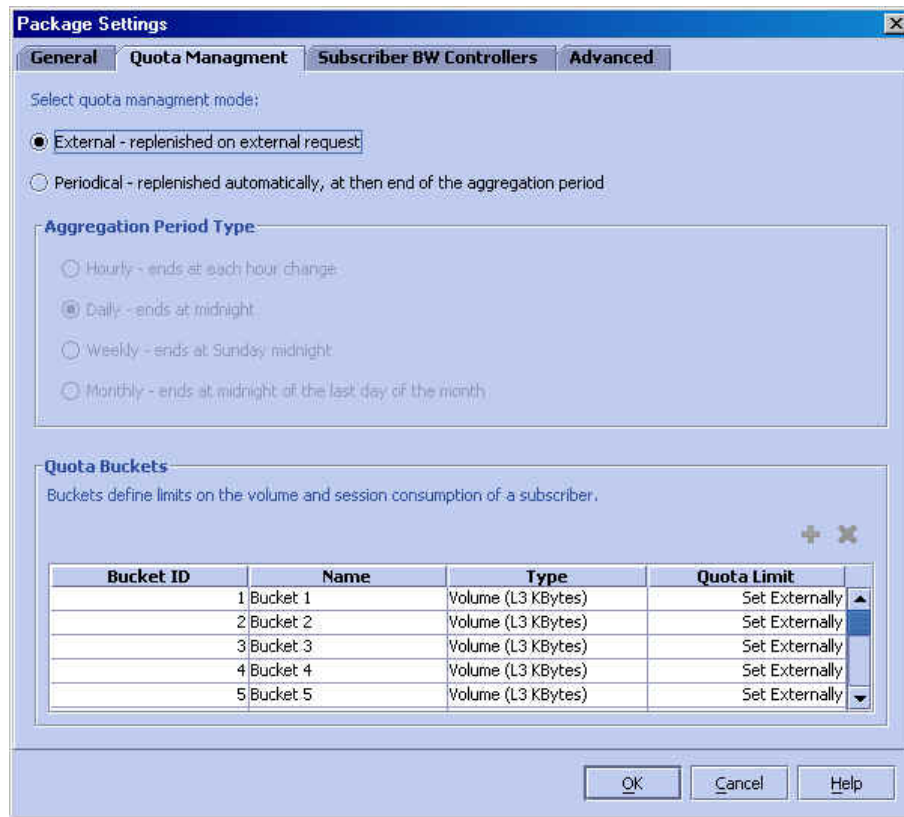
Use this tab to define whether the quota management will be performed by an external quota manager, or by the *SCAS BB* application according to the service configuration. Also use this tab to define the quota buckets associated with the package.

To select the quota management mode:

- Step 1** In the *Package Settings* dialog box, click the *Quota Management* tab.

The following dialog box appears.

Figure 5-28: Package Settings Dialog Box: Quota Management Tab



- Step 2** Select the quota management mode:
- *External*: Replenished on external request
 - *Periodical*: Replenished automatically
- Step 3** If "periodical" quota management is selected, you must select one of the four Aggregation Period Type options that specifies when the aggregation period is renewed for the Package:
- *Hourly Resolution*: Ends at each hour change
 - *Daily Resolution*: Ends at midnight
 - *Weekly Resolution*: Ends at Saturday midnight
 - *Monthly Resolution*: Ends at midnight of the last day of the month
- Step 4** Configure the quota buckets. Make sure that the configuration of the quota buckets is appropriate to the service rules applicable to the package. For example, if you do not configure a bucket with Type = number of sessions, you cannot define a rule with usage limits defined in number of sessions.
- To add a quota bucket: click *(Add)*. There is a maximum of 16 buckets per package.
 - To delete a quota bucket: select the bucket and click *(Delete)*
 - To edit a bucket: Click in the desired field to change the field:

- *Bucket ID* (cannot be edited)
- *Bucket Name*: assigning a meaningful name, such as "P2P bucket" or "Gold subscribers" is useful.
- *Type*: click in the field and select either Volume (in Kbytes) or Number of sessions
- *Quota Limit*: Define the actual limit for this bucket in Kbytes of number of sessions, depending on the selected *Type*.

To configure the subscriber bandwidth controller, see *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46).

Step 5 Click *OK*.

The new Package is added as a child to the package selected in the Package hierarchy, and the Default Service rule appears.

To change the default Rule and to add new Rules for Services that can be assigned to the Packages you created, see *Constructing and Modifying Services* (on page 5-6).

Using the Subscriber BW Controller Tab (Packages)

A *Subscriber BW Controller* (BWC) is a mechanism that supports the control of subscriber bandwidth consumption for the upstream and downstream bandwidth of flows. The BW Controller enables metering bandwidths of an aggregation of traffic flows of a Service or a group of Services.

Each Package has its own set of BW Controller parameters, thus determining the bandwidth of the Services for each subscriber who is associated with this Package.

The *Primary BW Controller* is at the subscriber level. It enables you to allocate bandwidth to specific subscribers, depending upon the CIR, PIR and the Subscriber relative priority settings.

The *BW Controller* is at the Services level. It allows you to define the allocation of bandwidth to each subscriber's Service, based upon the CIR, PIR, Global Controller and Assurance Level (AL) for the Service. Each Service Rule may include linking of the Service's flows to one of the BW Controllers.

Services that are not mapped to a specific BW Controller are automatically mapped to the *Default BW Controller*. This enables the BW Controllers mechanism to control rate sub-partitioning within the Default BW Controller rate control, based on the CIR, PIR, CoS and AL.

The *Extra BW Controller* is a unique capability that is also at the subscriber level. Extra BW Controllers are allocated for services that are not included in the Primary BW Controller. Extra BW Controllers are defined (based on CIR, PIR, Global Controller, and AL), in addition to the Primary BW Controller. These Services are not often used and they often have strict bandwidth requirements, for example, a video conference call. The Extra BW Controllers are bandwidth controllers that control a single service (service group). BW Controllers cannot borrow bandwidth from Extra BW Controllers and vice versa.

The following are the Configuration parameters, as seen in the figure below:

- **Name**: Use to designate a significant name.

- **CIR:** Committed Information Rate. Defines the minimal bandwidth that must be granted to traffic that is controlled by the BW Controller.
- **PIR:** Peak Information Rate. Defines the maximal bandwidth allowed to that traffic.
- **Global Controller:** This selects the global controller with which this subscriber BW controller is associated. The global controllers are virtual queues that are part of the bandwidth control mechanism (see *Global Control* (on page 5-30)). Traffic with similar bandwidth control properties should be directed to the same Global Controller.
- **AL:** Assurance Level. Controls how fast BW would decrease from PIR to CIR as congestion builds, or increase from CIR to PIR as congestion decreases. A higher AL ensures a higher BW compared to a similar BWC with a lower AL. 1 is the lowest assurance value, 10 (persistent) is the highest assurance value.

Assurance Level "persistent" has the added quality that it does not ever reduce below the relevant CIR, unless the total line rate cannot sustain this.

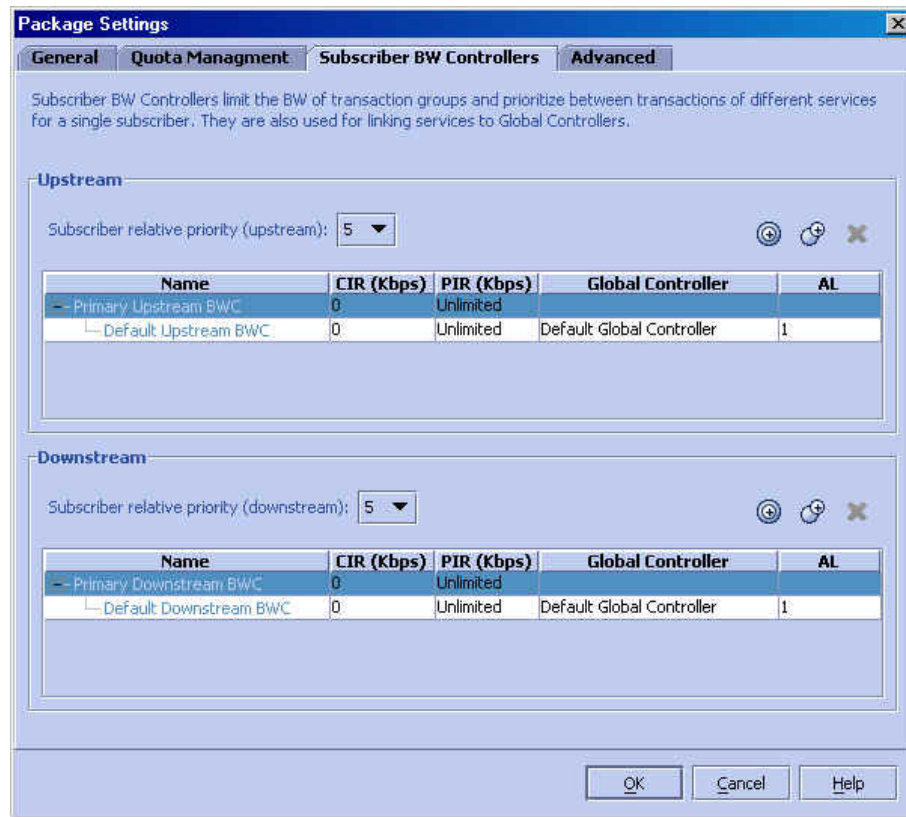
Subscriber relative priority: Assurance Level given to the Total BW Controller of the subscriber. It determines the assurance given to all the subscriber traffic when competing for bandwidth with other subscribers. 1 is the lowest value and 10 is the highest value.



To set the Package bandwidth controller parameters:

Step 1 In the *Package Settings* dialog box, click the **Subscriber BW Controllers** tab.

The following dialog box appears.

Figure 5-29: Package Settings: Subscriber BW Controller Tab



- Step 2** Change the values in the **Bandwidth Controllers Upstream** table and **Bandwidth Controllers Downstream** table, according to the system requirements.
- Step 3** Click  to add a BW Controller to the Service. This can be done for Upstream and Downstream.
- Step 4** Click  to add an Extra BW Controller, that comes in addition to the Primary BW Controller. This can be done for Upstream and Downstream.
- Step 5** (Recommended) Modify the names of the BW Controllers, to fit their logical application within the Service Configuration. This can help ease the process of BW Controller assignment when defining Service Rules.
- Step 6** In the *CIR* text box, type a number to set the BW Controller CIR in Kbps.
- Step 7** In the *PIR* combo box, select "unlimited" from the drop-down list, or type a number to set the BW Controller PIR in Kbps.
- Step 8** Select an option from the *Global Controller* drop-down list.
- Step 9** Select a listed number from the *AL* drop-down list.
1 is the lowest value and 10 (persistent) is the highest value.

Step 10 Select a listed number from the *Subscriber relative priority* drop-down list.

1 is the lowest value and 10 is the highest value.

If you want to specify an index for the package, define an exclusive usage counter, or define a calendar, skip to the instructions in the section *Using the Advanced Tab (Packages)* (on page 5-49).

Step 11 Click **OK**.



Note When you click **OK** the following message may appear:



Follow the instructions in this section to correct the problem.



Note When you click **OK** the following message may appear:



Follow the instructions in this section to correct the problem.

The new Package is added as a child to the package selected in the Package hierarchy, and the Default Service rule appears.

To change the default Rule and to add new Rules for Services that can be assigned to the Packages you created, see *Constructing and Modifying Services* (on page 5-6).

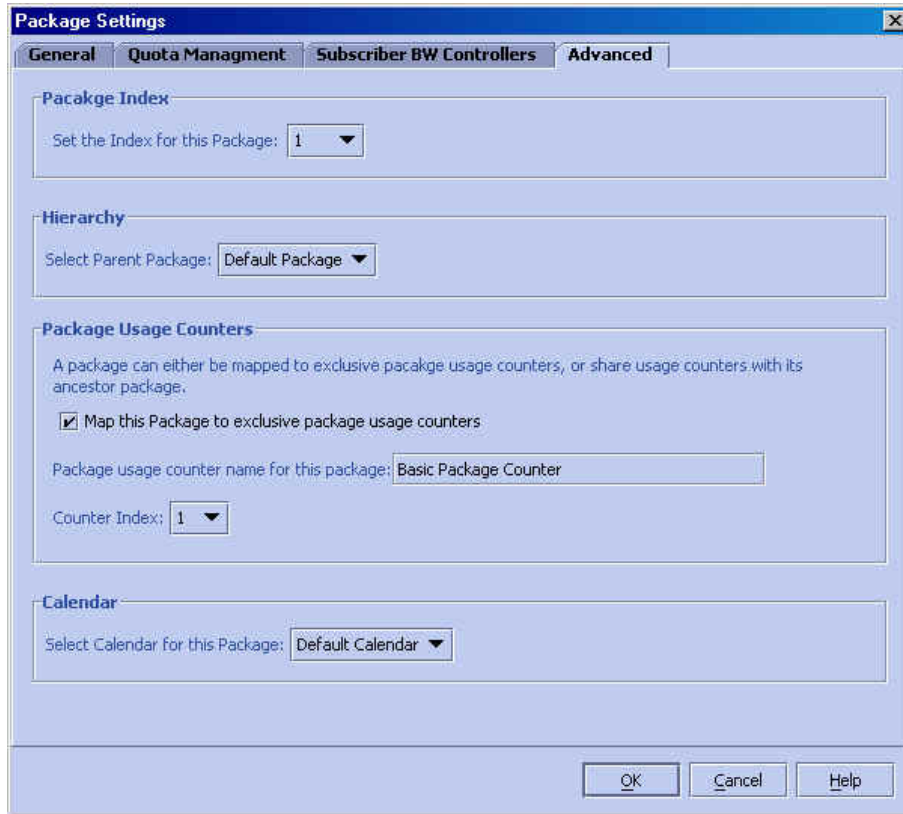
Using the Advanced Tab (Packages)

To set the Package advanced options:

Step 1 In the *Package Settings* dialog box, click the **Advanced** tab.

The following dialog box appears.

Figure 5-30: Package Settings: Advanced Tab



Step 2 From the *Set the Index for this Package* drop-down list, select a Package Index.

The maximum available value is 4998 (4999 is reserved for Unknown Subscriber Traffic). The system automatically assigns a free number to a newly created Package. Modify this number only in cases where a specific index value must be assigned to a Package.

Step 3 To define a parent package, select the desired parent from the *Select Parent Package* drop-down list.

Step 4 To define the package usage counter:

- To share a usage counter with the parent package: Uncheck the "**Map this Service to an exclusive package usage counters**" checkbox.

The counter name of the parent package appears in the usage counter name field.

- To define an exclusive usage counter: Check the "**Map this Service to an exclusive package usage counter**" checkbox.

The name of this package appears in the usage counter name field.

If desired, select a counter index from the *Counter Index* drop-down list.

Step 5 To define a Calendar that will determine the available time frames for time based rules, select the desired calendar from the *Select Calendar for this Package* drop-down list.

Step 6 Click **OK**.

The new Package is added as a child to the selected package, and the Default Service rule appears.

To change the default Rule and to add new Rules for Services that can be assigned to the Packages you created, see *Constructing and Modifying Services* (on page 5-6).

Duplicating a Package


You can duplicate an existing package. This is a useful way to create a package that is similar to an existing package. It is faster to duplicate a similar package and then make changes than to create the package from scratch.

A duplicated package is added at the same level in the Package hierarchy as the original package.

To duplicate a package:

Step 1 To activate the Network Traffic Band:

Follow the procedure in the section *Activating the Network Traffic Band* (on page 5-41).

Step 2 In the *Controlled Traffic* category, select the name of the Package that you want to duplicate.**Step 3** In Network Traffic band, click  (**Duplicate**).

A duplicate package is created with all the same attributes as the original package. The name of the new package is the name of the selected package followed by "(1)" (or(2), and so on if a package is duplicated more than once). For example "Mail & Web Boost (1)".

Editing Package Parameters

To edit a Package parameter:

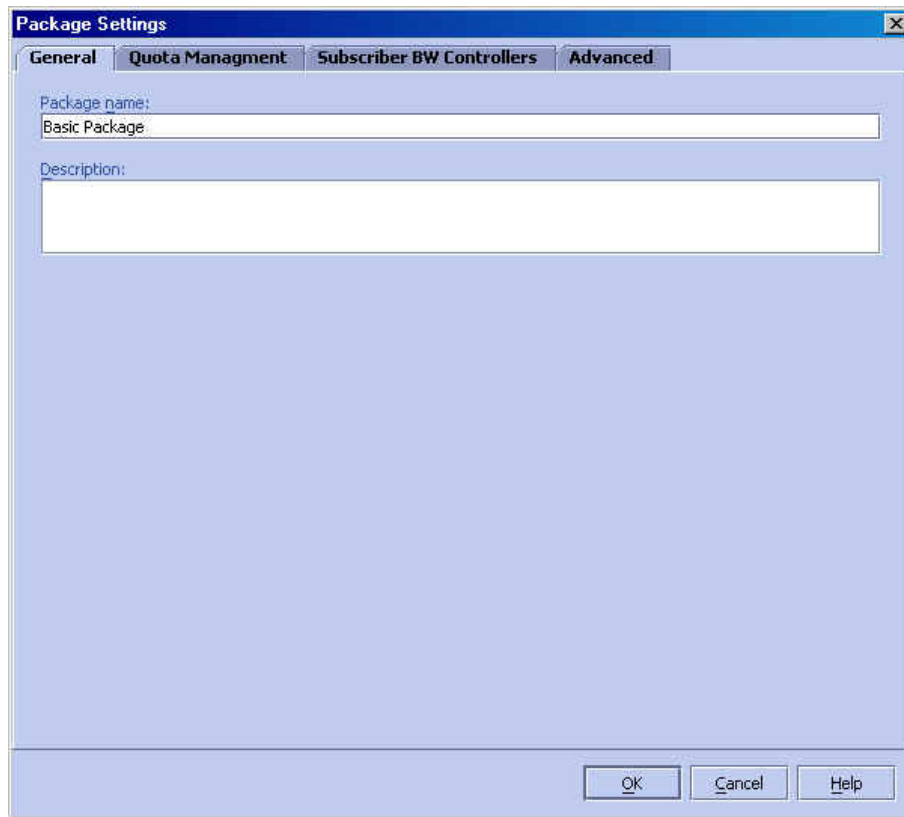
Step 1 To activate the Network Traffic Band:

Follow the procedure in the section *Activating the Network Traffic Band* (on page 5-41).

Step 2 In the Package hierarchy, select the name of the Package that you want to edit.**Step 3** In Network Traffic band, click  (**Edit**).

The *Package Settings* dialog box appears.

Figure 5-31: Package Settings: General Tab



Step 4 Click the tab that contains the parameters to be edited.

Use the reference list in the table below.

Step 5 Click **OK** to save the changes.

Table 5-3 Package Management Reference List


Tab Name	Instructions
General	See <i>Using the General Tab (Packages)</i> (on page 5-42).
Aggregation Period	See <i>Using the Quota Management Tab (Packages)</i> (on page 5-44).
Quota Buckets	See <i>Using the Quota Management Tab (Packages)</i> (on page 5-44).
Bandwidth Controllers	See <i>Using the Subscriber BW Controller Tab (Packages)</i> (on page 5-46).
Package Index	See <i>Using the Advanced Tab (Packages)</i> (on page 5-49).
Parent Package	See <i>Using the Advanced Tab (Packages)</i> (on page 5-49).
Exclusive Usage Counters	See <i>Using the Advanced Tab (Packages)</i> (on page 5-49).

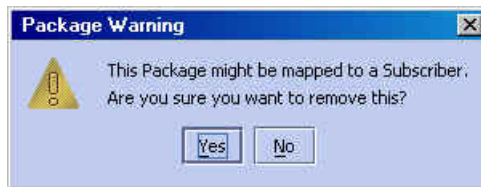
Tab Name	Instructions
Calendar	See <i>Using the Advanced Tab (Packages)</i> (on page 5-49).

Removing a Package

You can remove a user-defined package. The default package cannot be removed.

To remove a Package:

-
- Step 1** To activate the Network Traffic Band:
Follow the procedure in the section *Activating the Network Traffic Band* (on page 5-41).
- Step 2** In the Package hierarchy, select the name of the Package that you want to remove.
- Step 3** From the Network Traffic band, click  (**Remove**).
A *Package Warning - Remove Package* message appears.



- Step 4** Click **Yes**.
The Package is removed from the Network Traffic band and is no longer available.
-

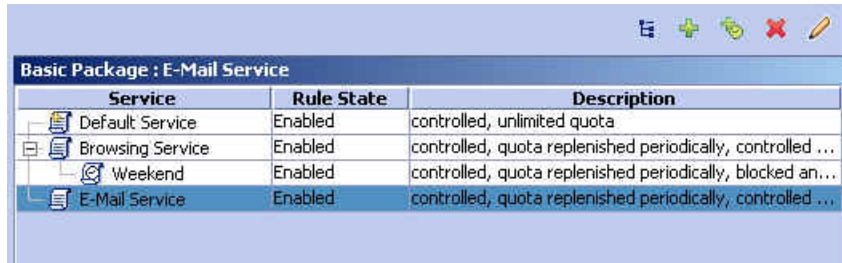
Assigning Services to Packages

Now that you have set up both Services and basic Packages, it is time to assign Services to Packages. A Service is assigned to a Package by defining a Service Rule for the Package. There are two types of rules:

- **Service Rule**
- **Time Based Rule:** This is a Rule that is attached to a Service Rule. The settings of the time-based rule take effect only during the specified time-frame, as defined in the Calendar defined for the package. It will be listed as a sub-rule in the Service Rule table.

An example of the two types of rules is shown below.

Figure 5-32: Two Types of Traffic Rules



Service	Rule State	Description
Default Service	Enabled	controlled, unlimited quota
Browsing Service	Enabled	controlled, quota replenished periodically, controlled ...
Weekend	Enabled	controlled, quota replenished periodically, blocked an ...
E-Mail Service	Enabled	controlled, quota replenished periodically, controlled ...

Traffic Rules

As you saw in *SCAS BB Console - New Package* (on page [Error! Bookmark not defined.](#)), a *Default Service Rule* is assigned by default to every Package.

The default values of this rule are:

- Enable reporting/control (depending on license).
- Admit (do not block) traffic.
- Map traffic to the default BW controller.
- Unlimited quota bucket (volume) for both upstream and downstream traffic.

Adding a New Rule to a Package

You can add additional Rules to a Package based on your requirements. Time Based Rules are described in the section *Adding a Time Based Rule* (on page [5-63](#)).

To add a new Service Rule:

Step 1 To activate the Network Traffic Band:

Follow the procedure in the section *Activating the Network Traffic Band* (on page [5-41](#)).

Step 2 In the Package hierarchy, select the desired Package.

Step 3 In the Main Window, click  (**Add**).

The *Add New Rule to Package* dialog box appears. This dialog box has the following tabs: **General**, **Control**, **Usage Limits**, and **Breach Handling**.

Figure 5-33: Add New Rule to Package: General Tab



The **General** tab has two sections:

- **Service:** Use to select the Service to which this Rule is applied. This field is not available under the Total Traffic Rule *General* tab because it is a global Rule that applies to all the Package's Services.
- **Rule State:** Supplies the state of this Rule: Enable reporting and active actions, Disable reporting and active action, or Report only - disable active actions. The Enable option is available only in *SCAS BB* Capacity Control.

To select the Service and Rule State:

- Step 1** Click the **General** tab.
- Step 2** In the **Service** section, select a Service from the *Select the Service to which the Rule will relate to* list.
- Step 3** In the **Rule State** section, select one of the options buttons in order to **Define the state for this Rule**.

The possible options are:

- **Enable reporting and active actions** (disabled under *SCAS BB* View mode)

- **Disable reporting and active actions**
- **Report only – disable active actions**

If you want to enter more information, skip to the instructions in the section *The Control Tab (Service Rule)* (on page 5-56).

Step 4 Click **OK**.

A new Service Rule is generated.

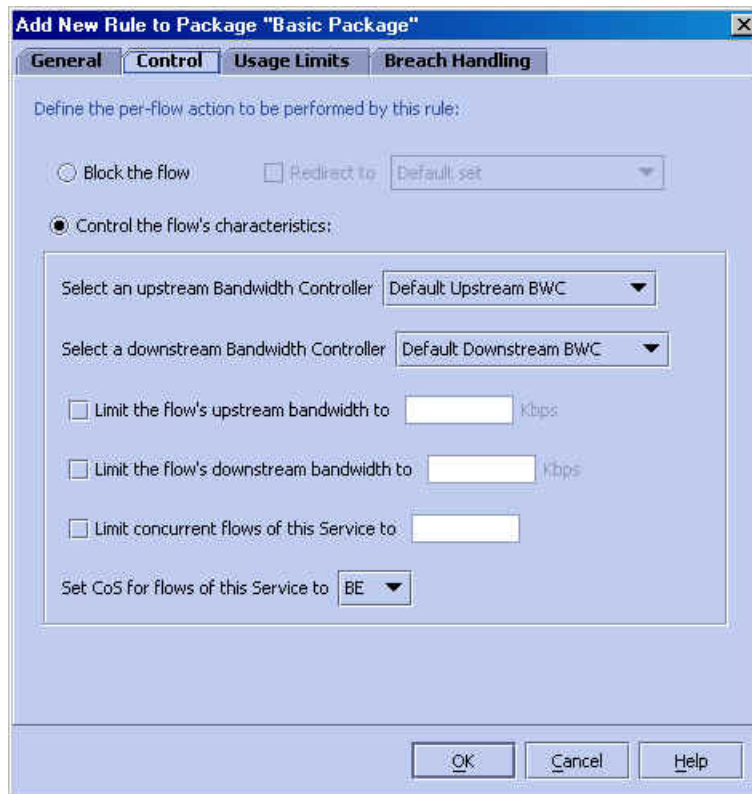
The Control Tab (Service Rule)

The **Control** tab of the *Add New Rule to Package* series gives you the ability to decide on the per traffic flow behavior of sessions that belong to the current Service.

The **Control** tab is disabled for *SCAS BB* View users.

When you select the **Control** tab, the following dialog box appears.

Figure 5-34: Add New Rule to Package: Control Tab



This screen supports traffic control and therefore is only available when running *SCAS BB* Capacity Control or *SCAS BB* Tiered Control.

The screen has two main sections. In the upper section you can determine what happens to the flow identified as belonging to this specific service:

- **Block the flow**
- **Redirect to (a redirection set):** When this option is active you should select the URL group to serve as the redirection target. URL groups are defined under **Configuration>System Settings>Redirection URLs Tab** (see the section *Configuring the Redirection Parameters* (on page 6-4)). This option is enabled only when the *Block the flow* option is selected. Only three protocol types support redirection: HTTP, HTTP Streaming and RTSP.
- **Control the flow characteristics:** When this option is active, the options in the second half of the screen are available.
 - **Select an upstream Bandwidth Controller [name]:** The BW Controller names in this list were set when you defined the BW Controller parameters during Package set up (see the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)). Use this option to map this Service's traffic flows to a specific upstream BW Controller. This sets up bandwidth metering of all the flows of this Service based on the characteristics of the selected BW Controller.

While the mouse is hovering over the combo-box with the selected BW controller, a tool tip appears describing the BW controller properties (CIR, PIR, Global Controller, AL).

Figure 5-35: Add New Rule to Package: Control Tab (BW Controllers)

The screenshot shows the 'Control' tab of a configuration window. The 'Control the flow's characteristics' radio button is selected. Below it, there are two dropdown menus for 'Select an upstream Bandwidth Controller' (set to 'Default Upstream BWC') and 'Select a downstream Bandwidth Controller' (set to 'Default Downstream BWC'). A tooltip for 'Default Downstream BWC' is displayed, showing the following properties: PIR = Unlimited, CIR = 0 Kbps, Global Controller = Default Global Controller, and Assurance Level = 1. There are also checkboxes for limiting upstream/downstream bandwidth and concurrent flows, and a dropdown for 'Set CoS for flows of this Service to' (set to 'BE'). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

- **Select a downstream Bandwidth Controller [name]:** The BW Controller names in this list were set when you defined the BW Controller parameters during Package set up (see the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)). Use this option to map this service traffic flows to a specific downstream BW Controller. This sets up bandwidth metering of all the flows of this Service based on the characteristics of the selected BW Controller.
- **Limit the flow's upstream bandwidth to [number] Kbps:** Use to set an upstream bandwidth limit to a single specific flow of the Service that this rule applies to.
- **Limit the flow's downstream bandwidth to [number] Kbps:** Use to set a downstream bandwidth limit to a single specific flow of the Service that this Rule applies to.

Limit concurrent flows of this Service to [number]: Use this option to limit the number of concurrent transactions (simultaneously performed by the subscriber) associated to the Service that the Rule applies to.

To define the traffic flow behavior of the Rule:

Step 1 Click the **Control** tab.

Step 2 Select the desired option(s): (a) **Block the flow** (b) **Redirect to [name]** (enabled only when Block the flow is selected) or (c) **Control the flow's characteristics**.

If the **Redirect to [name]** option is active, from the redirection list, select a Redirection set.



Note If the Service supports both protocols that can be redirected and protocols that cannot be redirected, the following message appears.



Click **OK** to continue.



Note If the Service supports only protocols that cannot be redirected, the following message appears.



Click **OK** to continue.

If the **Control the flow's characteristics** option is active, select the following options.

- Step 3** (Optional) Select the **Select an upstream Bandwidth Controller** check box. From the BW Controller drop-down list, select a BW Controller (the actual names that appear in this list were set in the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)).
- Step 4** (Optional) Select the **Select a downstream Bandwidth Controller** check box. From the BW Controller drop-down list, select a BW Controller (the actual names that appear in this list were set in the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)).
- Step 5** (Optional) Select the **Limit the flow's upstream bandwidth to** check box and type a value in the *Kbps* box.
- Step 6** (Optional) Select the **Limit the flow's downstream bandwidth to** check box and type a value in the *Kbps* box.
- Step 7** (Optional) Select the **Limit concurrent flows of this Service to** check box and type a value in the associated box.

If you want define the usage limits, skip to the instructions in the section *The Usage Limits Tab (Service Rule)* (on page 5-60).

- Step 8** Click **OK**.

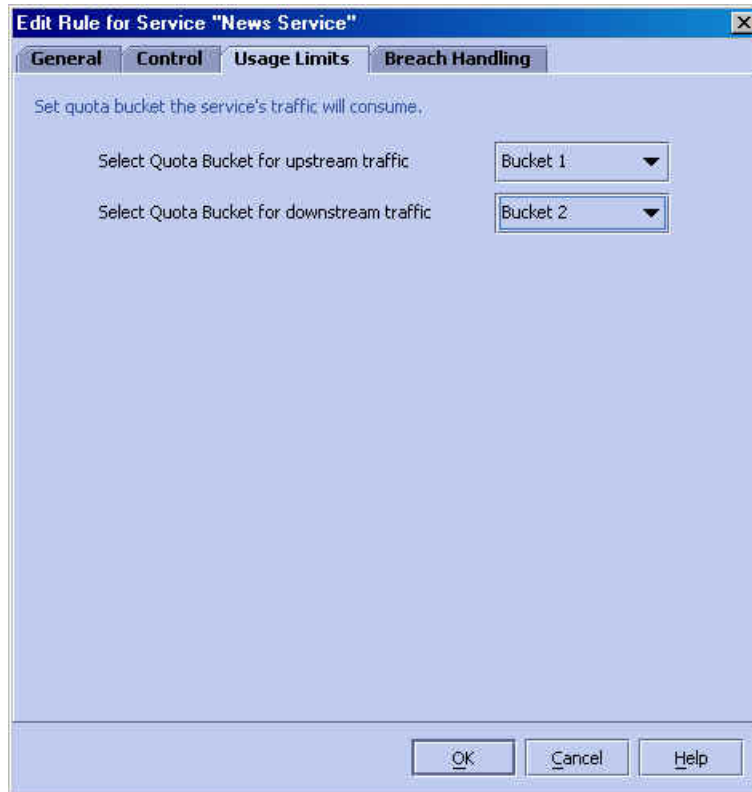
A new Service Rule is generated.

The Usage Limits Tab (Service Rule)

The *Usage Limits* tab is used to define the quota buckets to be used by this service. The quota buckets that will be available in the drop-down list are the ones that were defined for the selected package. If no quota bucket is appropriate for the service rule, you must add a new quota bucket to the package, or edit an existing bucket.

When you select the **Usage Limits** tab, the following dialog box appears.

Figure 5-36: Service Rule: Quota Limits External



To define quota buckets:

-
- Step 1** Click the **Usage Limits** tab.
- Step 2** Select the desired bucket(s) from the appropriate drop-down list(s):
- **Select Quota bucket for upstream traffic**
 - **Select Quota bucket for downstream traffic**
 - **Select Quota bucket for sessions**

You may select any bucket or no bucket for unlimited quota.

- Step 3** Click **OK**.

A new Service Rule is generated.

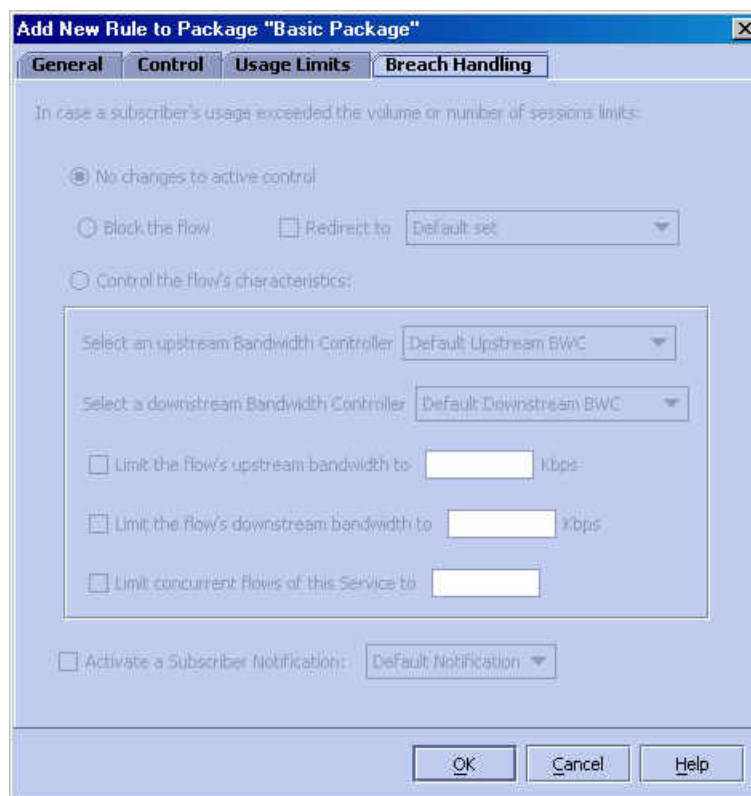
The Breach Handling Tab (Service Rule)

The options in this screen are disabled for *SCAS BB View* users.

Use this feature to change the SCE Platform behavior when the Aggregated volume limit, the Total number-of-sessions limit, or the externally imposed quota is exceeded.

- When one of the options in the *Usage Limit Tab (Service Rule)* is selected, the *Breach Handling Tab (Service Rule)* options are enabled.
- When the **Control the flow's characteristics** option is selected, the check boxes are enabled.

Figure 5-37: Add New Rule to Package: Breach Handling Tab



The available options are:

- **No changes to active control:** Use this feature to register the exceptions (RDR generation) and at the same time not to impose the set limits.
- **Redirect to [name]:** Use this feature to send the traffic to another server. It is active only when you enable the **Block the Flow** option. The redirection set names in this list were set when you defined the redirection options in the **System Settings** dialog boxes. See *Configuring the Redirection Parameters* (on page 6-4).
- **Control the flow's characteristics:** When this option is active, the options in the second half of the screen are available.

- **Select an upstream Bandwidth Controller** [name]: The BW Controller names in this list were set when you defined the BW Controller parameters during Package set up (see the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)). Use this option to map this Service traffic flows to a specific upstream BW Controller. This sets up bandwidth metering of all the flows of this Service based on the characteristics of the selected BW Controller.
- **Select a downstream Bandwidth Controller** [name]: The BW Controller names in this list were set when you defined the BW Controller parameters during Package set up (see the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)). Use this option to map this Service traffic flows to a specific downstream BW Controller. This sets up bandwidth metering of all the flows of this Service based on the characteristics of the selected BW Controller.
- **Limit the flow's upstream bandwidth to** [number] **Kbps**: Use to set an upstream bandwidth limit to a single specific flow of the Service that this Rule applies to.
- **Limit the flow's downstream bandwidth to** [number] **Kbps**: Use to set a downstream bandwidth limit to a single specific flow of the Service that this Rule applies to.
- **Limit concurrent flows of this Service to** [number]: Use this option to limit the number of concurrent transactions (simultaneously performed by the subscriber) associated to the Service that the Rule applies to.
- **Activate a Subscriber Notification**: Use this option to select a previously defined Subscriber Notification that should be activated when the subscriber has exceeded his quota limit. This notification could, for example, convey the quota breach situation to the subscriber and provide information on how to obtain additional quota. (*Subscriber Notification* (on page 5-85)).

Subscriber Notification may be selected in addition to any of the above breach handling options.

To set the breach handling settings:

Step 1 Click the **Breach Handling** tab.

Step 2 (Optional) Select the desired option(s):

- **No changes to active control**
- **Block the flow**
- **Control the flow's characteristics**

Step 3 If you have selected **Block the flow**, you can determine which redirection set to use. Select the **Redirect to** check box and select a redirection set from the drop-down list.

Step 4 If the **Control the flow's characteristics** option is active, select the following options.

- (Optional) Select the **Select an upstream Bandwidth Controller** check box. From the BW Controller drop-down list, select a **BW Controller** (the actual names that appear in this list were set in the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)).

- (Optional) Select the **Select a downstream Bandwidth Controller** check box. From the BW Controller drop-down list, select a **BW Controller** (the actual names that appear in this list were set in the section *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)).
- (Optional) Select the **Limit the flow's upstream bandwidth to** check box and type a value in the *Kbps* box.
- (Optional) Select the **Limit the flow's downstream bandwidth to** check box and type a value in the *Kbps* box.
- (Optional) Select the **Limit concurrent flows of this Service to** check box and type a value in the associated box.

Step 5 To activate subscriber notification, select the **Activate a Subscriber Notification** check box and select the desired subscriber notification from the drop-down list.

The subscriber notification must be previously defined via the **Subscriber Notification Settings** dialog (*Subscriber Notification* (on page 5-85)).

Note that **Subscriber Notification** can be activated in addition to any of the other three breach handling options.

Step 6 Click **OK**.

A new Service Rule is generated.

Adding a Time Based Rule

Use this procedure to add a Time Based Rule to any Service Rule. Adding a Time Based Rule enables you to specify alternate Rules parameters applicable only for a specific time frame. At all other times, the original Rule will be enforced.

The following example illustrates adding a Time Based Rule to a regular Service Rule.


To add a Time Based Rule:

Step 1 To activate the Network Traffic Band:

Follow the procedure in the section *Activating the Network Traffic Band* (on page 5-41).

Step 2 In the Packages hierarchy, select a Package.

Step 3 In the Main Window, click a Service Rule.

Step 4 Click  (**Add Time Based Rule**).

The following dialog box appears.

Figure 5-38: Add Time Based Rule



The *Add Time Based Rule to Service* screen has four tabs:

- General
- Control
- Usage Limits
- Breach Handling

Step 5 In the **General** tab, from the *Select the Time Frame for this Rule* drop-down list, select one of four possible time frames.

Step 6 Click an option button in the **Rule State** section.

The possible options are:

- **Enable reporting and active actions** (disabled under *SCAS BB* View mode)
- **Disable reporting and active actions**

Then proceed as with a regular Service Rule. Refer to the following table to find the section describing the procedure for each tab.

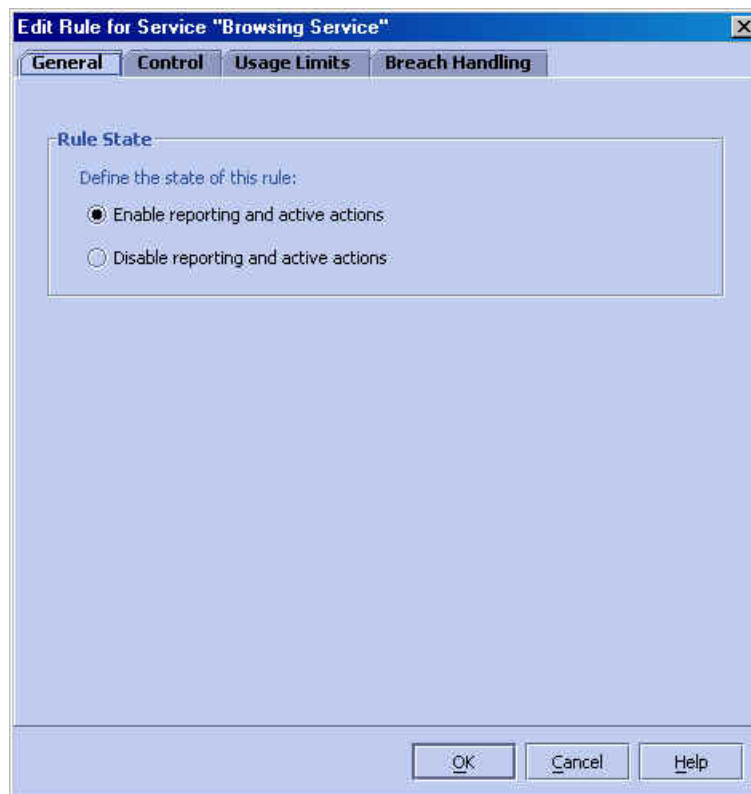
Table 5-4 Service Rule, Time Based (Procedures)

Tab	Follow Procedure
Control	<i>The Control Tab (Service Rule) (on page 5-56).</i>
Usage Limits	<i>The Usage Limits Tab (Service Rule) (on page 5-60).</i>
Breach Handling	<i>The Breach Handling Tab (Service Rule) (on page 5-61).</i>

Editing a Service Rule

To edit any rule, Service Rule, or a Time Based Rule, select the Rule and follow the relevant instructions in the sections following *Adding a New Rule to a Package* (on page 5-54). The screens are similar except for the screen title, which reflects the different status (see the figure below) and the *General* tab, which no longer has the option to choose the associated service.

Figure 5-39: Editing a Service Rule



Removing a Service Rule

Use this feature to remove Service Rules or Time Based Rules. The Default Traffic Rule cannot be removed. At times, you may prefer to temporarily remove a Rule, without losing its profile. In this case, access the *General* tab and change the Rule state to **Disable reporting and active actions**. This has the same effect as removing it, but it enables you to use the Rule again later, without having to set it up again from the beginning.

To remove a Service Rule:

Step 1 To activate the Network Traffic Band:

Follow the procedure in the section *Activating the Network Traffic Band* (on page 5-41).

Step 2 In the Packages hierarchy, select the Package.

Step 3 In the Main Window, click the Service Rule you want to remove.







Step 4 From the Main Window, click  (**Remove**).

The selected Rule will be removed.

Displaying the Services Affected by a Rule


If you have defined a service as a child of a another service, it may be affected by a rule defined for the parent service. (If you have defined a separate rule for the child service, it is not affected by the rule defined for the parent.) Any rule that affects children of the service displayed in the service rules listing is indicated by a small yellow mark on the icon, as illustrated for the Default Service and Streaming Service in the example below.

Figure 5-40: Child Services Indicator in the Service Rules Listing

Service	Rule State	Description
 Default Service	Enabled	blocked
 Browsing Service	Enabled	blocked and redirected
 E-Mail Service	Enabled	blocked
 News Service	Enabled	blocked
 Streaming Service	Enabled	blocked and redirected
 Generic IP Service	Enabled	blocked

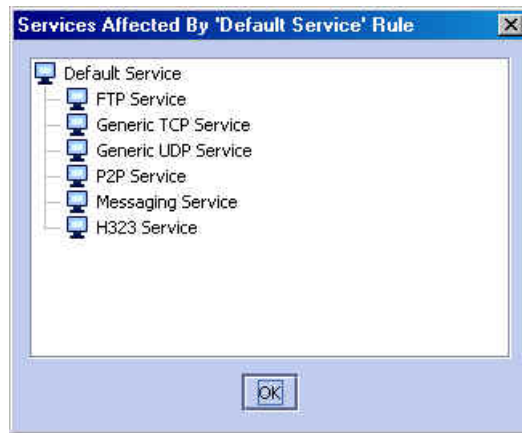
Note that the default service always affects all other services until rules are defined for those services.

To display a listing of all services affected by a specific rule:

Step 1 Select the rule in the service rule listing and click  (**Show All Services Affected By this Rule**).

The listing is displayed.

Figure 5-41: Services Affected by Rule Listing



Unknown Subscribers Traffic

If the traffic flow does not comply with any Filter Rule, and is therefore processed by the SCE Platform, the SCE device then tries to identify the subscriber responsible for the traffic flow. The SCE Platform looks at the IP address or VLAN tag of the traffic flow, and checks the internal database for a Subscriber that is identified by this IP Address or VLAN tag. If such a Subscriber is not found in the database, the traffic flow is mapped to the Unknown Subscribers Traffic category.

Therefore, *Unknown Subscribers Traffic* may be defined as traffic:

- That did not match a Filtered Traffic Rule
- and*
- For which a subscriber identified by its IP address or VLAN ID was not found in the database.

Traffic of one unknown subscriber cannot be distinguished from traffic of other unknown subscribers. This implies the following limitations when controlling traffic of unknown subscribers:

- No per-subscriber usage limits can be defined
- No subscriber-level metering with subscriber BW controllers can be defined. Subscriber BW controllers can only be used for linking a certain service to a global controller

Unknown subscriber traffic functions similarly to a package with the following parameters:

- Package Name = Unknown Subscriber Traffic
- Package Index = 4999
- Exclusive usage counter is defined named Unknown Subscriber Traffic Counter with Counter Index = 63

Following is a list of available procedures for unknown subscriber traffic:

- Editing the unknown subscriber traffic "package":
 - Subscriber bandwidth controllers tab (see *Using the Subscriber BW Controller Tab (Packages)* (on page 5-46)).
 - Calendar (see *Using the Advanced Tab (Packages)* (on page 5-49)).
- Adding service rules to unknown subscriber traffic (see *Adding a New Rule to a Package* (on page 5-54))
- Editing service rules:
 - Rule State (General tab, see *Adding a New Rule to a Package* (on page 5-54))
 - Control tab (see *The Control Tab (Service Rule)* (on page 5-56))

Weekly Time-Frames

The SCAS BB Console allows you to supply time-dependent differentiated services. Use this capability to divide the period of a week into four separate time frames, for example:

- Peak
- Off Peak
- Night
- Weekend

In addition, you can define up to ten calendars, each with a different time frame configuration.

A week is seven full days, twenty-four hours a day (24/7), and is divided into time-frames by assigning each of the 24x7 hours to a time-frame. Use these time blocks to impose further constraints on any service.

Managing Calendars

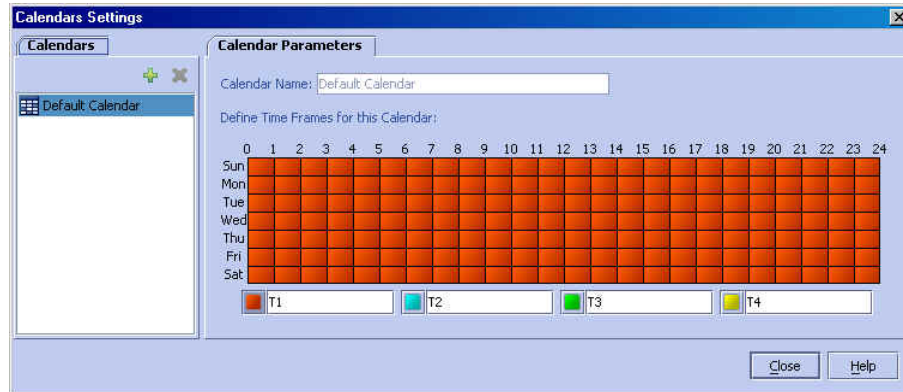
By default, *SCAS BB* includes one default calendar, but you can add up to nine more. You must create a calendar before you can define the related time frames.

To create a calendar:

-
- Step 1** From the **Configuration** menu, click **Weekly Time Frames**.

The following dialog box appears.

Figure 5-42: Calendar Settings Dialog Box



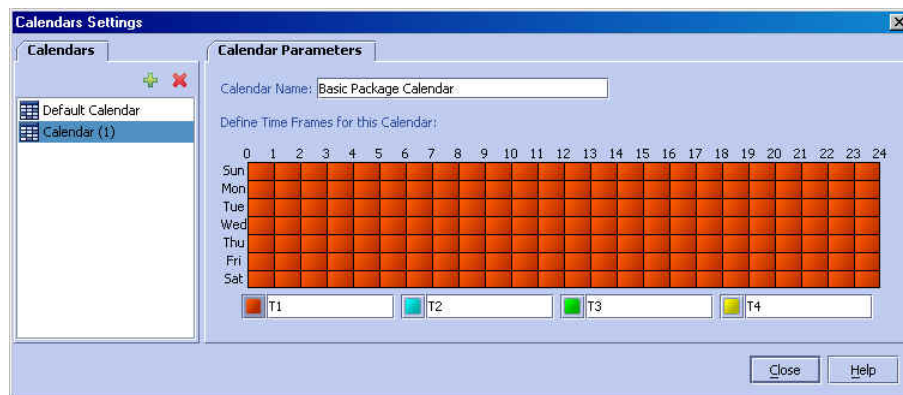
The tab on the left (**Calendar**) is used for adding and deleting calendars, while the tab on the right (**Calendar Parameters**) is used to define the time frames.

Step 2 From the **Calendar** tab, click  (**Add**).

A new calendar is added with the name Calendar(1).


Step 3 In the **Calendar Parameters** tab, click in the Calendar Name field to change the name to a meaningful name.

Figure 5-43: Adding a New Calendar



To delete a calendar:

Step 1 From the **Configuration** menu, click **Weekly Time Frames**.

Step 2 From the **Calendar** tab, select the desired calendar and click  (**Delete**).

Note that although the time frames may be configured differently in all ten calendars, the names of the Time Frames are the same in all calendars. By default the time frames are named T1, T2, T3, and T4. You can change these names at any time, but be aware that if you change the name when configuring one calendar, the names are also changed for all other calendars, existing and future.

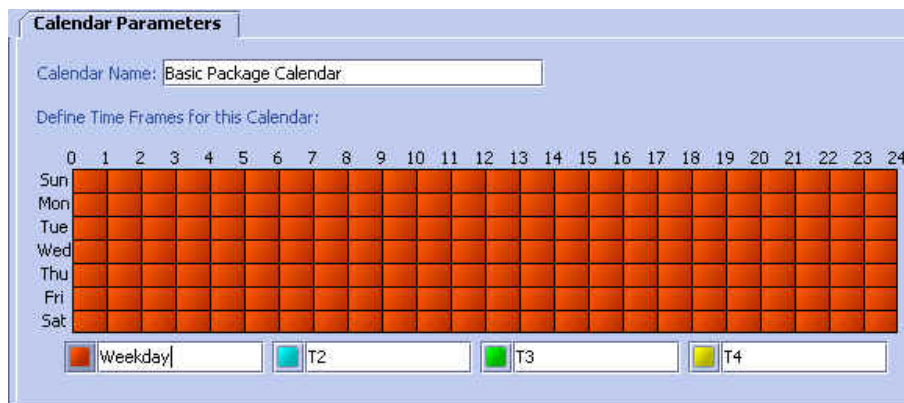
To rename the Time Frames:

Step 1 From the **Configuration** menu, click **Weekly Time Frames**.

In the **Calendar Parameters** tab, below the grid, each of the four time frames is listed in a text box next to a colored square.

Step 2 Click on the Time Tag field and type in the new name.

Figure 5-44: Editing the Time Tags



Step 3 Click **Close**.

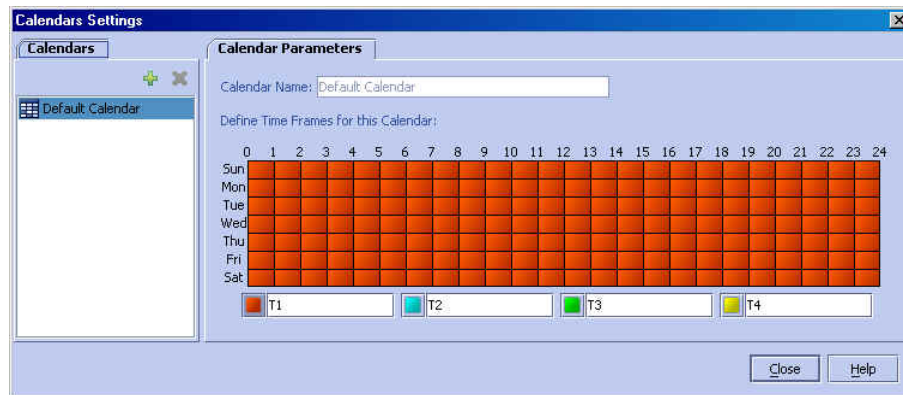
Configuring Weekly Time-Frames

To map the time frames:

Step 1 From the **Configuration** menu, click **Weekly Time Frames**.

The following dialog box appears.

Figure 5-45: Calendar Settings Dialog Box

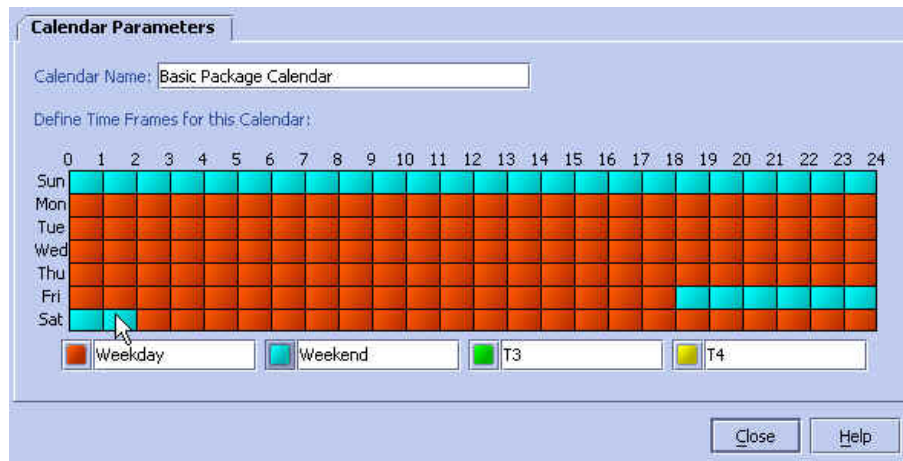


The tab on the left (**Calendar**) is used for adding and deleting calendars, while the tab on the right (**Calendar Parameters**) is used to define the time frames.

- Step 2** From the tab on the left (**Calendar**), select the calendar for which you want to configure the time frames.

In the **Calendar Parameters** tab, a grid, representing the hours in a 24/7 period with the instruction, **Define Time Frame names for this Calendar**, appears.

Figure 5-46: Defining the Time Frames



Below the grid, each of the four time frames is listed in a text box (*Time Tag*) next to a colored square.

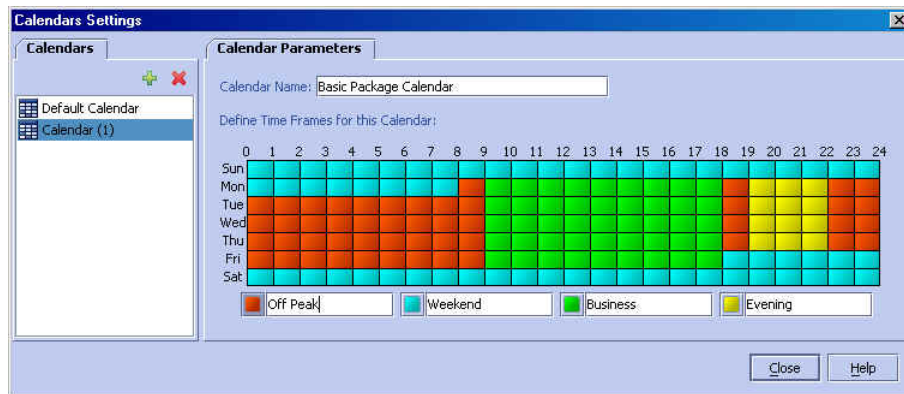
- Step 3** Click a colored square next to one of the time-tags.
- Step 4** Click one or more boxes within the Time Frames grid.
- Step 5** Repeat steps 2 and 3 until you have mapped the entire grid. You can change the grid by "overwriting" with another color.
- Step 6** If you wish to edit the time frame names, click on the Time Tag field next to the colored square and type in the new name.

Remember that this will change the time frame names for ALL calendars.

- Step 7** Click **Close** when you have completed the Time Frame mapping. This sets the changes you have made to the Service Configuration.

You have now mapped the period of 24/7 into 4 different time frames. The screen shown in the figure below illustrates a possible time partition plan:

Figure 5-47: Weekly Time Frames Settings Example



Bandwidth Control Revisited

This section explains how to combine the global controllers and subscriber BW controllers to achieve effective bandwidth control.

To configure total bandwidth control:

- Step 1** Configure the necessary global controllers.
- Try to ascertain which services are likely to be problematic, and what the maximum percentage of total bandwidth should be for each. Services/packages that are not likely to be problematic do not have to be specifically configured and can be included in the default controller.
- Step 2** Configure the subscriber BW controllers for the package.
- Add a subscriber BW controller for each type of upstream and/or downstream traffic that you want to limit, and configure the CIR and PIR accordingly.
- Step 3** Select the global controller with which each subscriber BW controller is to be associated.

For example, if you wanted to limit P2P and streaming traffic, you would:

- Step 1** Define two global controllers, name them P2P and streaming so that you remember which is which, and assign them each the desired percentage of traffic.

Figure 5-48: Global Controller Settings Link 1

Allow separate BW setting for each link

Link 1 Link 2

Upstream + -

Name	BW (%)	BW (Mbps)
Upstream Total Link Limit	100	1000Mbps
Default Global Controller	60	600Mbps
P2P Upstream	15	150Mbps
Streaming Upstream	25	1000Mbps

Downstream + -

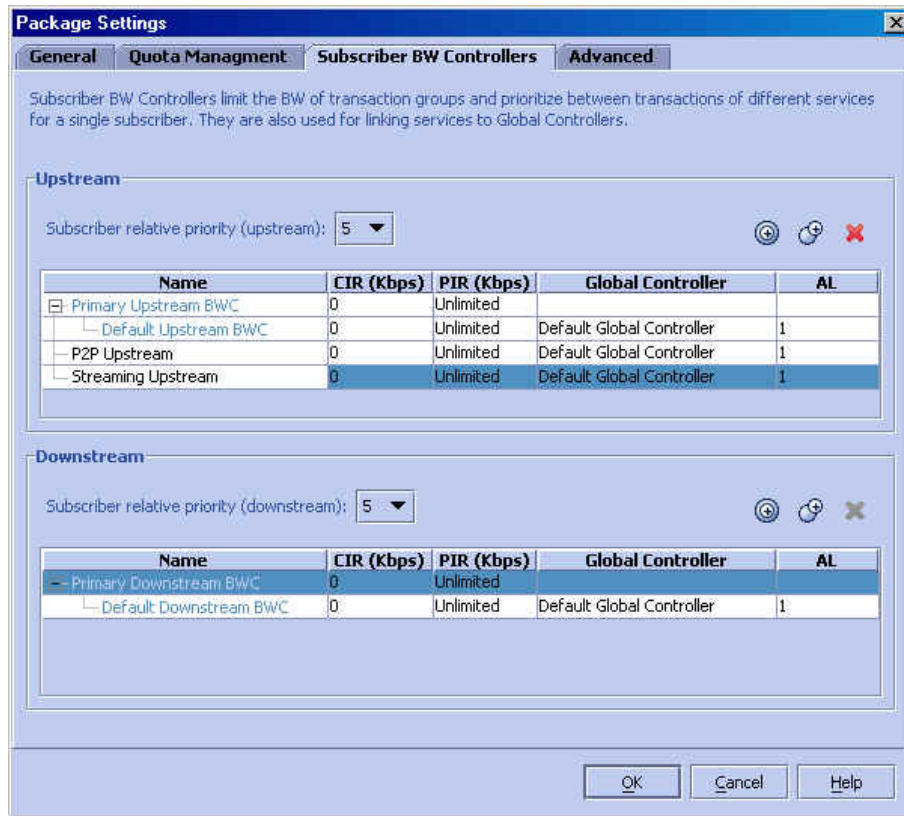
Name	BW (%)	BW (Mbps)
Downstream Total Link Limit	100	1000Mbps
Default Global Controller	60	600Mbps
P2P Downstream	15	150Mbps
Streaming Downstream	25	1000Mbps

View actual BW values for a specific SCE platform type: Gigabit Ethernet

OK Cancel Help

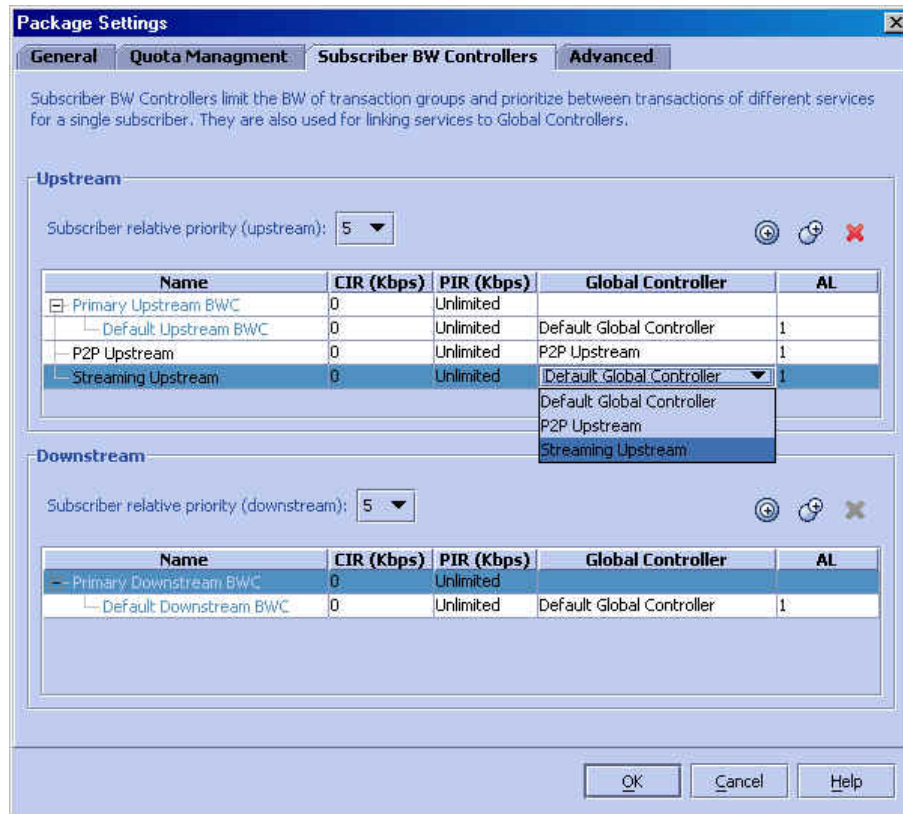
- Step 2** Then, in the default package you would add two BW controllers (decide whether they need to be both upstream and downstream) with appropriate PIR and CIR values.

Figure 5-49: Creating Subscriber BW Controllers



Step 3 Finally, you would assign one of the BW controllers to P2P, and the other to streaming. All subscriber traffic from these protocols will be added to the virtual queue total for these queues, and in turn, the bandwidth available to the subscriber for these protocols will fluctuate depending on how "full" these queues are.

Figure 5-50: Assigning the Subscriber BW Controllers



Managing RDR Settings

The SCE Platform creates and transmits RDRs that represent the information that is relevant to the provider for that traffic. These RDRs contain a wide variety of information and statistics, depending on the configuration of the system. For more details, see *RDR Format and Field Content* (on page C-1)

Use the *RDR Settings* dialog box to control the generation of RDRs for the entire Service Configuration. This dialog box contains six tabs:

- **Usage RDRs:** Enables and defines the time interval for total usage RDRs
- **Traffic Discovery:** Enables and defines the rate of generating transaction RDRs
- **Quota RDRs:** Defines the time interval for quota RDRs and enables the generation of quota breach RDRs.

- **Transaction Usage RDRs:** Specifies packages and services for which transaction usage RDRs should be generated.
- **Log RDRs:** Specifies packages and/or services for which log RDRs should be generated
- **Realtime RDRs:** enables the generation of realtime subscriber usage RDRs

Using the Usage RDRs Tab (RDR Settings)

- The SCE Platform can be configured to generate three types of usage RDRs:
- **Link Usage RDRs:** total usage of a particular service for the entire link
- **Package Usage RDRs:** total usage of a particular service by all the subscribers in a particular package
- **Subscriber Usage RDRs:** usage for each service by a particular subscriber

Use this tab to enable/disable the desired types of usage RDRs, and to define the time interval between generation of the specified usage RDRs.

To set the Usage RDR time intervals:

Step 1 From the **Configuration** menu, click **RDR Settings**.

The *RDR Settings* dialog box appears.

Figure 5-51: RDR Settings: Usage RDR Tab



Step 2 Click the **Usage RDR** tab.

Step 3 To enable a selected type of usage RDR, do the following:

- a) Check the appropriate **Generate Usage RDRs** checkbox.
- b) Type the interval in minutes between the generation of this type of usage RDRs in the appropriate field.

Step 4 Due the large number of subscribers, you may wish to limit the total rate of subscriber usage RDRs. Type the maximum number of subscriber usage RDRs to be generated per second in the appropriate field.

Step 5 Click **OK**.

The generation of usage RDRs is configured.

Using the Transaction Usage RDRs Tab (RDR Settings)

Each network transaction can generate a transaction usage RDR. If a Collection Manager is present, these RDRs are collected in CSV files and can be used for creating a transaction-level log of specific subscribers and services, suitable, for example, for transaction-based billing. As generating and collecting an RDR for each transaction might present a performance penalty, you should enable RDR generation only for those services and packages that will actually be monitored and/or controlled by the system.

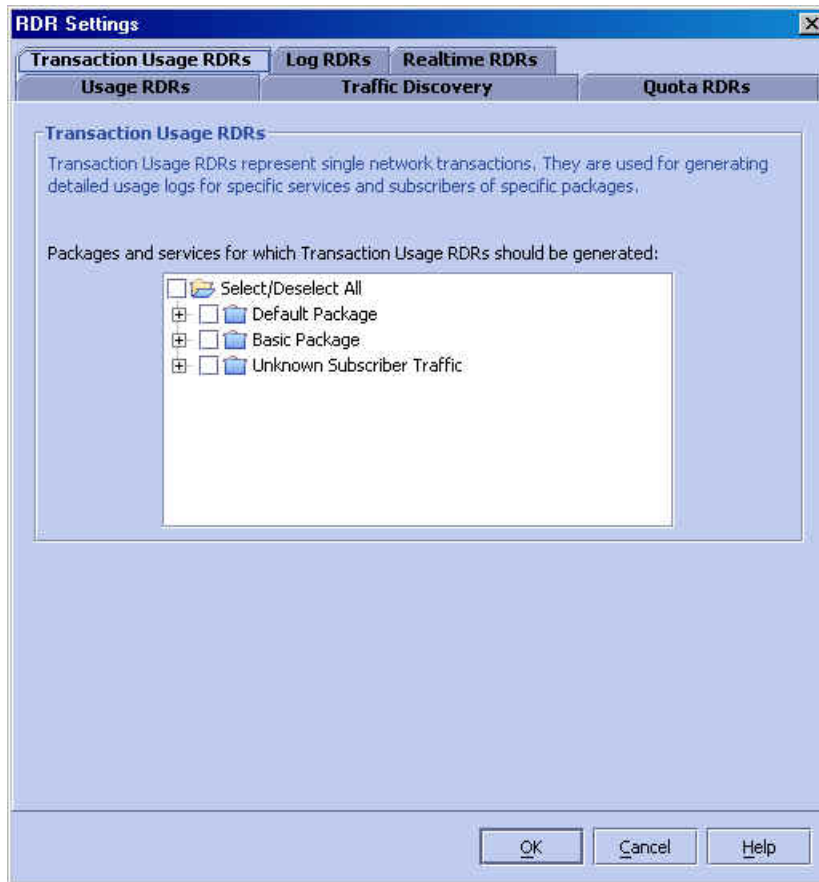
Use this tab to select the packages and/or services for which RDRs will be generated.

To set the Usage RDR time intervals:

Step 1 From the *RDR Settings* dialog box, click **Transaction Usage RDRs**.

The following dialog box appears.

Figure 5-52: RDR Settings: Transaction Usage Tab



Step 2 Select the packages and/or services for which transaction usage RDRs should be generated:

- To enable/disable transaction usage RDRs for an entire package: check/uncheck the checkbox next to the package name.

The package expands to show all component services, which are all selected/de-selected.

- To enable transaction usage RDRs for selected services only: click on the circle next to the package name to expand the package and display all component services.

Check the checkbox next to the desired service name to select that service.

Step 3 Click **OK**.

The generation of transaction usage RDRs is enabled for the selected packages/services.

Using the Log RDRs Tab (RDR Settings)

Log RDRs provide information regarding system events. They are generated in response to specific actions or state changes. Blocking RDRs and Breach RDRs are both log RDRs. As with Transaction usage RDRs, when a Collection Manager is present, these RDRs are collected in CSV files.

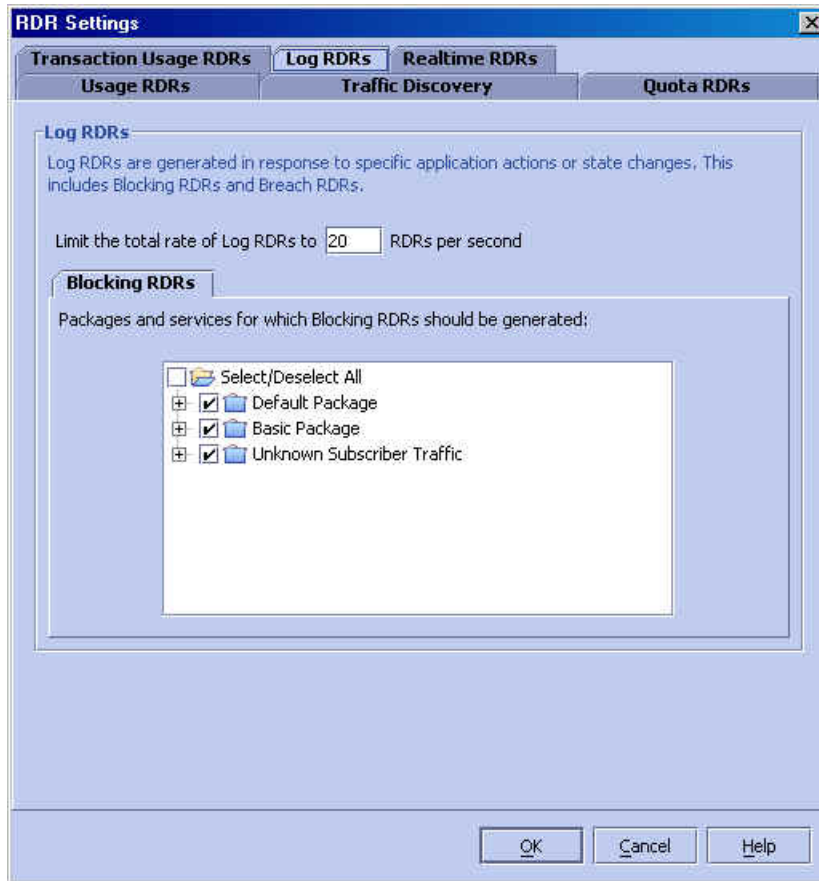
You should enable the generation of log RDRs only for services and packages where blocking or breach events actually need to be monitored.

To set the Log RDR parameters:

Step 1 From the *RDR Settings* dialog box, click **Log RDRs**.

The following dialog box appears.

Figure 5-53: RDR Settings: Log Tab



Step 2 Type in the maximum number of log RDRs to be generated per second.

Step 3 Select the packages and/or services for which blocking or breach RDRs should be generated:

- To enable/disable blocking and/or breach RDRs for an entire package: check/uncheck the checkbox next to the package name.

The package expands to show all component services, which are all selected/deselected.

- To enable blocking and/or breach RDRs for selected services only: click on the circle next to the package name to expand the package and display all component services.

Check the checkbox next to the desired service name to select that service.

Step 4 Click **OK**.

Using the Traffic Discovery Tab (RDR Settings)

Each network transaction can generate a transaction RDR. If a Collection Manager is present, these RDRs are collected in a DB for traffic discovery, that is, generating statistical histograms that help understand what kind of traffic is traversing the network.

Use this tab to enable/disable the generation of transaction RDRs and to define the number of RDRs generated per second.

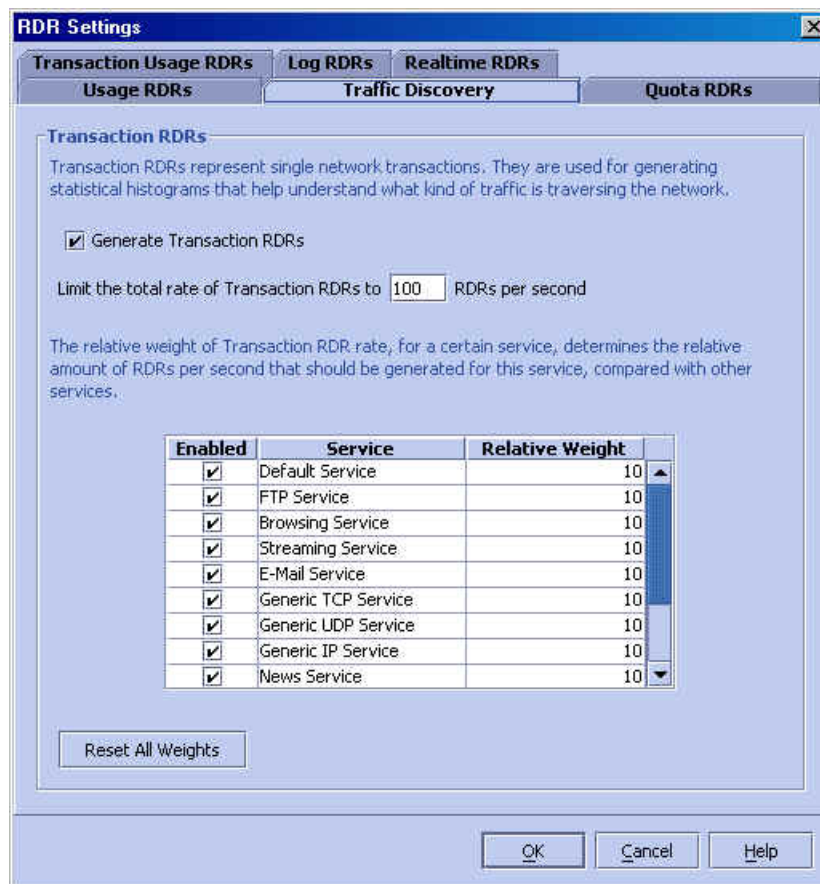
You can also set the relative amount of RDRs generated per second for each service by assigning relative weights to services. This lets you focus on transactions of specific services, while reducing the rate of transaction RDRs generated for other services.

To configure the generation of transaction RDRs:

Step 1 From the *RDR Settings* dialog box, click **Traffic Discovery**.

The following dialog box appears.

Figure 5-54: RDR Settings: Traffic Discovery Tab



Step 2 To enable transaction RDRs, do the following:

- Check the **Generate Transaction RDRs** checkbox.

- Type rate of transaction RDR generation in seconds in the field.

Step 3 For each service for which you wish transaction RDRs to be generated, do the following:

- Check the **Enabled** checkbox next to the service name.
- Double-click on the weight in the **Relative Weight** column and type in the desired weight

Step 4 Click **OK**.

The generation of transaction RDRs is configured.

Using the Quota RDRs Tab (RDR Settings)

There are three types of Quota RDRs:

- **Remaining Quota RDRs:** As quota is consumed, Remaining Quota RDRs are generated. The user can choose to enable or disable these RDRs (default is disable) and specify how often the RDR is generated.

The RDR contains the subscriber-ID and the remaining quota in each of the subscriber's quota buckets. The RDR is only generated if bucket state has change since the last RDR.

- **Quota Threshold RDRs:** When quota in a bucket falls below a configured threshold, a Quota Threshold RDR is generated. This RDR can be used by external systems, which can handle this RDR as a quota request, and provision the subscriber with more quota before the bucket is depleted.
- **Quota Breach RDRs:** When a quota bucket is depleted, services that try to consume from that bucket are regarded as "breached". A Quota Breach RDR is generated when quota breach occurs.

When a subscriber's service is in "breached" state, it is handled according to the service's breach-handling settings. For example, it is possible to block flows of a specific service once the quota for that service is breached.

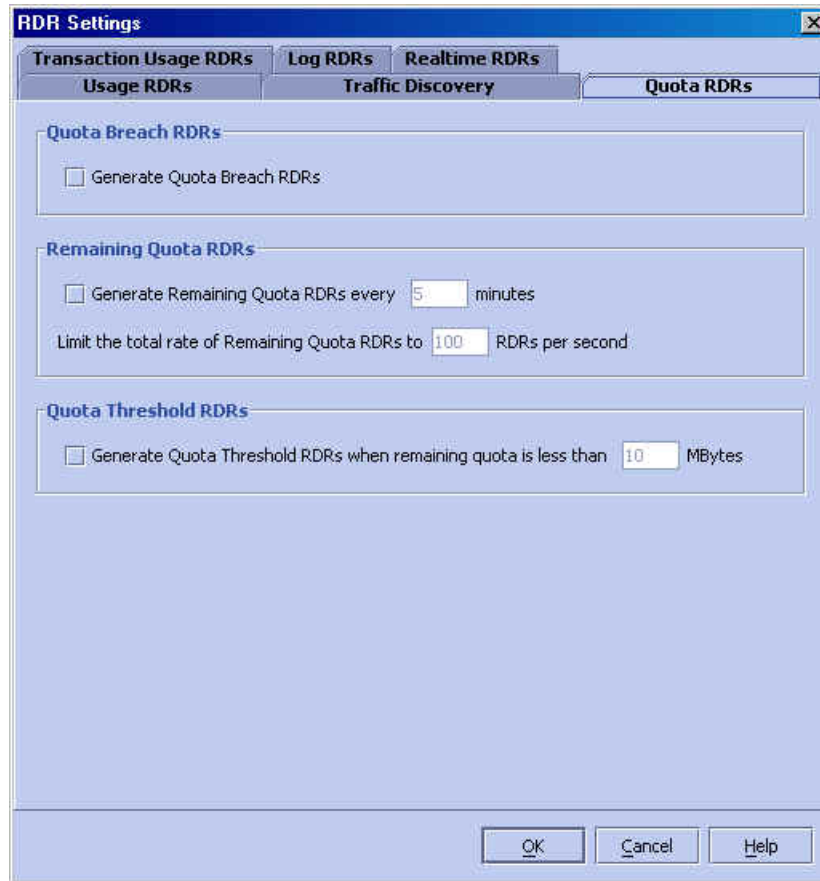
Use this tab to enable/disable the generation of quota RDRs and to define the number of RDRs generated per minute/second.

To configure the generation of quota RDRs:

Step 1 From the *RDR Settings* dialog box, click **Quota RDRs**.

The following dialog box appears.

Figure 5-55: RDR Settings: Quota RDRs



Step 2 To enable "Quota Breach" RDRs, check the **Generate Quota Breach RDRs** checkbox

Step 3 To enable "Remaining Quota" RDRs, do the following:

- a) Check the **Generate Remaining Quota RDRs** checkbox.
- b) Type rate of quota RDR generation per minute per service in the field.

Step 4 Type in the maximum number of Remaining Quota RDRs to be generated per second.

Step 5 To enable "Quota Threshold" RDRs, do the following:

- a) Check the **Generate Quota Threshold RDRs** checkbox.
- b) Type threshold under which Quota Threshold RDR should be generated in the field.

Step 6 Click **OK**.

Using the Realtime RDRs Tab (RDR Settings)

Realtime RDRs are RDRs that report subscriber usage. These RDRs are generated for each individual subscriber for each service used, at specified intervals. These RDRs permit a more granular monitoring of selected subscribers when necessary.

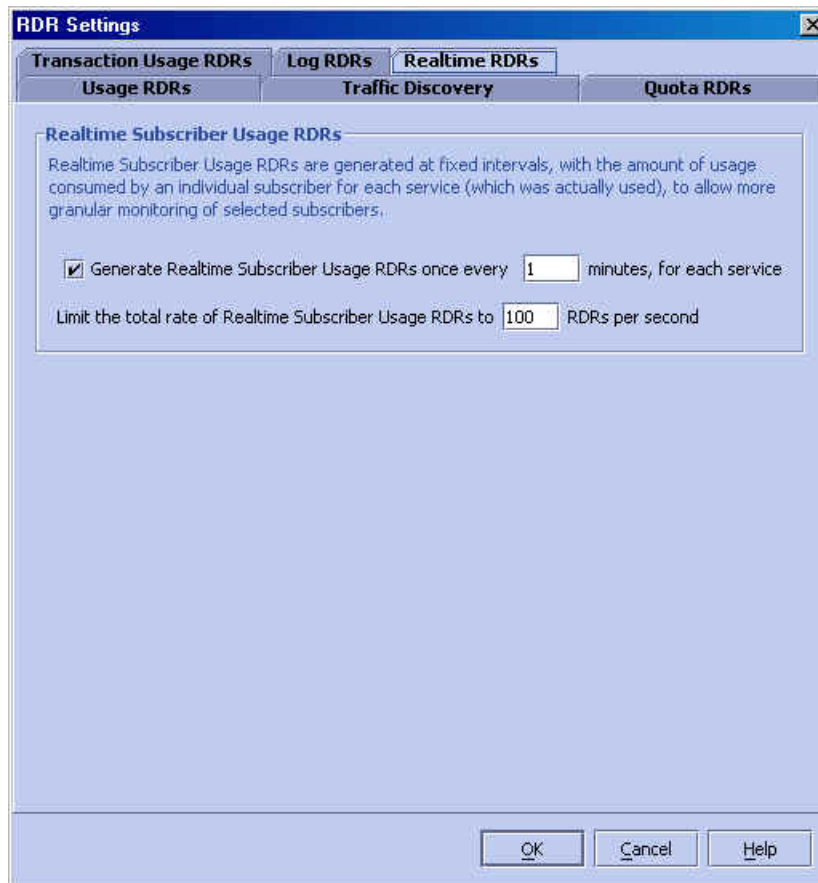
See *Managing Real-time Subscriber Usage RDRs* (on page 7-21) for more information on selecting subscribers to be monitored.

To set the Realtime RDR parameters:

Step 1 From the *RDR Settings* dialog box, click Realtime **RDRs**.

The following dialog box appears.

Figure 5-56: RDR Settings: Realtime Tab



Step 2 To enable Realtime RDRs, do the following:

- a) Check the **Generate Realtime Subscriber Usage RDRs** checkbox.
- b) Type rate of realtime RDR generation per minute per service in the field.

Step 3 Type in the maximum number of Realtime Subscriber Usage RDRs to be generated per second.

Step 4 Click **OK**.

Subscriber Notification

The subscriber notification feature provides the means to push a web-based message to a subscriber by redirecting the subscriber HTTP traffic to the relevant web pages. These web pages contain information relevant to the subscriber, such as notifications of quota depletion. HTTP redirection starts when the subscriber notification is activated, and ceases when the notification is dismissed.

The SCAS BB Console supports a maximum of 31 subscriber notifications. For each subscriber notification, the following information must be configured

- **Name:** The name assigned to the notification. (Default is “Notification #”.)
- **Destination URL:** URL to which the subscriber HTTP traffic will be directed. This web page usually contains the message that needs to be conveyed to the subscriber.
- **Notification Parameters:** The query part of the destination URL, which can be optionally added upon redirection.

The format of the notification parameters to be added to the destination URL is:

```
?n=<notification-ID>&s=<subscriber-ID>
```

Where <notification-ID> is the numeric ID of the notification that redirected the subscriber, and <subscriber-ID> is the subscriber name.

These parameters can be used by the destination web server to carry a more purposeful message to the subscriber.

- **Notification is dismissed when:** indicates when to dismiss, or deactivate, the notification state. May be any one of the following:
 - **Subscriber browses to destination URL (default):** As soon as the subscriber browses to the destination URL defined above, he has been duly notified and the notification state is dismissed.

For instance, if a subscriber has exceeded his quota, the notification state may be dismissed as soon as he browses to the destination URL, which informs him of this fact (even though the subscriber would still remain in breach state)..
 - **The condition that activated the notification no longer holds:** The dismissal of the notification state is dependent on the resolution of the condition, rather than on the subscriber

For instance, if a subscriber has exceeded his quota, the notification state may only be dismissed when he has completed the procedure to refresh his quota.
 - **Subscriber browses to dismissal URL:** The subscriber must proceed from the destination URL to a different final URL before the notification state is dismissed.

The dismissal URL is composed of the URL hostname and the URL path, separated by a colon, in the following format:

```
[ * ]<hostname> : /<path> [ * ]
```

- <hostname> may optionally be preceded by a wildcard (*), to match all hostnames with the same suffix.
- <path> may be followed by a wildcard, to match all paths with common prefix.
- /<path> must always start with '/'.

For example, the entry:

```
*.some-isp.net:/redirect/*
```

will match all these URLs:

- www.some-isp.net/redirect/index.html
- support.some-isp.net/redirect/info/warning.asp
- noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8

For instance, if a subscriber has exceeded his quota, the web page at the destination URL may ask the subscriber to press an 'acknowledge' button after reading the message. The acknowledge URL would be defined as the dismissal URL, and would therefore deactivate further notifications.

- **List of Allowed URLs:** list of URLs that will not be blocked and redirected although notification is activated.

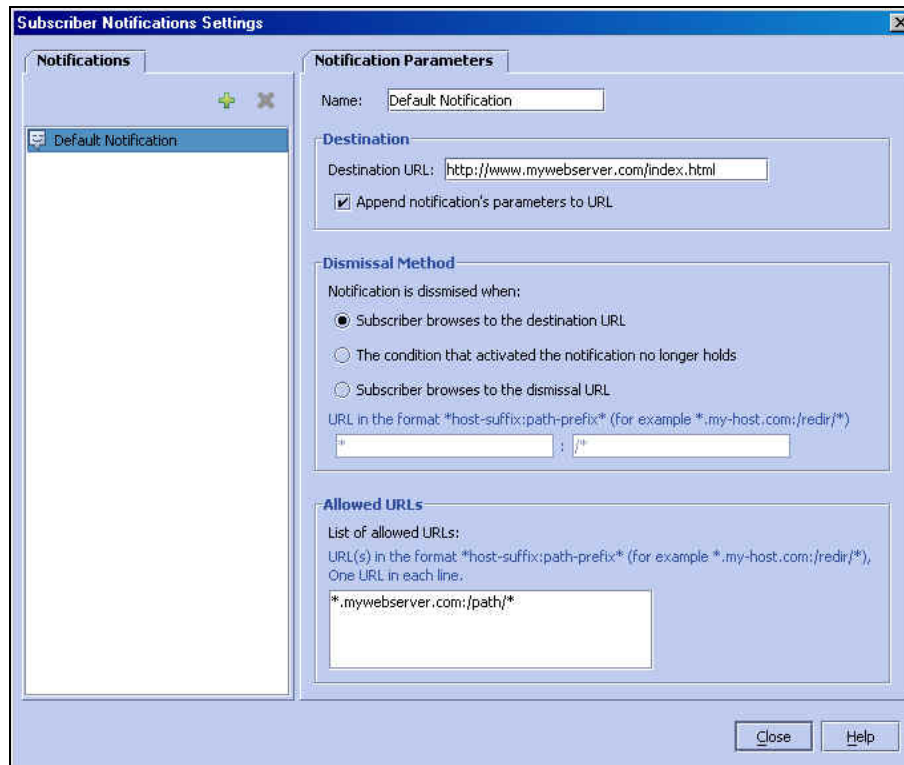
The allowed URLs are defined same format as the dismissal URL, (see above).

Note that the creation of a subscriber notification does not activate the subscriber notification feature. After the subscriber notification is defined, it must be activated for a particular package. (*The Breach Handling Tab (Service Rule)* (on page 5-61))


To create a Subscriber Notification:

Step 1 In the **Configuration** menu, select **Subscriber Notification**.

Figure 5-57: Subscriber Notification Dialog



The **Subscriber Notification Settings** dialog opens.

- Step 2** Click the add icon  the **Name** field, type in the desired name, if different from the default (Notification #).
- Step 3** In the **Destination URL** field, type in the desired Destination URL. If the notification parameters should be appended to the entered Destination URL, check the appropriate check box.
- Step 4** Check the appropriate check box to indicate when the notification is to be dismissed.
- If **Subscriber browses to dismissal URL** is selected, type the dismissal URL host-suffix and path-prefix in the fields provided.
- Step 5** Type any allowed URLs in the box provided.

To edit a Subscriber Notification:

-
- Step 1** In the **Configuration** menu, select **Subscriber Notification**.
The **Subscriber Notification Settings** dialog opens.
- Step 2** Select the desired Subscriber Notification from the list in the left pane.
- Step 3** Edit the fields as desired.
-

To delete a Subscriber Notification:


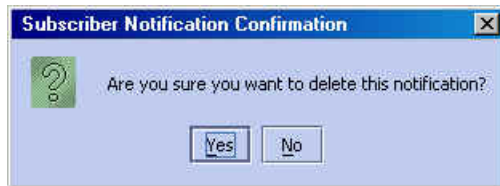
-
- Step 1** In the **Configuration** menu, select **Subscriber Notification**.
The **Subscriber Notification Settings** dialog opens.
- Step 2** Select the subscriber notification to be deleted from the list in the left pane.
- Step 3** Click the delete icon .
The system asks for confirmation.

Figure 5-58: Subscriber Notification Delete Confirmation



- Step 4** Click *Yes*.
The selected subscriber notification is deleted.
-

A subscriber notification that is currently used by any rule cannot be deleted. The following warning will appear:

Figure 5-59: Subscriber Notification Warning



Filtering the Traffic Flows

Filter Rules are the part of the Service Configuration that lets you direct the SCE Platform to ignore some types of transactions based on Layer 3 and Layer 4 properties, and transmit them unchanged.

When a traffic flow enters the SCE Platform, the SCE Platform checks whether a Filter Rule applies to this traffic flow.

If a Filter Rule does apply to this traffic flow, the SCE Platform passes the traffic flow to its transmit queues. No RDR generation or Service Configuration enforcement is done. This means that these flows will not appear within any records generated for analysis purposes nor will they be controlled (under *SCAS BB* Capacity/Tiered Control) by any active rule belonging to the active Service Configuration.

It is recommended to create filter rules for OSS protocols (such as DHCP) and routing protocols (such as BGP) which might traverse the SCE Platform, as these protocols usually should not be affected by policy enforcement and are also insignificant for reporting.

Use this feature to add, remove or edit a Filter Rule.

Constructing a Filter Rule

Construct a Filter Rule by defining the filter values for the various flow properties. When a flow, identified based on Layer 3 and Layer 4 properties as matching this filter definition, reaches the SCE Platform, the system automatically ignores the transaction. You can construct multiple Filter Rules as well as delete them.

Constructing a Filter Rule consists of defining the Layer 3 and Layer 4 parameters of the traffic flow that are to be ignored.

You construct a Filter Rule by setting the values for a variety of the traffic flow parameters.

The following parameters are defined within a Filter Rule:

- Transport Type
- Direction
- Source IP address
- Destination IP address
- Source port
- Destination port
- ToS
- CoS
- Filter Rule Name

Adding a Filter Rule

The Add Filter Rule Wizard guides you through the process of adding a Filter Rule.

To add a Filter Rule:

Step 1 From the **Configuration** menu, click **Network Traffic**

or

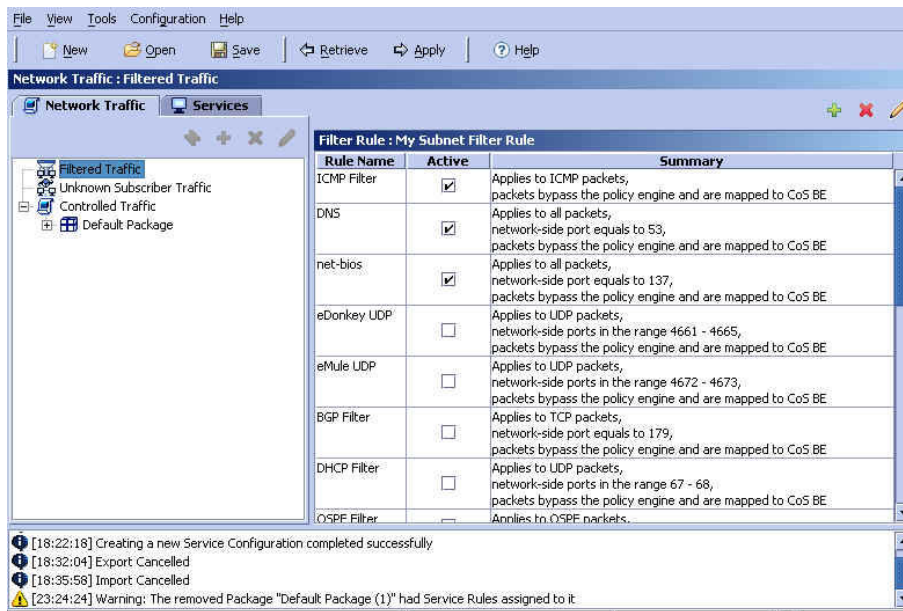
In the Network Traffic/Services band, click the **Network Traffic** tab and select the *Filtered Traffic*

Filtering the Traffic Flows

category.

The *SCAS BB Console - Network Traffic Tab with Filtered Traffic* appears.

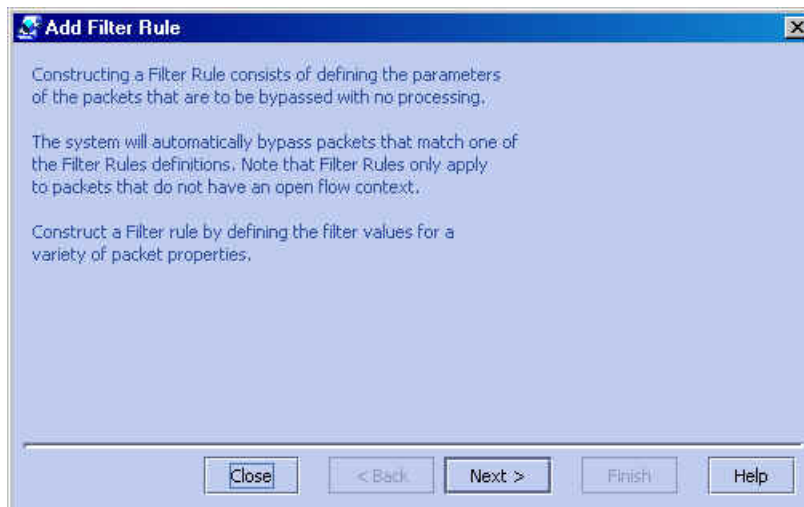
Figure 5-60: Network Traffic Tab with Filtered Traffic



Step 2 Click  (**Add**) on the right hand side.

The *Add Filter Rule Wizard - Start* dialog box appears.

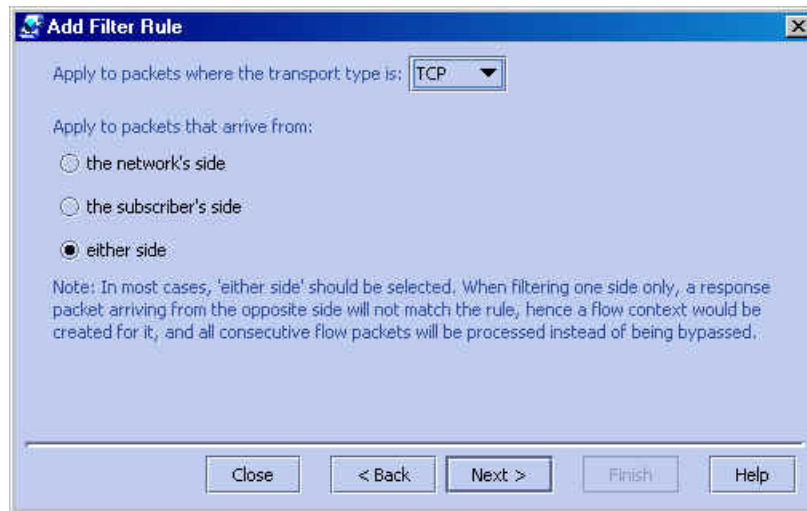
Figure 5-61: Add Filter Rule Wizard - Start



Step 3 Click **Next**.

The *Add Filter Rule Wizard - Protocol* dialog box appears.

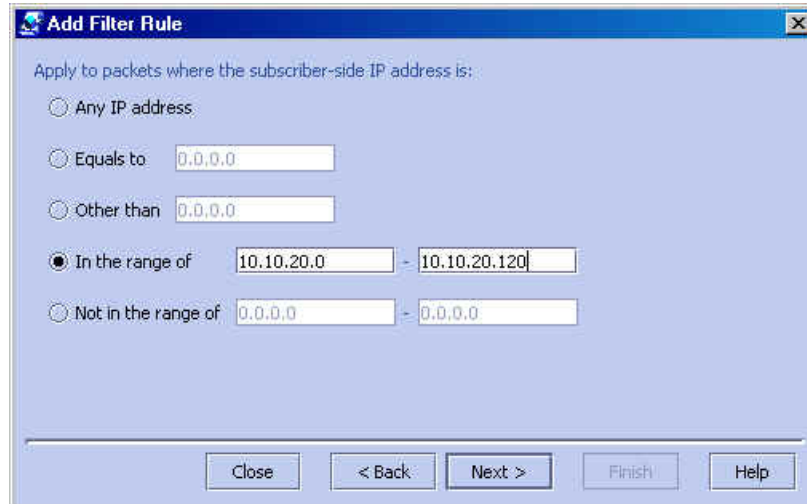
Figure 5-62: *Add Filter Rule Wizard - Protocol*



Step 4 Select the transport type and initiating side, and click **Next**.

The *Add Filter Rule Wizard - Source IP Address* dialog box appears.

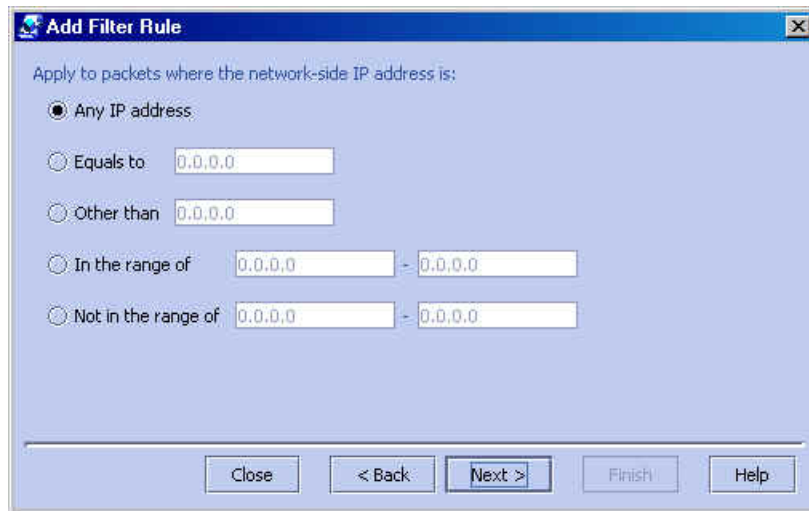
Figure 5-63: *Add Filter Rule Wizard - Source IP Address*



Step 5 Define the source IP address and click **Next**.

The *Add Filter Rule Wizard - Destination IP Address* dialog box appears.

Figure 5-64: *Add Filter Rule Wizard - Destination IP Address*

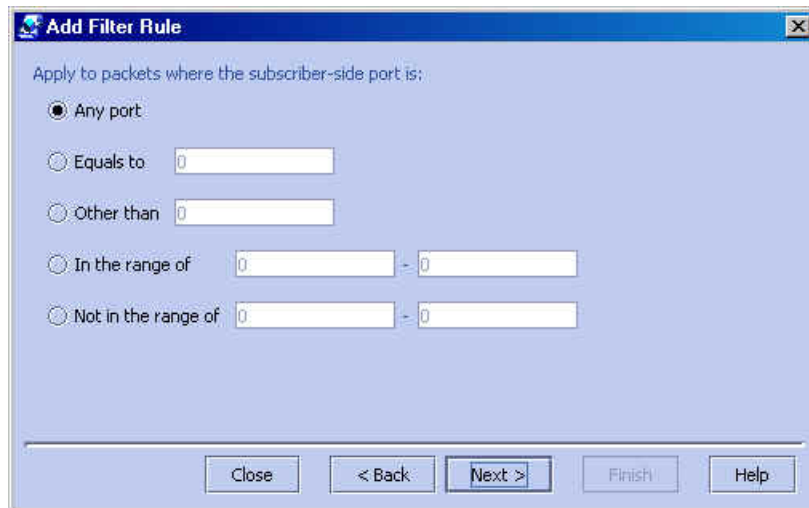


Step 6 Define the destination IP address and click **Next**

If the transport protocol selected was TCP, UDP or ANY, the *Add Filter Rule Wizard - Source Port* dialog box appears.

If any other transport protocol was selected, the *Add Filter Rule Wizard - ToS* dialog box appears. Go to step 9.

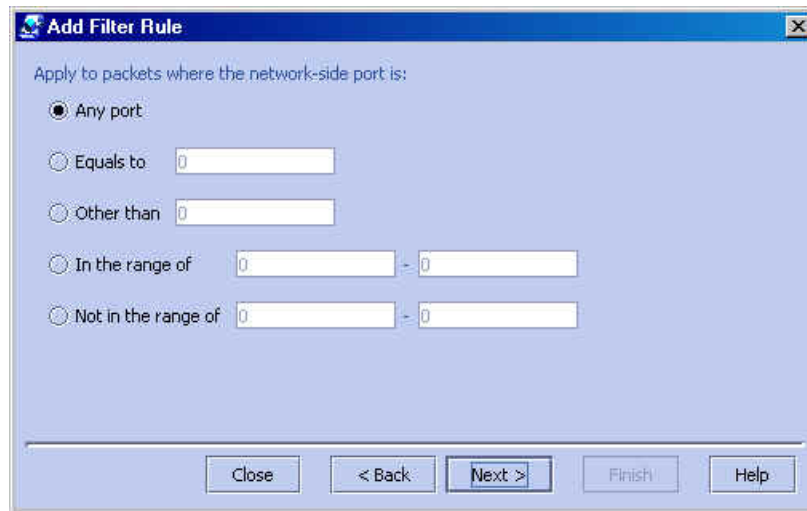
Figure 5-65: *Add Filter Rule Wizard - Source Port*



Step 7 Define the source port and click **Next**.

The *Add Filter Rule Wizard - Destination Port* dialog box appears.

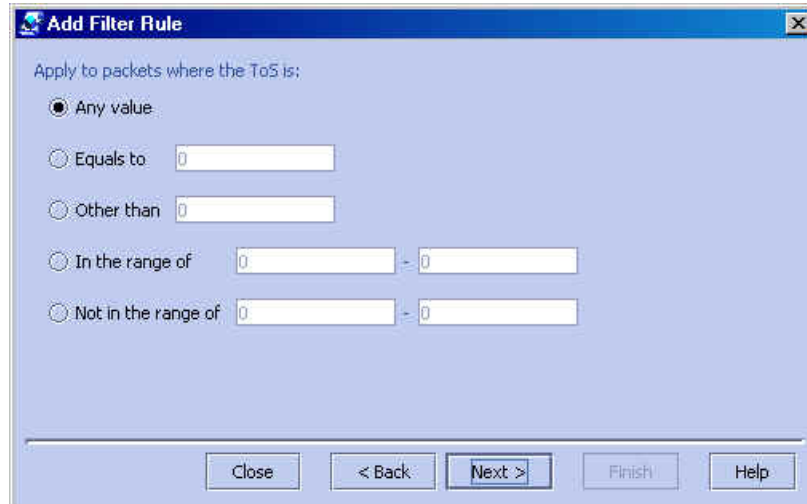
Figure 5-66: *Add Filter Rule Wizard - Destination Port*



Step 8 Define the destination port and click **Next**

The *Add Filter Rule Wizard - ToS* dialog box appears.

Figure 5-67: *Add Filter Rule Wizard - ToS*



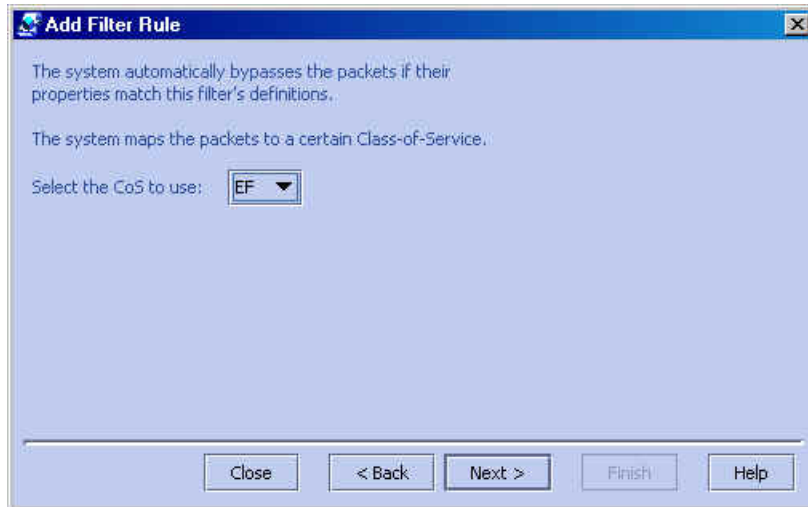
Step 9 Define the ToS and click **Next**.

Note: ToS acceptable values are 0-63.

Filtering the Traffic Flows

The *Add Filter Rule Wizard - CoS* dialog box appears. (*SCAS BB* Capacity Control and *SCAS BB* Tiered Control only)

Figure 5-68: Add Filter Rule Wizard - CoS



Step 10 Select the CoS value and click **Next**. The *Add Filter Rule Wizard - Finish* dialog box appears.

Figure 5-69: Add Filter Rule Wizard - Finish

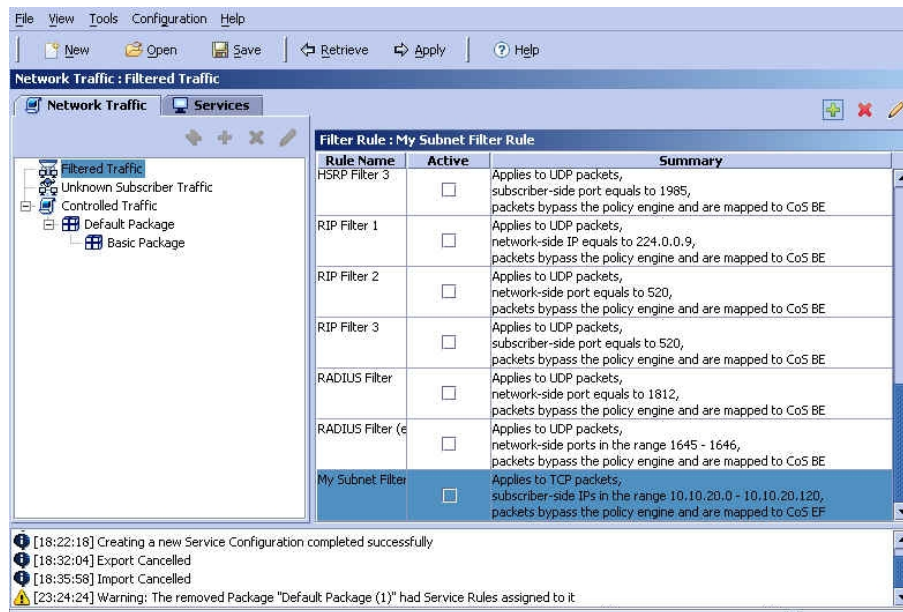


Step 11 (Recommended) In the *Rule Name* text box, type a meaningful name.

(Optional) Select the *Activate this rule* check box to activate the Filter Rule. Traffic will be filtered according to the rule only when it is activated.

The Filter Rule is added and displayed in the Filter Rule table.

Figure 5-70: New Filter Rule



Editing a Filter Rule

You can view and edit the parameters of a Filter Rule.

To edit a Filter Rule:

Step 1 In the Network Traffic/Services band, click the **Network Traffic** tab and select the *Filtered Traffic* category.

Step 2 Select the Filter Rule from the Filter Rule table.

Step 3 Click  (**Edit**).

The *Edit Filter Rule Wizard - Start* dialog box appears.

The Edit Filter Rule Wizard is the same as the Add Filter Rule Wizard except that in *SCAS BB* View mode, the option in the CoS dialog box is disabled.

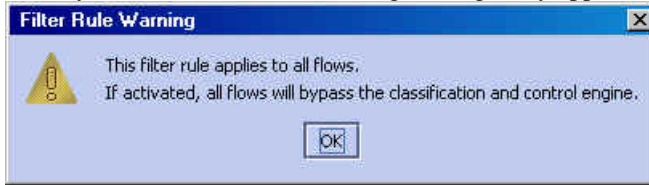
Step 4 Follow the instructions in the section *Adding a Filter Rule* (on page 5-89), step 4 through step 12

Step 5 Click **Finish**.

The Filter Rule is changed and displayed in the Filter Rule table.

**Note**

When you click **Finish** the following message may appear:




Click **OK**

Removing a Filter Rule

Filter Rules can be removed, for example, when you want the system to resume handling the IP addresses and their attributes according to the individual rules that were previously defined for each subscriber IP address.

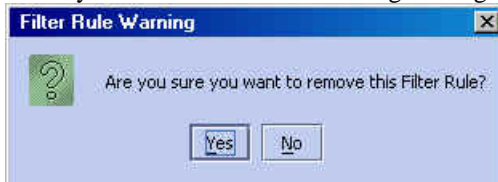
To remove a Filter Rule:

- Step 1** In the Network Traffic/Services band, click the **Network Traffic** tab and select the *Filtered Traffic* category.
- Step 2** Select the Filter Rule from the Filter Rule table.
- Step 3** Click  (**Remove**).

The Filter Rule is removed and is no longer displayed in the Filter Rule table.

**Note**

When you click **Finish** the following message may appear:



Click **Yes**.

Activating a Filter Rule

To activate a Filter Rule:

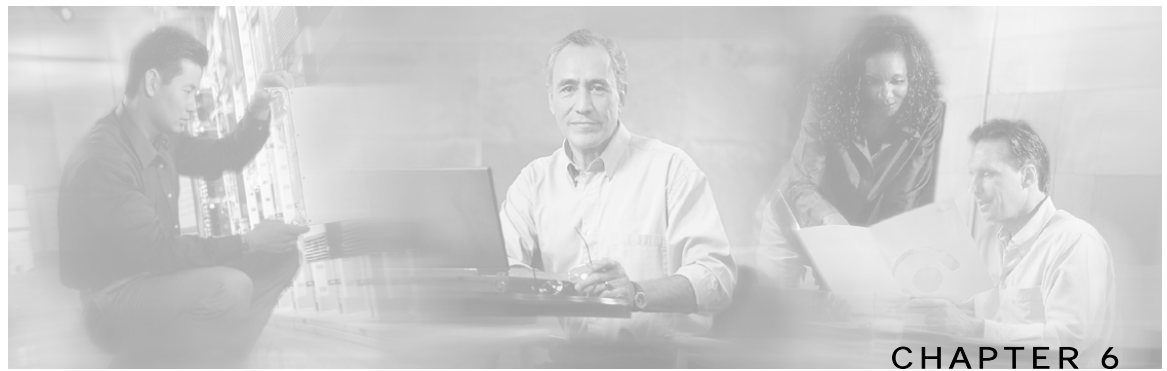
-
- Step 1** In the Network Traffic/Services band, click the **Network Traffic tab** and select the *Filtered Traffic* category.
 - Step 2** Select the Filter Rule from the Filter Rule table.
 - Step 3** Select the **Active** check box.
The Filter Rule is activated.
-

Deactivating a Filter Rule

You can deactivate a Filter Rule. This has the same effect as removing it, but the parameters are retained in the Service Configuration, and the Filter Rule can be reactivated at a later date.

To deactivate a Filter Rule:

-
- Step 1** In the Network Traffic/Services band, click the **Network Traffic tab** and select the *Filtered Traffic* category.
 - Step 2** Select the Filter Rule from the Filter Rule table.
 - Step 3** Clear the **Active** check box.
The Filter Rule is no longer activated.
-



Managing the System Settings

In this chapter you learn how to manage the System Settings. This feature is a part of the options available via the SCAS BB Console, allowing you additional control of the Service Control Application Suite for Broadband application.

In addition, this chapter explains how to import dynamic signatures to enable detection of new protocols and how to configure attack filtering.

This chapter contains the following sections:

- [Understanding the System Settings](#) 6-1
- [Dynamic Signature Management](#) 6-10
- [Attack Filtering and Subscriber Notification](#) 6-13

Understanding the System Settings

The SCAS BB Console allows you to determine various system parameters that control:

- The operational state of the system.
- The redirection URLs for protocols that support redirection.
- P2P detection.
- Ongoing Policy Check configuration.

Configuring the System Mode Parameter

The SCAS BB Console allows you to select the operational mode of the system. This feature allows you to define how the system handles network traffic.

(Note that Service Rules have an enabled/disabled mode of their own, which might differ from the system mode. In this case, the "lower" of the two modes is used. For example, if a rule is enabled, but the system mode is report-only, the rule will only generate RDRs).

The three System Modes are explained below:

- **Full functionality:** In *SCAS BB* View, this option is disabled. The system performs reporting, as well as active network enforcement according to the defined settings and Rules. This System Mode is limited to systems with a license for *SCAS BB* Capacity/Tiered Control.

- **Report only:** The system performs reporting functions only (that is, generating RDRs) according to the System Settings and Rule definitions. No active Rule enforcement is performed on the network traffic. In this mode, the report-only status is assigned to all Rules in the entire system. Therefore, the report option functions for analysis or debug purposes only, for example, to report when certain limitations are reached. No active networking enforcements are performed, meaning that the Rule parameters are not enforced by the SCE Platforms.
- **Transparent:** The system does not generate RDRs and does not enforce active Rules on the network traffic.

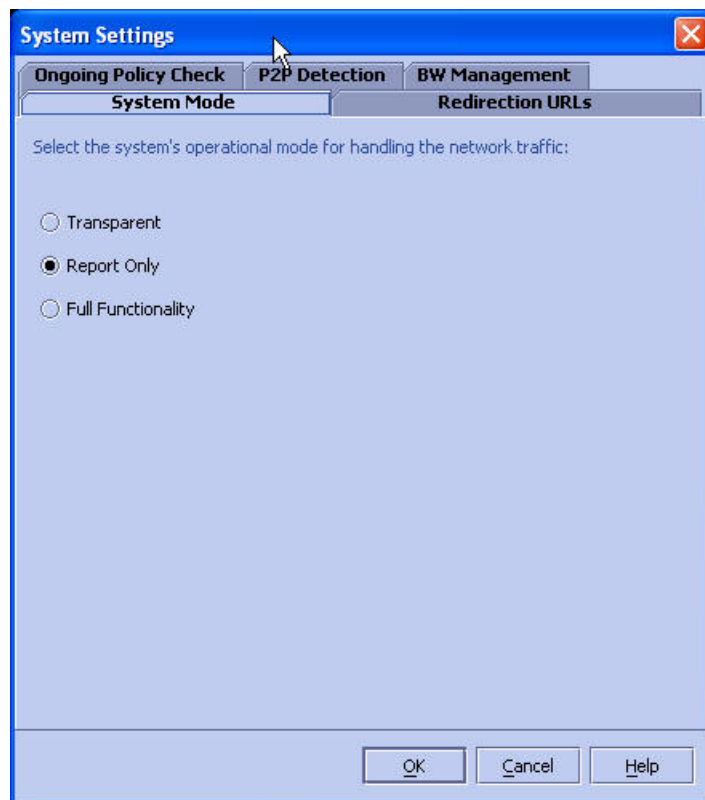
To configure the System Mode parameter:

Step 1 From the **Configuration** menu, click **System Settings**.

Step 2 Click the **System Mode** tab.

The following dialog box appears.

Figure 6-1: System Settings: System ModeTab



Step 3 Click one of the three option buttons:

- **Full functionality**
- **Reports only**
- **Transparent**

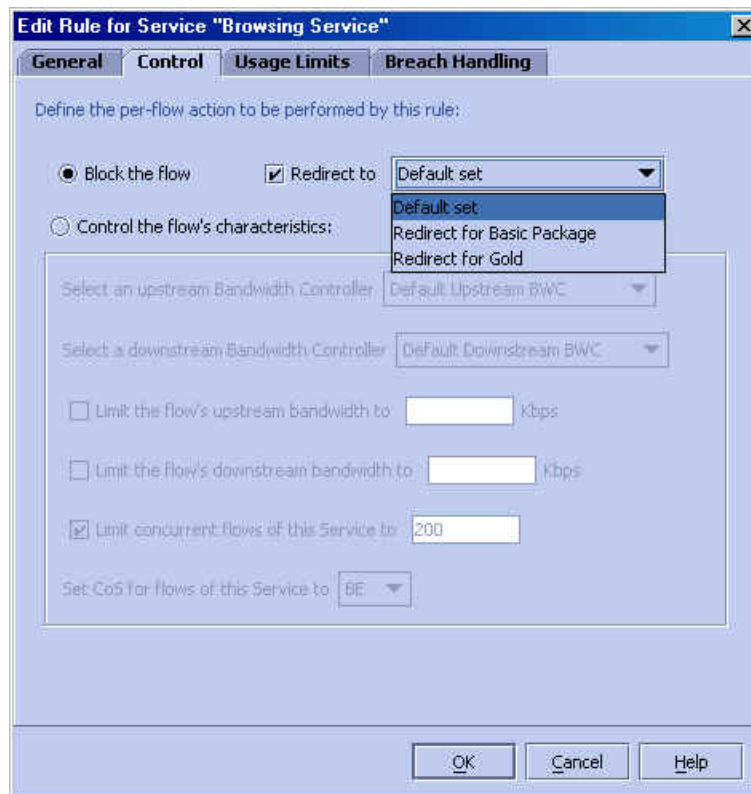
Step 4 Click **OK**.

The new System Mode setting is saved.

Setting Redirection Parameters

The rules for any package may deny access to certain protocols. When access to a protocol is blocked, the traffic flow may be redirected to an appropriate URL. As a result, when subscribers belonging to that Package attempt to use the Service, they are redirected to a selected set of URLs. This feature is configured via the **Control** tab of Rules definition. (See *The Control Tab (Service Rule)* (on page 5-56)). These sets of redirection URLs are defined in the *Redirection URLs* tab of the System Settings.

Figure 6-2: System Settings: Control Tab



Use the SCAS BB Console Redirection feature to define the URL to which specific types of protocols will be redirected. Not all protocols are supported. The three protocols that are supported are:

- HTTP Browsing
- HTTP Streaming
- RTSP Streaming

Each set of redirection URLs contains one redirection option for each of these three protocols.

The system provides a default set of URLs (*Default set*). This set cannot be removed. You can add additional sets, assigning each a significant name. When generating a new set, the system will automatically supply the current default URL values. You can assign a different URL to each protocol, or you can use the same URL supplied under the Default set of redirection URLs.

Each redirection URL includes the URL specified name, the Subscriber ID and the Service ID, set in the following format:

```
<URL>?n=<subscriber-ID>&s=<service-ID>
```

One possible use of this feature is to redirect subscribers to a server that you set up, where a posted web page provides them with an explanation that includes details on the cause for the redirection. The reason may be, for example, a "Silver" subscriber trying to access a Service that is only available to "Gold" subscribers. It is possible to use this web page to then offer the subscriber the opportunity to upgrade their package.

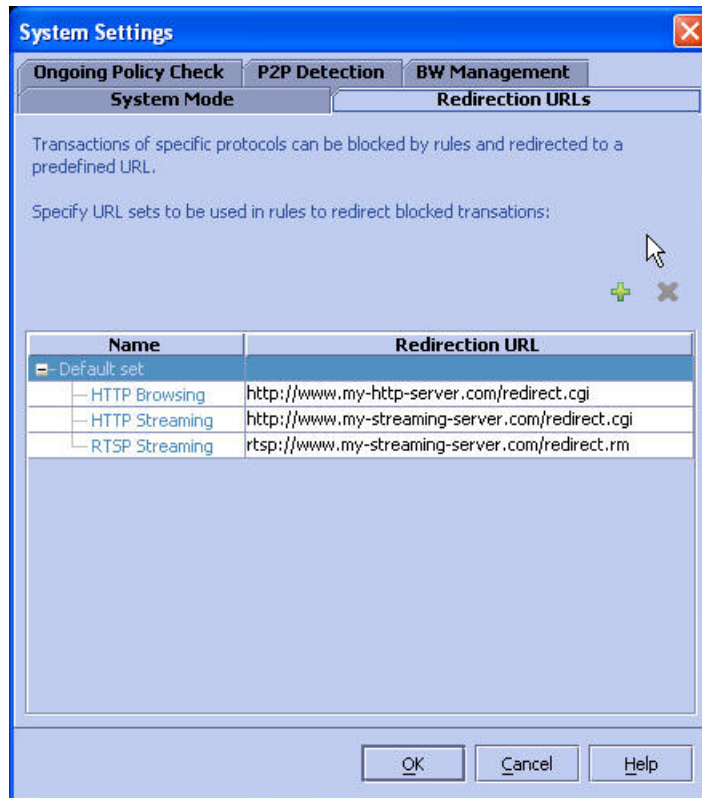
Configuring the Redirection Parameters

To edit an existing set of Redirection URLs:

-
- Step 1** From the **Configuration** menu, click **System Settings**.
 - Step 2** Click the **Redirection URLs** tab.

The following dialog box appears.

Figure 6-3: System Settings: Redirection Tab



Step 3 Click the URL in the **Redirection URL** column that you want to edit.

Step 4 Type in the desired changes.

Step 5 Click **OK**.

The Redirection settings are saved.

Adding a Set of Redirection URLs

You must have an *SCAS BB* Tiered Control license in order to add URL sets.

To add a redirection set:

Step 1 From the **Configuration** menu, click **System Settings**.

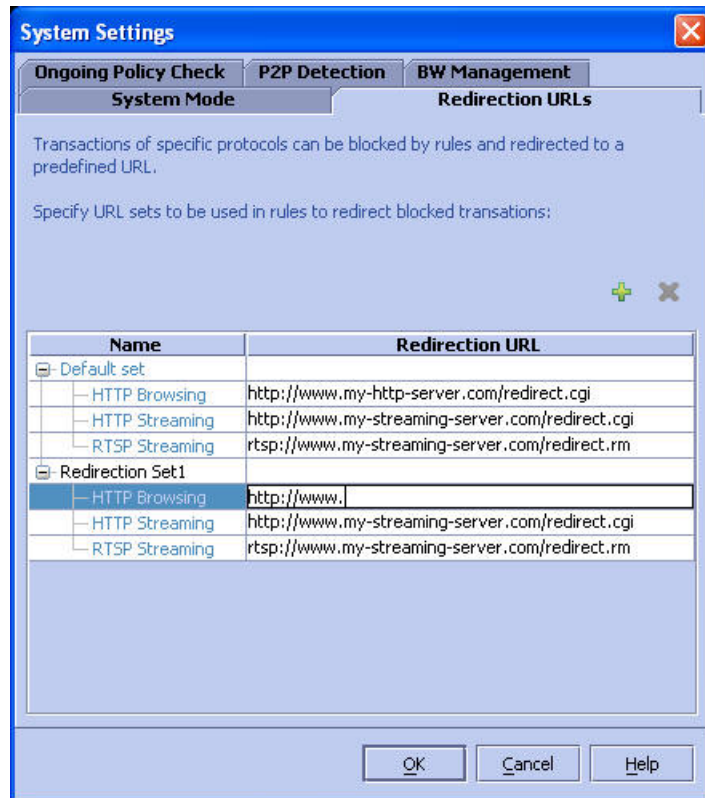
Step 2 Click the **Redirection URLs** tab.

The *System Settings - Redirection URLs Tab* dialog box appears, see the figure below.

Step 3 Click  (**Add**).

A new set will appear with the default URL names.

Figure 6-4: System Settings - Adding a Set of Redirection URLs



Step 4 (Optional) Edit the name of the group that appears in the **Name** column.

Step 5 Click **OK**.

The Redirection group is added.

Removing a Set of Redirection URLs

To remove a redirection set:

Step 1 From the **Configuration** menu, click **System Settings**.

Step 2 Click the **Redirection URLs** tab.

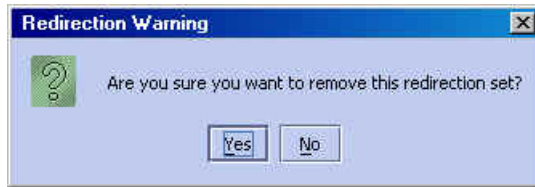
The *System Settings - Redirection URLs Tab* dialog box appears, see *Adding a Set of Redirection URLs* (on page 6-5).

Step 3 Click the redirection group name.

Step 4 Click  (**Remove**).

Step 5 Click **OK**.

A *Redirection Warning* message appears.



Click **Yes**.

The redirection group is removed.

Setting Ongoing Policy Check Parameters

The system classifies network transactions and enforces the appropriate rule when the transaction starts. The system then re-examines the transaction periodically, to see whether different enforcement is required due to change in the subscriber state or change in the service configuration. This examination during the life cycle of the transaction is called Ongoing Policy Check. For example, an ongoing policy check may discover that the subscriber breached her daily volume limit in the middle of a long streaming session, and block the rest of the session. On the other hand, it may discover that the subscriber was moved from the "Limited BW" package to the "Turbo" package in the middle of a long FTP download, and will therefore remove the BW limitation that is enforced on the FTP download.

The **Set the number of seconds between policy checks** text box allows you to supply an interval value for the number of seconds between these check points.



Note The default value is 30 seconds, and usually need not be changed.

To set the Ongoing Policy Check parameter:

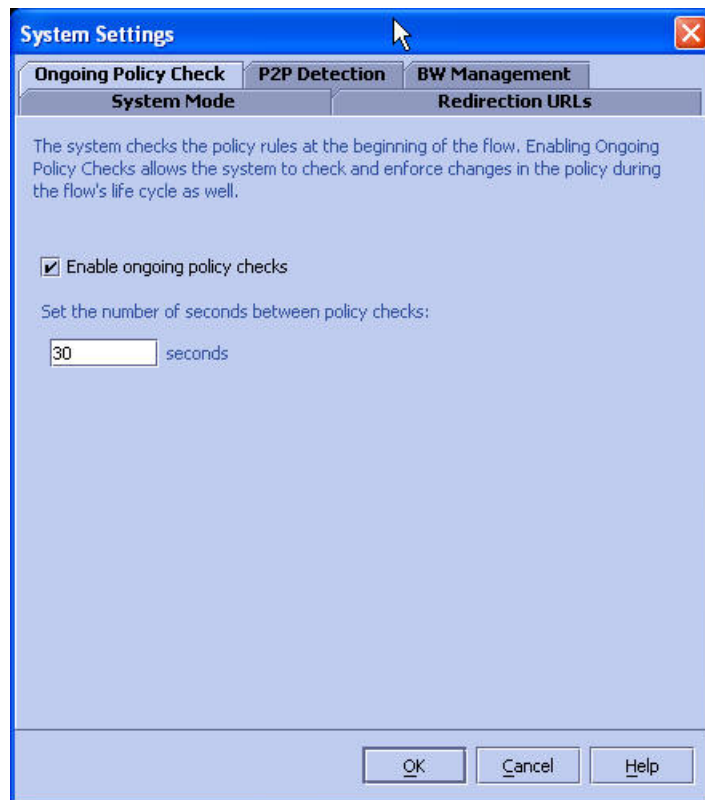
Step 1 From the **Configuration** menu, click **System Settings**.

Step 2 Click the **Ongoing Policy Check** tab.

Understanding the System Settings

The following dialog box appears.

Figure 6-5: System Settings: Ongoing Policy Check Tab



Step 3 (Optional) Select the **Enable ongoing policy checks** check box and type a threshold value in bytes in the *Set the number of seconds between policy checks* text box.

The minimum value is 30 seconds.

The default value is 30 seconds.

Step 4 Click **OK**.

The Ongoing Policy Checks settings are saved.

Setting P2P Detection Parameters

While the system automatically detects P2P traffic on standard P2P port numbers, you can specify a wider range of ports on which P2P detection should take place, using this dialog box.



Note The default range is port 0 to port 65535, and usually does not need to be changed.

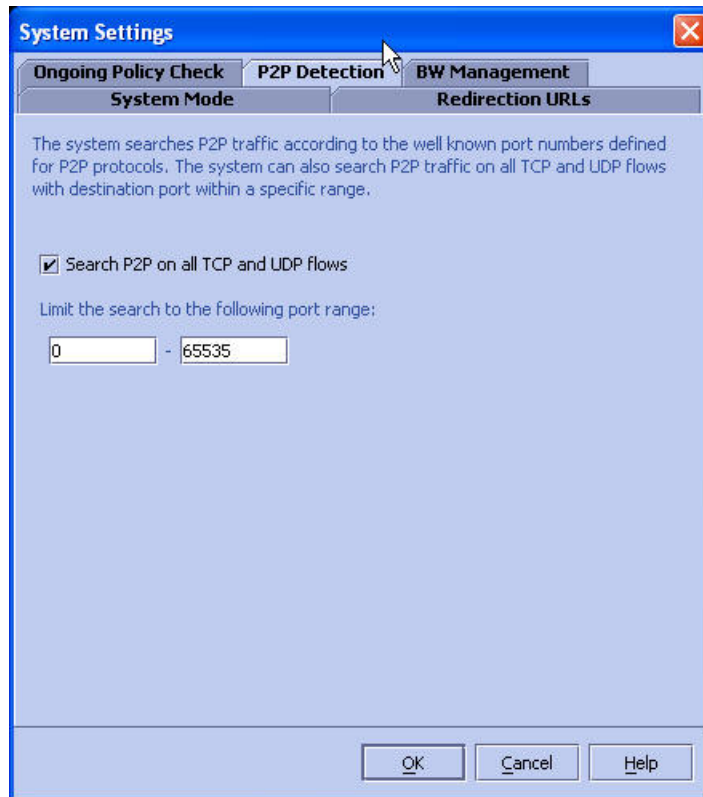
To set the P2P parameters:

Step 1 From the **Configuration** menu, click **System Settings**.

Step 2 Click the **P2P Detection** tab.

The following dialog box appears.

Figure 6-6: System Settings: P2P Detection Tab



Step 3 Check the **Search P2P on all TCP flows** check box.

Step 4 Type a port number range in the *Limit the search to the following port range* boxes

Step 5 Click **OK**.

The P2P settings are saved.

Setting BW Management Parameters

Relative priority is the level of assurance that internal BW controllers get when competing against other internal BW controllers for bandwidth. There are two relative priority options:

- **Global Prioritization Mode:** flows that go through internal BW controllers get their relative priority from the BW controller's assurance level.

- **Subscriber Prioritization Mode** (default): the relative priority of the flow is determined by the relative priority of the subscriber.

To set the BW Management parameters:

Step 1 From the *Configuration* menu, click *System Settings*.

Step 2 Click the *BW Management* tab.

The following dialog box appears.

Step 3 Select "Global Prioritization Mode" or "Subscriber Prioritization Mode".

Step 4 Click *OK*.

The selected BW management parameter is saved.

Dynamic Signature Management

Dynamic signatures are a mechanism through which classification of new protocols can be added to a configuration. This is useful for cases where a new protocol is released and a customer would like to be able to classify its traffic (for example, a new P2P protocol in a P2P-Control solution). Dynamic signatures are provided in special Dynamic Signature Script (DSS) files which can be added to a PQB file using the SCAS BB Console or API. Once a DSS file is loaded into a PQB, the new protocols it supports will be available in the protocol list, and can be added to Services as appropriate, and used when viewing reports. DSS files are periodically released by Cisco or partners in accordance with customer requirements and market needs.

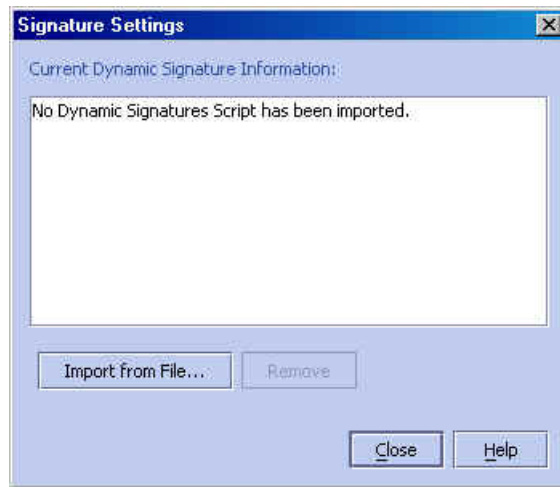
To import a dynamic signature script:

Step 1 Make sure the DSS file (obtained from Cisco or one of its selected partners) is available and that you know the location of the file.

Step 2 From the Configuration menu, select "**Signatures**"

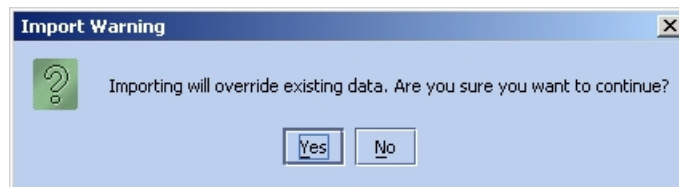
The Signature Settings dialog box opens.

Figure 6-7: Signature settings



Step 3 Click "Import Dynamic Signatures File...".

The system asks for confirmation of importing and overwriting the previous signatures file.



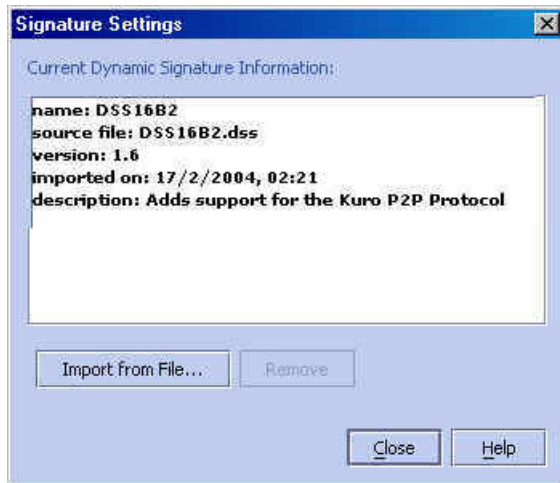
Step 4 Click **Yes**.

A standard file browser opens.

Step 5 Select and open the desired file.

The signature file is imported to the current service configuration.

Figure 6-8: Dynamic Signatures File Imported



The following information is displayed:

- Signature ID
- Source file
- Version
- Import date and time
- Description

To remove a signature file:

Step 1 In the Signature Settings dialog, click **Remove**.

The following warning appears



Step 2 Click **Yes** to confirm

Step 3 The script is removed from the system.

Attack Filtering and Subscriber Notification

Attack filtering is a feature of the SCE Platform, whose aim is to detect attacks that occur in the traffic flowing through the SCE Platform, to report such attacks via management channels, and to handle these attacks by blocking them, if configured to do so. In addition, with **SCAS BB** running in the SCE Platform, a subscriber whose IP address is associated with an attack that was identified can be notified about the attack on-line by the SCE device.

This section describes how to activate subscriber notifications as part of the attack filtering and handling settings. Please refer to the "Attack Filtering" chapter in the SCE User Guide for a complete description of attack detection and handling.

Subscriber Notification on Network Attack

Subscriber notification is a feature for notifying a subscriber in real-time about current attacks involving IP addresses mapped to that subscriber. **SCAS BB** notifies the subscriber about the attack by redirecting HTTP flows originating from the subscriber to a server that supplies information about the attack.

When an attack is identified, if the IP address is detected on the subscriber side and is mapped to a subscriber, **SCAS BB** stores information about the attack. This enables **SCAS BB** to notify the subscriber about the attack on-line by redirecting subsequent HTTP requests of this subscriber to a server that will notify it of the attack.

In addition, when blocking TCP traffic, the system can be configured to not block certain ports in order to make this redirection possible. A list of up to three port numbers can be configured to be un-blockable

Destination URL

Once an attack is identified, HTTP flows of the subscriber are redirect to a configurable destination URL. For example, all HTTP flows can be redirected to a URL such as "http://www.some-isp.net/warning.html", which will warn the subscriber about the attack.

Description Tail

Optionally, a tail with a description of the attack can be added to the destination URL. This tail can be used by the destination server to create a more specific warning. The tail is added as the “query-part” of the URL, and has the following format:

The attack information is formatted in the following way:

```
?ip=<ip>&side=<side>&dir=<dir>&prot=<protocol>&no=<open-
flows>&nd=<suspected-flows>&to=<open-flows-threshold>&td=<suspected-flows-
threshold>&ac=<action>&nh=<handled-flows>
```

The meaning of each field in the tail is described in the following table:

Table 6-1 Description Tail Fields

Field	Indicates
side	<ul style="list-style-type: none"> • s=subscriber • n=network
dir	<ul style="list-style-type: none"> • s=source • d=destination
protocol	<ul style="list-style-type: none"> • TCP • UDP • ICMP • OTHER
open-flows	Number of open flows
suspected flows	Number of attack-suspected flows
open-flows-threshold	Threshold for open flows
suspected-flows-threshold	Threshold for attack-suspected flows
action	<ul style="list-style-type: none"> • B=block • R=report
handled-flows	Number of handled flows since attack began (non-zero only during attack end).

Thus, a URL with a description tail may, for example, look like this:

```
http://www.some-isp.net/warning?ip=80.178.113.222&side=s&dir=s&prot=TCP&no=3
4&nd=4&to=34&td=10&ac=B&nh=100
```

Notification Dismissal

All HTTP flows will continue to be redirected until the notification is dismissed. The notification is dismissed when the subscriber accesses the dismissal URL. By default, the destination URL is also the dismissal URL, so a notification is dismissed once the first redirection takes place. However, it is possible to define a different dismissal URL, so that the user will have to acknowledge the notification.

The dismissal URL includes the URL hostname and the URL path, separated with a colon, in the following format:

```
[*]<hostname>:<path>[*]
```

The optional prefix and suffix wildcards make it possible to define a range of URLs for dismissal. See below on how these wildcards are used to match URLs.

Allowed URL List

When a notification is active, all HTTP flows, except flows to the destination URL and to the dismissal URL, are blocked and redirected to the destination URL. However, subscribers can be permitted to access an additional set of URLs. This can be useful, for example, to let subscribers access additional support information. These URLs should be added to the allowed-URL list.

Each entry in the allowed URL list is made of the URL hostname and the URL path, separated with a colon, in the following format:

```
[*]<hostname>:<path>[*]
```

The hostname may optionally be preceded by a wildcard (*), to match all hostname with the same suffix. Similarly, the path may be followed by a wildcard, to match all paths with common prefix.

For example, the entry:

```
*.some-isp.net:/redirect/*
```

will match all these URLs:

```
www.some-isp.net/redirect/index.html
```

```
support.some-isp.net/redirect/info/warning.asp
```

```
v4.windowsupdate.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8
```



Note The path element must always start with '/'.

Configuring Subscriber Notifications

Subscriber notification is configured, as are other attack filtering settings, using the SCE CLI.



Note Attack Filtering Subscriber Notification settings are not part of the Service Configuration PQB file.

To enable subscriber notification redirection and configure a destination URL:

Step 1 At the SCE# prompt type and press **Enter**:

configure

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**:

The SCE(config if)# prompt appears.

Step 3 Type:

attack-filter subscriber-notification redirect destination-URL <URL>

The destination URL must be complete, including the “http://” prefix, hostname and path. For example, “http://www.some-isp.net/redirect.html” is a valid destination URL, while “www.some-isp.net” is not.

To disable subscriber notification redirection:

Step 1 At the SCE# prompt type and press **Enter**:

configure

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**:

The SCE(config if)# prompt appears.

Step 3 Type:

no attack-filter subscriber-notification redirect destination-URL

This command will also dismiss all the currently active notifications

To enable the attack description tail:

Step 1 At the SCE# prompt type and press **Enter**:

configure

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**:

The SCE(config if)# prompt appears.

Step 3 Type:

```
attack-filter subscriber-notification redirect tail
```

To disable the attack description tail:

Step 1 At the SCE# prompt type and press **Enter**:

```
configure
```

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**:

The SCE(config if)# prompt appears.

Step 3 Type:

```
no attack-filter subscriber-notification redirect tail
```

To set a dismissal URL:

Step 1 At the SCE# prompt type and press **Enter**:

```
configure
```

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**:

The SCE(config if)# prompt appears.

Step 3 Type:

```
attack-filter subscriber-notification redirect dismissal-URL  
[*]<hostname>:<path>[*]
```

To remove the dismissal URL:

Step 1 At the SCE# prompt type and press **Enter:**
configure

The SCE(config)# prompt appears.

Step 2 Type:
interface linecard 0 and press **Enter:**

The SCE(config if)# prompt appears.

Step 3 Type:
no attack-filter subscriber-notification redirect dismissal-URL

The destination URL is used for dismissal instead of the previously configured dismissal URL.

To add a URL to the allowed-URL list:

Step 1 At the SCE# prompt type and press **Enter:**
configure

The SCE(config)# prompt appears.

Step 2 Type:
interface linecard 0 and press **Enter:**

The SCE(config if)# prompt appears.

Step 3 Type:
attack-filter subscriber-notification redirect allowed-host<String Url>

To clear the allowed URL list:

Step 1 At the SCE# prompt type and press **Enter:**
configure

The SCE(config)# prompt appears.

Step 2 Type:

```
interface linecard 0 and press Enter:
```

The SCE(config if)# prompt appears.

Step 3 Type:

```
no attack-filter subscriber-notification redirect allowed-host
```

To monitor the attack filter subscriber notification settings:

Step 1 At the SCE prompt type:

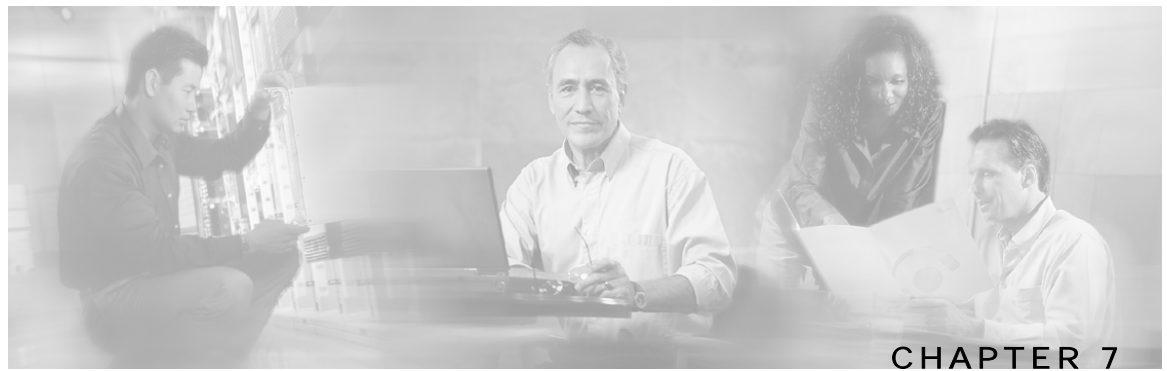
```
show interface LineCard 0 attack-filter subscriber-notification redirect
```

Below is a sample of the output of this CLI command:

```
Attack-Filter Subscriber-Notification Redirection Settings:
Destination URL: http://www.my-isp.net/warning
Tail is used.

Dismissal URL: www.my-isp.net:/acknowledge*

Allowed Hosts:
*.my-isp.net:/softwareupdate/*
*.my-isp.net:/support/*
```

Managing Subscribers

In this chapter we will take a look at subscriber management in Service Control Application Suite for Broadband.

In cases where the Service Control Application Suite for Broadband is used to enforce different policies on different subscribers, and tracks usage on an individual subscriber basis, the smartSUB Manager (SM) component is required to function as middleware software used to bridge between the OSS and the SCE Platform(s). SCE devices use the subscriber information to provide subscriber-aware functionality, per-subscriber reporting and policy enforcement. Subscriber information is stored in the SM database and can then be distributed between multiple devices according to actual subscriber placement.

The SM provides subscriber awareness, mapping network IDs to subscriber IDs. It obtains subscriber information using dedicated integration modules, which integrate with AAA devices like Radius or DHCP servers.

SCAS BB can also operate in subscriber-less mode, where control and link level analysis functions are provided at a global device resolution, and anonymous subscriber mode, where the system dynamically creates "anonymous" subscribers using user-defined IP address ranges as the subscriber-name.

This chapter contains the following sections:

- [Introducing the SCAS BB SM GUI](#) 7-2
- [Working with Individual Subscribers](#) 7-8
- [Working with Subscriber csv Files](#) 7-15
- [Managing Subscribers via Other System Components](#) 7-18

Introducing the SCAS BB SM GUI

The *SCAS BB* SM GUI is a tool that allows you to manage subscribers on the smartSUB Manager. It is useful when the smartSUB Manager holds a static list of subscribers. In addition to importing and exporting the subscriber files, managing subscribers includes operations on individual subscribers, such as adding a new subscriber; editing parameters of an existing subscriber, and removing a subscriber.

Service Control Application Suite for Broadband subscriber management is performed via the *SM Main Window*.



Note The *SCAS BB* SM GUI provides only a small fraction of the operations that can be performed on the smartSUB Manager. For more information, see the smartSUB Manager User Guide.

Accessing the SCAS BB SM GUI

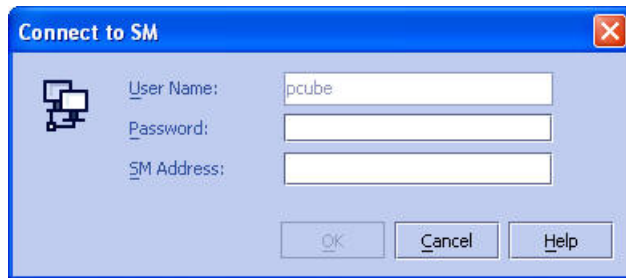
You can access the *SCAS BB* SM GUI from either the **Start** menu or the SCAS BB Console.

To access the *SCAS BB* SM GUI from the Start menu:

Step 1 Select **Start > Programs > Cisco SCAS > SCAS BB x.x.x. > Subscriber Manager**.

The **Connect to SM** dialog opens.

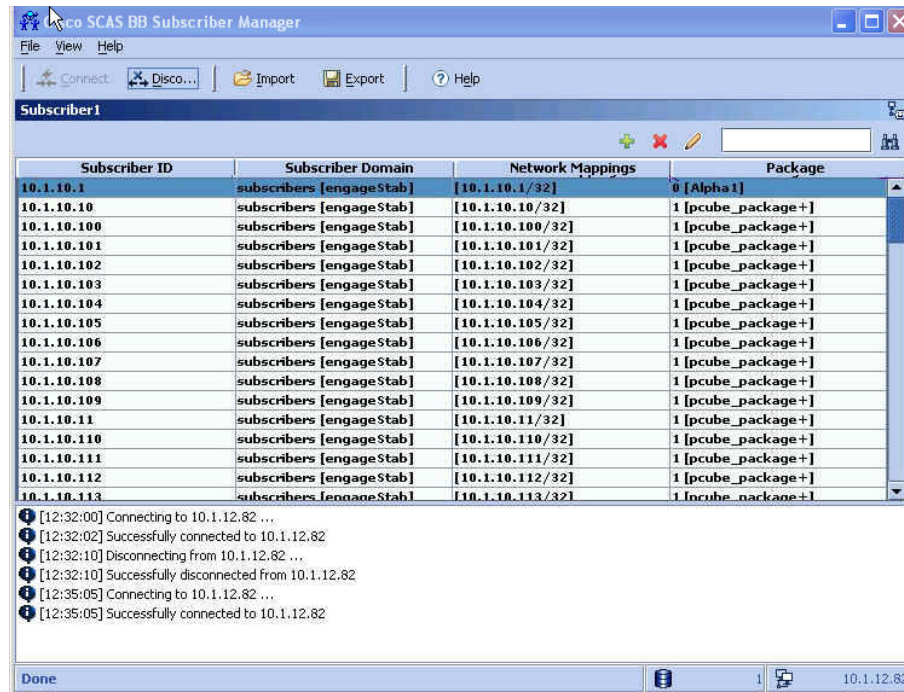
Figure 7-1: SM Connection Dialog



Step 2 Type in the password and IP address of the SM.

The system connects to the SM, and the *SM Main Window* opens.

Figure 7-2: *SM Main Window*

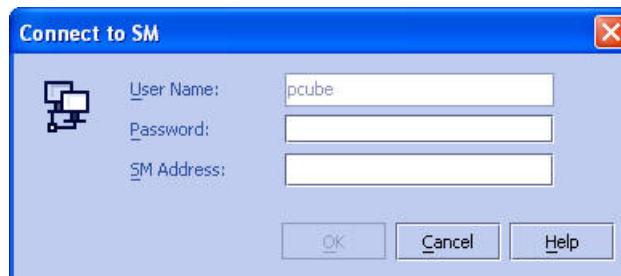


To access the SM GUI from the SCAS BB Console:

Step 1 In the **SCAS BB Console**, select **Tools > Subscriber Manager**.

The **Connect to SM** dialog opens.

Figure 7-3: *SM Connection Dialog*



Step 2 Type in the password and IP address of the SM.

The system connects to the SM, and the *SM Main Window* opens (see *The Subscriber Manager Main Window* ("[The SM GUI Main Window](#)" on page 7-5)).

Connecting and Disconnecting

You must connect to an SM in order to access the SM and open the SM Main Window. However, when you disconnect from the SM, the SM Main Window does not close automatically. This is to enable you to connect to a different SM.

Note in *The Subscriber Manager Main Window* ("[The SM GUI Main Window](#)" on page 7-5) that the toolbar looks as follows:

- **Connect** is disabled, since the system is already connected.
- **Disconnect** is enabled.
- **Import** and **Export** are enabled, since you must be connected to the SM in order to import or export files.

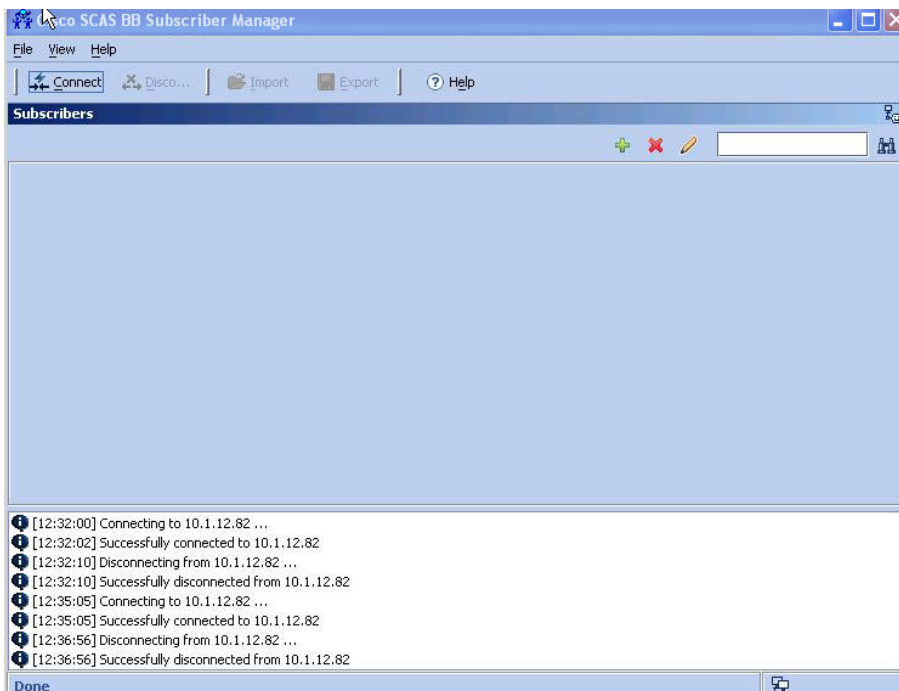
To disconnect from the current SM and reconnect to a different SM:

Step 1 In the SM toolbar, click **Disconnect**.

The *SCAS BB* disconnects from the SM, but the Main Window remains open. Note that now **Connect** is enabled and **Disconnect** is disabled. **Import** and **Export** are disabled, since you must be connected to the SM in order to import or export files.

Note also that the Subscriber Listing section is empty.

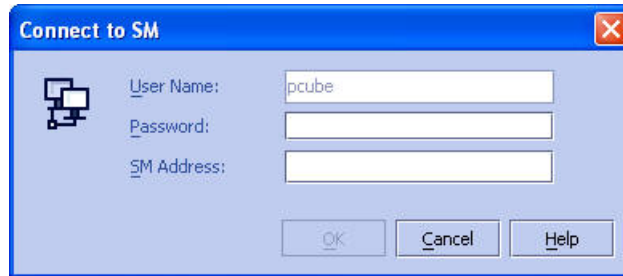
Figure 7-4: SM Main Window (disconnected)



Step 2 In the SM toolbar, click **Connect**.

The **Connect to SM** dialog opens.

Figure 7-5: SM Connection Dialog



Step 3 Type in the password and IP address of the SM.

The system connects to the specified SM, and the *SM Main Window* returns to the connected state, displaying the subscribers in the currently connected SM.

Exiting the SCAS BB SM GUI

To exit the SM GUI:

Step 1 From the Command Menus, select **File > Exit**.

SCAS BB disconnects from the SM and the *SM Main Window* closes.

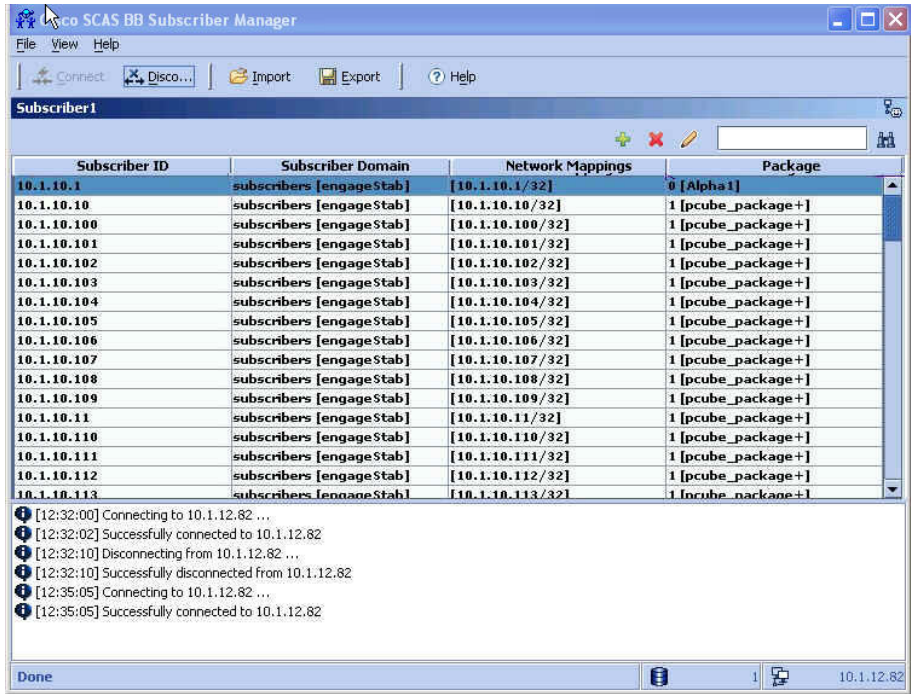
The SM GUI Main Window

The SM GUI Main Window is illustrated below. It contains the following components:

- **Command Menus:** Provide access to the following menus:
 - File Menu
 - View Menu
 - Help Menu
- **SM Toolbar:** Provides easy access to the most commonly used functions
- **Subscriber Listing:** Displays subscribers information
- **Message Band:** Shows system messages and events as they happen

- **Status Bar:** Displays the IP address of the SM






Figure 7-6: SM Main Window





The SM Command Menus and Toolbar

The upper portion of the SM Main Window contains the command menus and the SM toolbar. The following table describes these three command menus and the SM toolbar.

Table 7-1 SM Menu and Toolbar

Menu	Sub-Menu Icon	Description	Comments
File		Connects to an SM.	
		Disconnects from the SM in order to switch to a different SM or before closing the application.	
		Imports subscriber information into the SM from a csv file.	
		Exports subscriber information to a csv file.	
		Closes the application.	Keyboard shortcut: Ctrl+Q
View	View Status	When enabled, displays the Message Band at the bottom of the screen.	

Menu	Sub-Menu Icon	Description	Comments
Help	Help Contents 	Accesses help information by topic.	
			
	License Manager	Allows you to activate <i>SCAS BB</i> Capacity Control and <i>SCAS BB</i> Tiered Control licenses.	
	About	Shows the current version of the Subscriber Manager.	

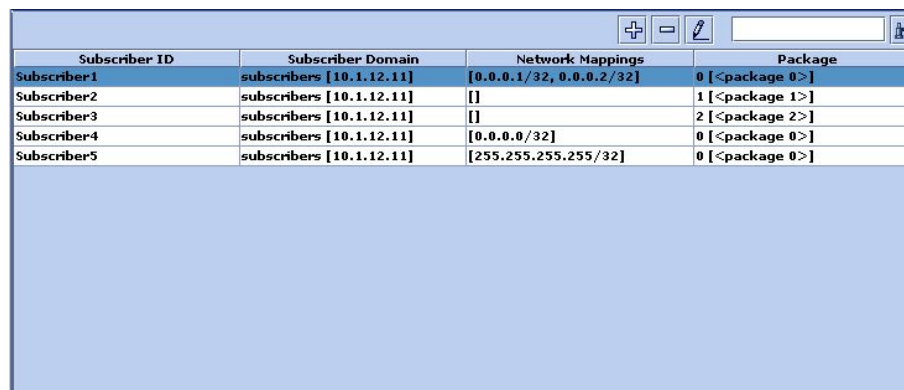
Subscriber Listing

The main component of the SM Main Window is the Subscriber Listing. All subscribers currently introduced into Service Control Application Suite for Broadband are listed in this table. Use this section of the Main Window to manage individual subscribers, adding, editing, or removing single subscribers, or groups.

The Subscriber Listing has the following columns:

- **Subscriber ID:** Name of the subscriber in the system
- **Subscriber Domain:** Domain to which the subscriber is assigned The names of the SCE Platforms that belong to each domain appear in square brackets.
- **Network Mappings:** IP address, range of IP addresses, or VLAN tag mapped to the subscriber
- **Package:** Package assigned to the subscriber.

Figure 7-7: Subscriber Listing



Subscriber ID	Subscriber Domain	Network Mappings	Package
Subscriber1	subscribers [10.1.12.11]	[0.0.0.1/32, 0.0.0.2/32]	0 [<package 0>]
Subscriber2	subscribers [10.1.12.11]	[]	1 [<package 1>]
Subscriber3	subscribers [10.1.12.11]	[]	2 [<package 2>]
Subscriber4	subscribers [10.1.12.11]	[0.0.0.0/32]	0 [<package 0>]
Subscriber5	subscribers [10.1.12.11]	[255.255.255.255/32]	0 [<package 0>]

Message Band

At the bottom of the SM Main Window, the message band reports events as they occur, as well as displaying system messages.

The message band can be hidden by selecting **View> Hide** from the command menus.

Status Bar

The status bar displays the IP address of the SM and the number of subscribers currently in the SM database. For example, in *The Subscriber Manager Main Window* ("[The SM GUI Main Window](#)" on page 7-5), it shows that there are 1031 subscribers.

Working with Individual Subscribers

Once the subscribers have been imported into system, the database may be maintained and updated manually. You can do the following manually:

- Add subscribers
- Edit information for a selected subscriber(s)
- Remove selected subscribers(s)

Locating and Selecting Subscribers

First a word about how to navigate in the Subscriber Listing. For ease of use, the Subscriber Listing incorporates two standard features:

- Find: Search for a specific subscriber
- Multiple Select: Select a range of subscribers or a number of individual subscribers

Finding Subscribers


Use this feature to find a specific subscriber or a group of subscribers according to a name prefix. This is extremely useful when you want to edit the parameters of either a specific subscriber or a group of subscribers.

The following figure shows an enlarged view of the top-right hand of the Subscriber Listing with the **Find** field and icon.



To find a subscriber or group of subscribers:

Step 1 In the *Find* text box, type the prefix to be matched.

Step 2 Click **Find**  (in the right-hand corner)

In the *SM Main Window*, only those subscribers who match the specified prefix are displayed.

Selecting a Group of Subscribers

You can remove or edit a group of subscribers all at one time by selecting a group of subscribers from the subscriber listing. The group may be either of the following:

- A range of contiguous subscribers

- A number of individual (not contiguous) subscribers

The procedure for either of these is standard.

To select a range of subscribers:

-
- Step 1** Select the first subscriber in the range, then hold down the <Shift> key on the keyboard while you click on the last subscriber in the range.

All subscribers in the range are selected.

This function is often combined with the search function. Search to display only the subscribers you want, and select the entire range.

To select a number of non-contiguous subscribers:


-
- Step 1** Hold down the <Ctrl> key on the keyboard while you select all the desired subscribers.

All the subscribers you clicked on are selected, but the intervening ones are not.

Adding a Subscriber

Although subscriber profiles are usually imported from a Radius Server or ISP client list files, it is sometimes necessary to manually add a subscriber to the system.

To add a subscriber:

-
- Step 1** Click  (**Add**) at the top right of the Subscriber Listing.

The *Add a New Subscriber - General Tab* dialog box appears.

Figure 7-8: Add a New Subscriber: General Tab

- Step 2** In the *Subscriber ID* text box, type the subscriber name.
- Step 3** In the *Description* text box, type a meaningful description of the subscriber.
- Step 4** From the *Subscriber Domain* drop-down list, select **Domain** to make sure that the new subscriber is introduced to the proper subscriber domain.
- Step 5** From the *Subscriber Package* drop-down list, select the package that is assigned to this subscriber. The available list depends on the subscriber domain.

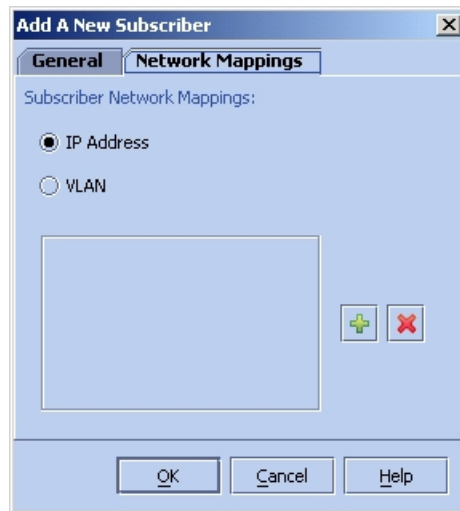


Note If you are not going to define the network mappings click **OK** now to exit.

- Step 6** Click the **Network Mappings** tab.


The following dialog box appears.

Figure 7-9: Add a New Subscriber - Network Mappings Tab



Step 7 Click the appropriate radio button for the type of Network ID:

- **IP Address**
- **VLAN**

Step 8 Click  (**Add**) to add a IP address or VLAN ID.

A white field appears in the network ID list area with the appropriate default network ID.

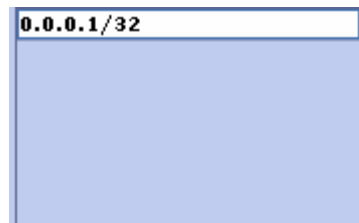


Figure 7-10: Adding an IP Address



Figure 7-11: Adding a VLAN ID

Step 9 Change the default IP address or VLAN tag to the desired value

Step 10 Click **OK** to save the information.

Editing Subscribers

Sometimes you may want to edit parameters of a specific subscriber or a group of subscribers. Use the **Find** feature to perform the search and then edit the subscriber list following the instructions in this section.

To edit a subscriber:

Step 1 Click the **Subscriber ID** of the subscriber whose details you want to change.

Step 2 Click  (**Edit**).

The following dialog box appears. The ID of the selected subscriber appears in the title.

Figure 7-12: Editing Subscribers: General Tab



Step 3 Edit the desired subscriber details:

- *Description:* In the *Description* text box, type a description of the subscriber. This field is for use in identifying the subscriber or entering any other relevant information.
- *Subscriber Domain:* From the drop-down list, select a subscriber domain. The available list depends on the domain you connected with.
- *Subscriber Package:* From the drop-down list, select the package assigned to the subscriber. The available list depends on the domain you connected with.

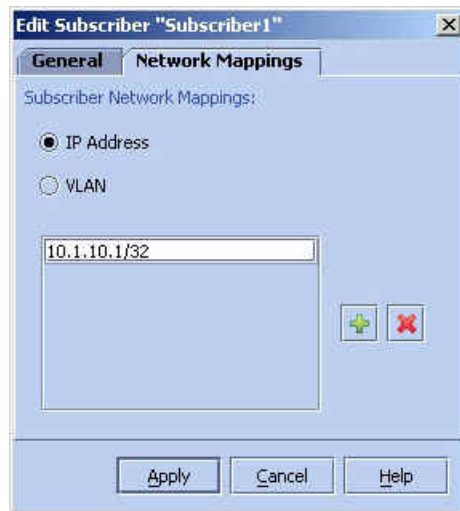
If you do not want to edit the network mappings, skip to step 7.

Step 4 Click the **Network Mappings** tab.

The *Edit Subscriber - Network Mappings tab* dialog box appears.

The system supports either IP addresses or VLAN tags as network identification for subscribers.


Figure 7-13: Edit Subscriber - Network Mappings Tab




- Click the appropriate radio button for the type of Network ID:
 - **IP Address**
 - **VLAN**
- Edit the mapping listing.

You can add a mapping to the list or remove an existing mapping from the current list.

- To add a new mapping to the list:

Click  (**Add**) to add to the desired IP address, IP address range, or VLAN ID. Type the desired network ID (IP address or VLAN tag) in the white field that appears.



- To delete a mapping from the list:
 - Select the entry in the listing that you want to remove.
 - Click  (**Remove**).

Step 5 When you are finished editing the subscriber details, click **Apply** to save the information.

Editing Multiple Subscribers

You may want to assign the same package and/or domain to many subscribers. It is extremely time-consuming to perform such a task for only one subscriber at a time. Use this feature to assign a package and/or domain to a group of subscribers.

To edit details for a group of subscribers:

Step 1 Select the subscribers (see *Selecting a Group of Subscribers* (on page 7-8))

Step 2 Click  (**Edit**).

The *Edit Multiple Subscribers* dialog box appears.

Figure 7-14: Edit Multiple Subscribers



This is exactly the same as the regular *Edit Subscribers* dialog box, with the following exceptions:

- The **Subscriber ID** field is disabled, and shows the name of the last subscriber you added to the group.
- The *Network Mapping* tab is disabled

Step 3 Select the domain and/or package in the same manner you do for a single subscriber.

Step 4 Click **Apply**.


The selected package and/or subscriber domain is assigned to all the selected subscribers

Removing Subscribers

Use this procedure to remove subscribers from the database.

To remove a subscriber from the database:

Step 1 Select a single subscriber or a group of subscribers (see *Selecting a Group of Subscribers* (on page 7-8)).

Step 2 At the top right-hand section of the Subscriber Listing, click  (**Remove**).

The system asks for confirmation before removing the selected subscriber(s):

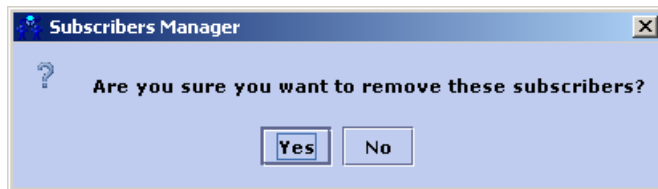


Figure 7-15: Subscribers Manager – Remove Message

Step 3 Click **Yes** to confirm.

The selected subscriber(s) is removed from the list.

Working with Subscriber csv Files

As noted above, due to the large number of subscribers that must be introduced into the system, it is not feasible to enter the subscriber information manually. The subscriber information is usually generated by the Radius server, or some similar source, and imported into the SM.

It is also possible to export updated subscriber information to a *csv* file.

The *csv* file format is described in *csv File Formats* (csv File Formats "[Subscriber CSV File Formats](#)" on page 7-24).

Importing Subscriber Files

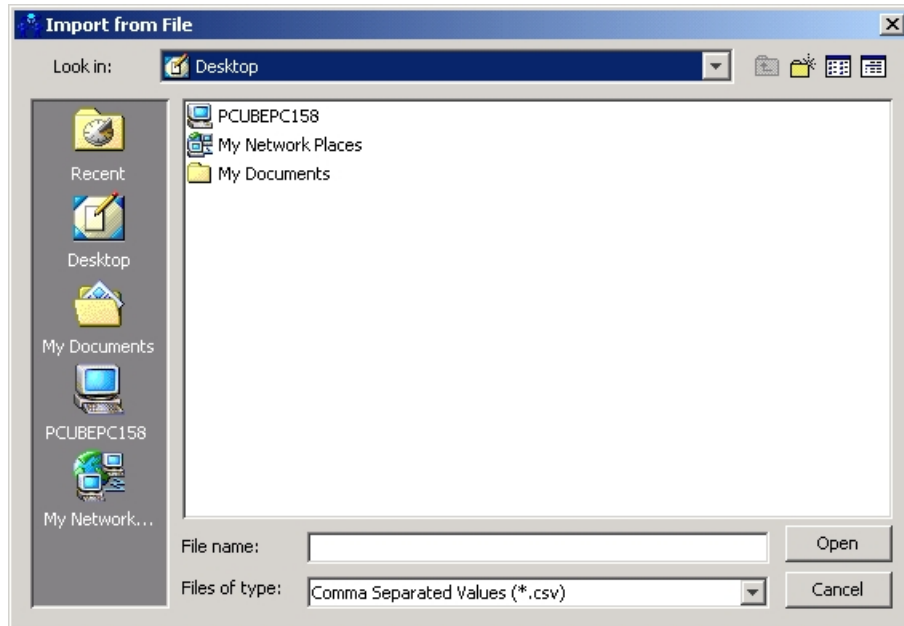
The subscriber information must be in the form of a *csv* file. This file is imported into the SM, which constructs the SM database from the information. A listing of subscribers then appears in the Subscriber Listing as described in *Subscriber Listing* (on page 7-7).

To import a subscriber file:

Step 1 In the SM toolbar, click **Import**.

The *Import from File* dialog box opens..

Figure 7-16: *Import from File*

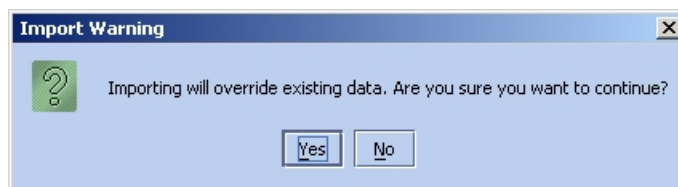


Step 2 The *Import from File* dialog box is a standard file browser. Specify the file you want to open by doing either of the following:

- In the **File name** field, type the path/filename of the desired file.
- Browse to find and select the desired file.

Step 3 Click **Open**.

Since existing data will be lost when the file is imported, the system asks for confirmation.



Step 4 Click **Yes**.

The selected file is imported into the SM.

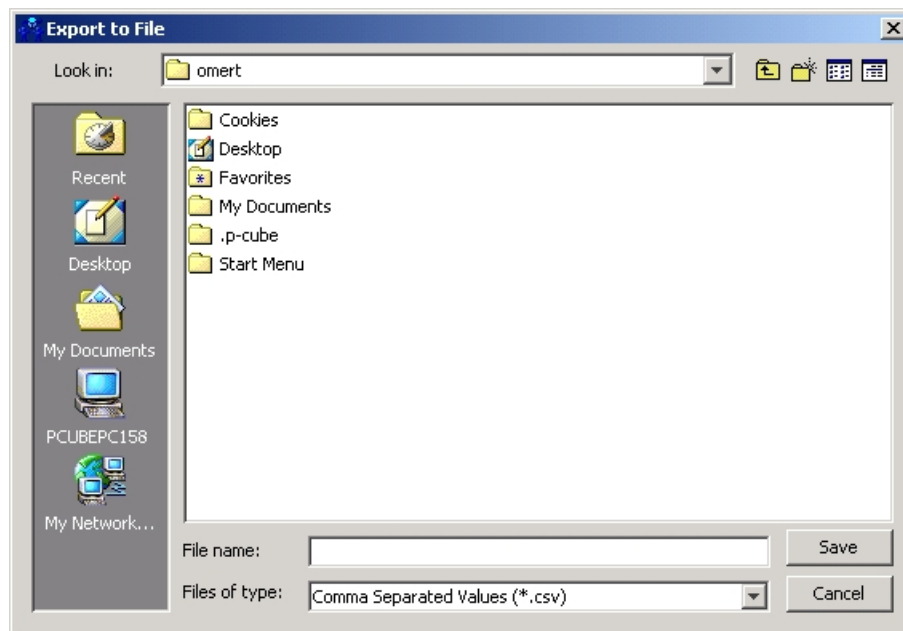
Exporting Subscriber Files

If you have changed the SM database, you may wish to export the updated subscriber information to a csv file.

To export subscriber information to a csv file:

-
- Step 1** In the SM toolbar, click **Export**.
The *Export to File* dialog box opens..

Figure 7-17: *Export to File*



- Step 2** The *Export to File* dialog box is a standard file browser. Specify the file you want to export to by doing either of the following:

- In the **File name** field, type the path/filename of the desired file.
- Browse to find and select the desired file.

- Step 3** Click **Save**.
-

Managing Subscribers via Other System Components

Other components of the Service Control solution offer alternatives for subscriber management. In addition to working directly via the smartSUB Manager, as opposed to accessing the SM from the SCAS BB Console, the SCE Platform itself has a wide range of subscriber-related functions.

The purpose of this section is to acquaint the user with these options, with emphasis on Service Control Application Suite for Broadband-specific subscriber management options. For in-depth explanations, refer to the appropriate Service Control documentation

Anonymous-Subscriber Mode

An anonymous subscriber is one with an internally generated name, generated automatically by the SCE device according to an anonymous subscriber group specification. An anonymous subscriber is always mapped to a single IP address. The actual identity of the customer(s) is unknown to the system. (See *Subscribers and Subscriber-Modes* (on page 2-3))

An anonymous group is a specified IP range, possibly assigned a subscriber template. When an anonymous group is configured, the SCE Platform generates anonymous subscribers for that group when it detects traffic with an IP address that is in the specified IP range. If a subscriber template has been assigned to the group, the anonymous subscribers generated have properties as defined by that template. If no subscriber template has been assigned, the default template is used.

Anonymous subscriber groups and subscriber templates are managed using the SCE Platform Command Line Interface (CLI). CLI commands can be entered via a telnet session. For more information, refer to the *SCE 1000/SCE 2000 User Guide*.

Use the following commands to import anonymous subscriber groups and subscriber templates from csv files and to export subscriber data to these files:



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the SCE(config if)# prompt displayed.

- `subscriber anonymous-group import csv-file`
- `subscriber anonymous-group export csv-file`
- `subscriber template import csv-file`
- `subscriber template export csv-file`

Use the following commands to remove anonymous groups or subscriber templates from the system.



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the SCE(config if)# prompt displayed.

- `no subscriber anonymous-group [all] [name "groupname"]`
- `clear subscriber anonymous`
- `default subscriber template all`

Use the following commands to display anonymous subscriber information:

- `show interface linecard 0 subscriber templates [index]`
- `show interface linecard 0 subscriber anonymous-group [all] [name "groupname"]`
- `show interface linecard 0 subscriber amount anonymous [name "groupname"]`
- `show interface linecard 0 subscriber anonymous [name "groupname"]`

Subscriber-Aware Mode

In subscriber-aware mode, each subscriber is a specific customer with an externally generated name. This externally generated name allows the subscriber to be mapped to more than one IP address and still be identified. Each traffic session (single IP flow, or a group of related IP flows) processed by the SCE device is assigned to a recognized subscriber on the basis of the configured subscriber mappings.

There are three options for introducing and managing these subscribers:

- The *SCAS BB* SM GUI: As described in this chapter
- SCE Platform CLI
- smartSUB Manager Command Line Utilities (CLU)

SCE Platform Subscriber CLI

Use the following commands to import subscriber data from *csv* files and to export subscriber data to these files:



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the `SCE(config if)#` prompt displayed.

- `subscriber import csv-file`
- `subscriber export csv-file`

Use the following command to remove subscribers from the system.



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the `SCE(config if)#` prompt displayed.

- `no subscriber [all] [name "subscriber-name"]`

Use the following commands to display subscribers meeting various criteria:

- `show interface linecard 0 subscriber [amount] [prefix "prefix"] [property "propertyname" equals|greater-than|less-than "property-val"]`
- `show interface linecard 0 subscriber [amount] prefix "prefix"`

- `show interface linecard 0 subscriber [amount] suffix "suffix"`
- `show interface linecard 0 subscriber mapping IP "iprange"`
- `show interface linecard 0 subscriber [amount] mapping intersecting IP "iprange"`
- `show interface linecard 0 subscriber mapping VLANid "vlanid"`

Use the following commands to display information about a specific subscriber:

- `show interface linecard 0 subscriber properties`
- `show interface linecard 0 subscriber name "name"`
- `show interface linecard 0 subscriber name "name" mappings`
- `show interface linecard 0 subscriber name "name" counters`
- `show interface linecard 0 subscriber name "name" properties`

smartSUB Manager CLU

Use the **p3subs** smartSUB Manager utility to manage subscribers. You can add or remove subscribers. You can also manage subscriber properties and mappings with this utility.

For more information, refer to the *smartSUB Manager User Guide*.

To manage subscribers:

- ➔ From the Solaris shell prompt, type a command having the following general format:

```
p3subs <operation> --subscriber=<Subscriber-Name> [--ip=<IP-
address>]
[--property=<property-name=value>] [--domain=<domain-name>] [--
overwrite]
```

The following table lists the **p3subs** operations relevant to managing subscribers.

Table 7-2 p3subs Subscriber Operations

Operation	Description
--add	Adds a subscriber or replaces the existing subscriber configuration.
--set	Updates mappings and/or properties for specified subscriber.
--remove	Removes the specified subscriber.
--show	Displays information for specified subscriber.

Managing Real-time Subscriber Usage RDRs

The real-time subscriber usage RDRs report the network activity of a single subscriber per service per metric, in real-time. You must enable the generation of these subscriber usage RDRs for each subscriber that you want to monitor.

The "**monitor**" subscriber property indicates whether the generation of real-time subscriber usage RDRs is enabled for the subscriber, as follows:

- Enabled: **monitor** = 1
- Disabled: **monitor** = 0 (default)

You can modify this property for the desired subscriber(s) using either the smartSUB Manager CLU or the SCE Platform CLI.

Managing Subscriber Monitoring via the SM

You can enable/disable the generation of the real-time subscriber usage RDRs using the SM **p3subs** utility. You can also create a file that will process a batch of subscribers. For more information, see the *smartSUB Manager User Guide*.

To enable subscriber monitoring for subscriber "Smith":

Step 1 Type the following command at the command line prompt:

```
sm/server/bin/p3subs --set --subscriber Smith --property monitor=1
```

To disable subscriber monitoring for subscriber "Smith":

Step 1 Type the following command at the command line prompt:

```
sm/server/bin/p3subs --set --subscriber Smith --property monitor=0
```

To enable subscriber monitoring for a group of subscribers:

Step 1 Create a text file (named *monitor.txt* in this example) containing the sequence of CLU invocations. The file would look something like this:

```
p3subs --set --subscriber Jerry --property monitor=1  
  
p3subs --set --subscriber George --property monitor=1  
  
p3subs --set --subscriber Elaine --property monitor=1  
  
p3subs --set --subscriber Kramer --property monitor=1  
  
p3subs --set --subscriber Newman --property monitor=1
```

Step 2 Type the following command at the command line prompt:

```
sm/server/bin/p3batch -f monitor.txt
```

You can check to see whether subscriber monitoring is enabled for a specific subscriber.

To see whether subscriber monitoring is enabled for subscriber "Smith":

Step 1 Type the following command at the command line prompt:

```
sm/server/bin/p3subs --show-property --subscriber Smith --property monitor
```

Managing Subscriber Monitoring via the SCE Platform

You can also enable/disable the generation of the real-time subscriber usage RDRs using the SCE Platform. For more information, see the *SCE 1000/SCE 2000 User Guide*.

(The prompt is included in these examples to illustrate how it changes. You must see the **SCE(config if)#** prompt in order to invoke the actual subscriber command.)

To enable subscriber monitoring for subscriber "Smith":

Step 1 Type the following sequence of commands at the command line prompt:

```
SCE# configure
SCE(config)# interface LineCard 0
SCE(config if)# subscriber name Smith property monitor value 1
```

To disable subscriber monitoring for subscriber "Smith":

Step 1 Type the following sequence of commands command at the command line prompt:

```
SCE# configure
SCE(config)#interface LineCard 0
SCE(config if)# subscriber name Smith property monitor value 0
```

To enable subscriber monitoring for a group of subscribers:

Step 1 Create a text file (named *monitor.txt* in this example) containing the sequence of CLI invocations, including the commands to access the appropriate CLI mode. The file would look something like this:

```
configure
```

```
interface LineCard 0

subscriber name Jerry property monitor value 1

subscriber name George property monitor value 1

subscriber name Elaine property monitor value 1

subscriber name Kramer property monitor value 1

subscriber name Newman property monitor value 1
```

Step 2 Type the following command at the command line prompt:

```
SCE# script run monitor.txt
```

You can check to see whether subscriber monitoring is enabled for a specific subscriber. To see whether subscriber monitoring is enabled for subscriber "Smith":

Step 1 Type the following command at the command line prompt:

```
SCE# show interface LineCard 0 subscriber name Smith properties
```

The properties are displayed. **monitor** is the relevant parameter.

```
Subscriber smith properties:
subscriberPackage=0
monitor=1
Subscriber 'smith' read-only properties
```

Managing csv Files

Use the **p3subsdb** smartSUB Manager utility to import and export subscriber *csv* files. You can import subscriber information for a group of subscribers from a *csv* file into the SM database. You can also export subscriber information from the SM database to a *csv* file.

For more information, refer to the *smartSUB User Guide*.

To import *csv* files:

Step 1 From the Solaris shell prompt, type a command having the following general format:

```
p3subsdb --import <filename>
```

To export *csv* files:

Step 1 From the Solaris shell prompt, type a command having the following general format:

```
p3subsdb --export <filename>
```

EXAMPLE:

The following example shows how to export subscribers with filtering options to a specified CSV file.

```
p3subsdb --export --prefix=a --output=silverSubscriberFile.csv
```

Subscriber CSV File Formats

Following are file formats for various subscriber *csv* files referred to in this chapter. For more information regarding *csv* file formats, see the *SCE 1000/SCE 2000 User Guides* and the *smartSUB User Guide*.

Import/Export file: mappings field format

The *mappings* field can be one or more of these values delimited by colon (':') or semicolon (;):

- A single IP address in dotted notation (xx.xx.xx.xx):
- An IP address range in dotted notation (xx.xx.xx.xx/mask): implies a range of IP addresses
- A single VLAN (xx): an integer in decimal notation in the range of 0-4095
- A VLAN range in ('xx-yy') format: Implies a range of VLAN tags.

**Note**

Specifying VLAN and IP Mappings together in the same line is not allowed.

EXAMPLES:

- Multiple IP mappings: **10.1.1.0/24;10.1.2.238**
- Multiple VLAN mappings: **450:896-907**

SCE Subscriber files

Following is a sample *csv* file for use with SCE CLI.

```
# CSV line format: subscriber-id, mappings, package-id
JerryS,80.179.152.159;80.179.152.179,0
ElainB,194.90.12.2,3
```

SM Subscriber files

Following is a sample *csv* file for use with SM CLU.

If no domain is specified, the default domain (subscribers) is assigned.

```
# CSV line format: subscriber-id, domain, mappings, package-id
JerryS,subscribers,80.179.152.159,0
ElainB,subscribers,194.90.12.2,3
```


Anonymous Group csv files

Anonymous Group *csv* files have a fixed format. All lines have the same structure, as described below:

- Anonymous-group-name, IP-range[, subscriber-template-number].

If no subscriber-template-number is specified, then the anonymous subscribers of that group will use the default template (#0), which cannot be changed by template import operations.

Initially, 32 templates are preconfigured, one for each package ID.

Following is an example of an anonymous group *csv* file:

```
# CSV line format: anonymous-group-name, IP-range, subscriber-template-  
number  
  
group1, 10.1.0.0/16;10.5.0.0/16, 2  
group2, 176.23.34.0/24, 3  
group3, 10.7.0.0/16
```




Generating Reports

The SCAS Reporter is the Service Control Application Suite for Broadband tool that allows you to produce reports based on the traffic analysis performed by the SCE Platform. The information is sent to the Collection Manager, which can generate a comprehensive range of reports, including global monitoring, subscriber monitoring, traffic analysis and P2P reports.

The **Reporter** is available only in a deployment with a Collection Manager.

Generating a report can be divided into two broad steps:

-
- Step 1** Create the report definition using the *Reports Wizard*
 - Step 2** Edit, print, and/or export the report using the *Reporter Main Screen*
-

This chapter contains the following sections:

- [Introducing the SCAS Reporter](#) 8-1
- [Defining the Report](#) 8-6
- [Working with Reports](#) 8-19

Introducing the SCAS Reporter

The available reports can be presented using a variety of graphs (for example, line or pie) or in table form. The graphs can be edited to produce any look desired, and then printed and/or exported to a file.

SCAS Reporter consists of two main components:

- *Reports Wizard*: Used to define and generate the report, selecting and editing the appropriate report template.
- *Reporter Main Screen*: Used to edit the appearance of the report, and to print and/or export the report.

Accessing the SCAS Reporter

You can access the **SCAS Reporter** from either the **Start** menu or the **SCAS BB** console. **SCAS BB** must connect to the Collection Manager in order to open the **SCAS Reporter**.

To access the SCAS Reporter:


Step 1 Choose the most convenient of the following two options:

- To access the SCAS Reporter from the **Start** menu:
Select **Start > Programs > Cisco SCAS > SCAS Reporter x.x.x > Reporter**.
- To access the SCAS Reporter from within the SCAS BB Console:
Select **Tools > SCAS Reporter**

The **Connect to Collection Manager** dialog opens.

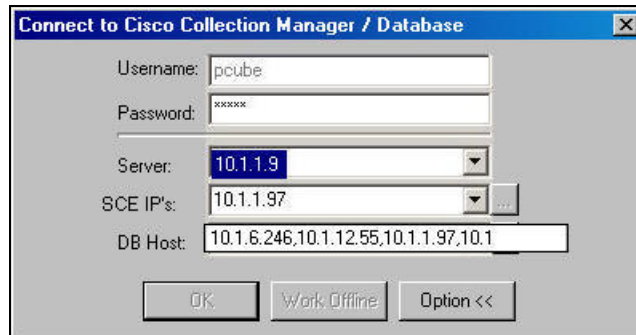
Figure 8-1: Logging on to the Reporter

Step 2 Type in the password and Server IP address.

You can click the  button next to the **SCE IP's** field to display a listing of the IP addresses of all SCE devices that were or are connected to the Collection Manager. All options presented in the *Reporter Wizard* (available packages, services, etc.) are determined by the Service Configuration currently applied to the first SCE Platform in the list. However, the reports are generated on the basis of data from all the SCE devices in the list. Make sure the desired SCE Platform is at the beginning of the list.

If you want reports for one SCE Platform only, delete the other IP addresses from the list.

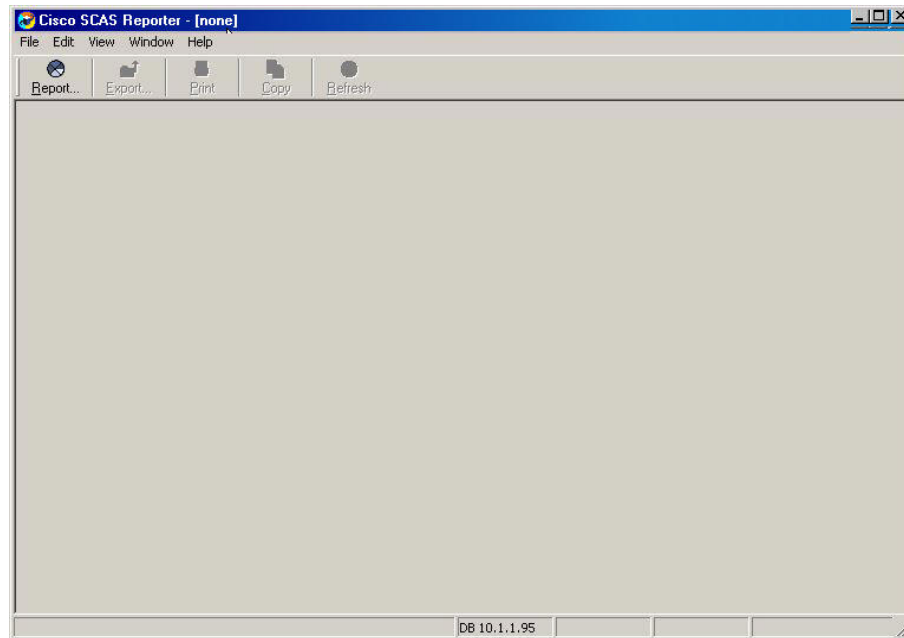
The **DB Host** field displays the same IP address as the **Server** field.



Step 3 Click **OK**.

The system connects to the Collection Manager, and the *Reporter Main Screen* opens.

Figure 8-2: Reporter Main Screen



Exiting the Reporter

To exit the **Reporter**:

Step 1 From the Command Menus, select **File > Exit**.

SCAS BB disconnects from the Collection Manager and the *Reporter Main Screen* closes.

The Reporter Main Screen

The *Reporter Main Screen* displays the reports, and is used to edit the look and feel of the generated report. It is illustrated in the following figure.

The *Reporter Main Screen* contains the following components:

- Command Menus: Provide access to the following menus:
 - File Menu
 - Edit Menu
 - View Menu
 - Window Menu
 - Help Menu
- Reporter Toolbar: Provides easy access to the most commonly used functions
- Report Display Area: Displays report(s)

Figure 8-3: Reporter Main Screen

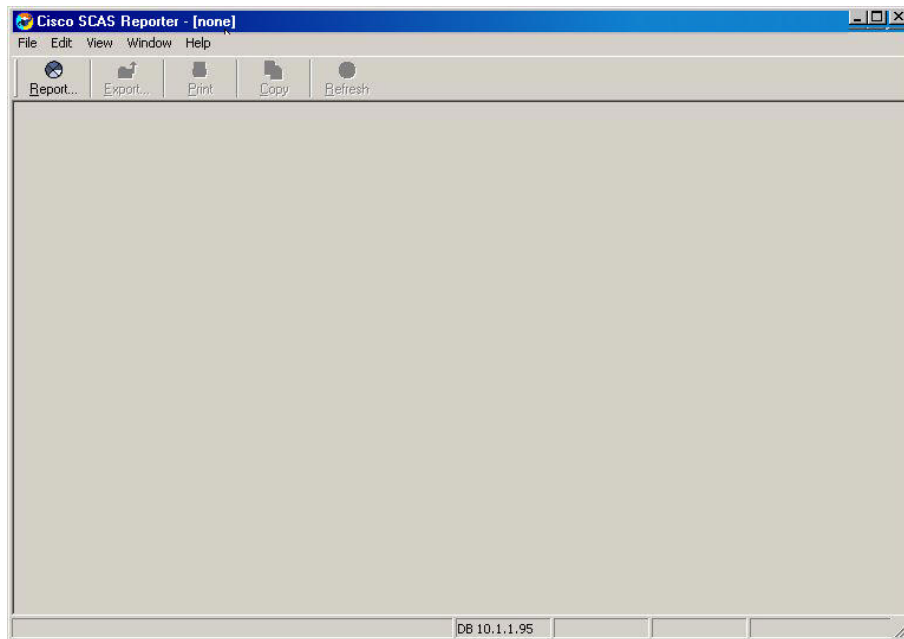







Table 8-1 SCAS Reporter Menu and Toolbar

Menu	Sub-Menu	Toolbar Icon	Description	Comments
File	Report		Opens the <i>Report Wizard</i> .	Keyboard shortcut Ctrl+N
	Export		Saves the report to a file.	

Menu	Sub-Menu	Toolbar Icon	Description	Comments
	Print		Sends the report to a printer.	Keyboard shortcut Ctrl+P
	Print Preview		Displays the report in print layout.	
	Print Setup		Allows you to set the printer settings.	
	Exit		Closes the SCAS Reporter .	Keyboard shortcut Ctrl+Q
Edit	Undo		Not available.	
	Copy		Not available.	
	Find		Opens the <i>Find</i> dialog box.	Keyboard shortcut Ctrl+F
View	Toolbar		View or hide the toolbar.	Default: enabled
	Status Bar		View or hide the Status bar.	Default: enabled
	Refresh		Refreshes the current graph by polling the database for new values.	Keyboard shortcut Ctrl+R
Window	Tile		These three options allow you to organize the reports open on your desktop.	
	Cascade			
	Arrange Icons			
Help	About		Current version of SCAS Reporter .	

The Reports Wizard

The second component of the **SCAS Reporter** is the *Reports Wizard*. This window is used to define the parameters for generating the report.

To open the Reports Wizard:

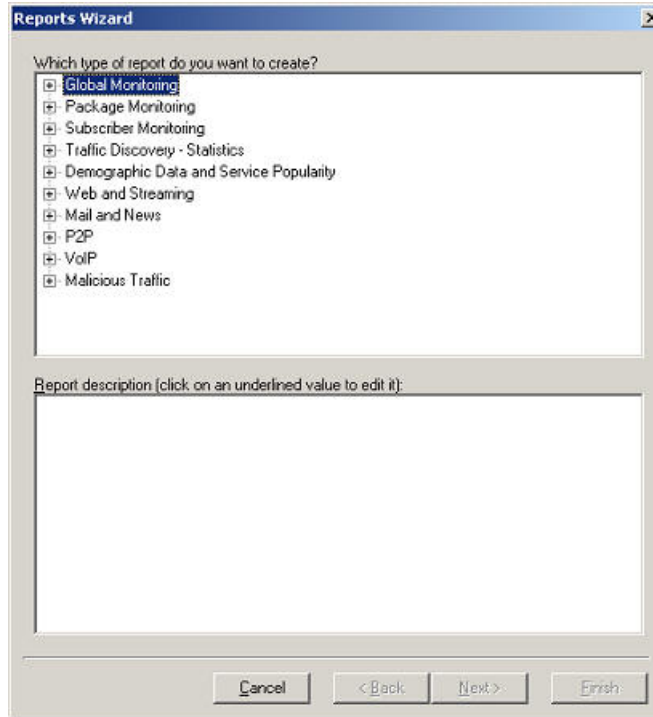
Step 1 From the **File** menu, click **Report**

-or-

Click the **Report** icon in the toolbar.

The *Reports Wizard* appears.

Figure 8-4: The Reports Wizard



The *Reports Wizard* buttons are defined in the following table.

Table 8-2 Reports Wizard Buttons

Button	Description
New	Creates a new report definition
Copy	Makes a duplicate of the selected report definition
Rename	Renames the selected report definition
Modify	Opens the selected report definition for editing
Delete	Deletes the selected report definition
Report	Generates the selected report
Close	Closes the <i>Reports Wizard</i>
Help	Not currently available.

Defining the Report

The SCAS Reporter supplies templates for a wide variety of reports, such as:

- Global or package hourly or daily volume per service
- Top server/clients/protocols/web hosts/email senders/newsgroups

- Subscriber hourly or daily volume per service
- Top P2P consumers/uploaders/downloaders/protocols
- Global, package, or subscriber bandwidth per service

The template presents all the parameters of the report, both required and optional, so that you can select the desired values. For example, if you want to see global bandwidth per service, the template will prompt you to specify the desired service(s), traffic direction, and time frame (either start/end time or previous number of hours). For a complete description of all templates, see *SCAS Reporter Templates* (on page [A-1](#)).

The report is defined in the *Reports Wizard*. When the report is generated from the report definition, it appears in the *Reporter Main Screen*, and the *Reports Wizard* then closes.

Creating a New Report Definition

When you create a report, you select the desired report template and then specify values for the various report parameters.

The precise procedure for defining a report varies, depending on the report selected and the number of changes made to the basic report description. Not all reports present the "iteration values" screen (step 4). Also, the exact steps in selecting specific values for conditions may vary. In addition, you may sometimes need to move back and forth between two stages of the definition, using the **Next** and **Back** buttons. Or you could immediately edit the underlined values in the report description as soon as it appears (step 3), rather than after the report description is completed. Therefore, the following example is intended only as a general guide to the process of creating a new report definition.

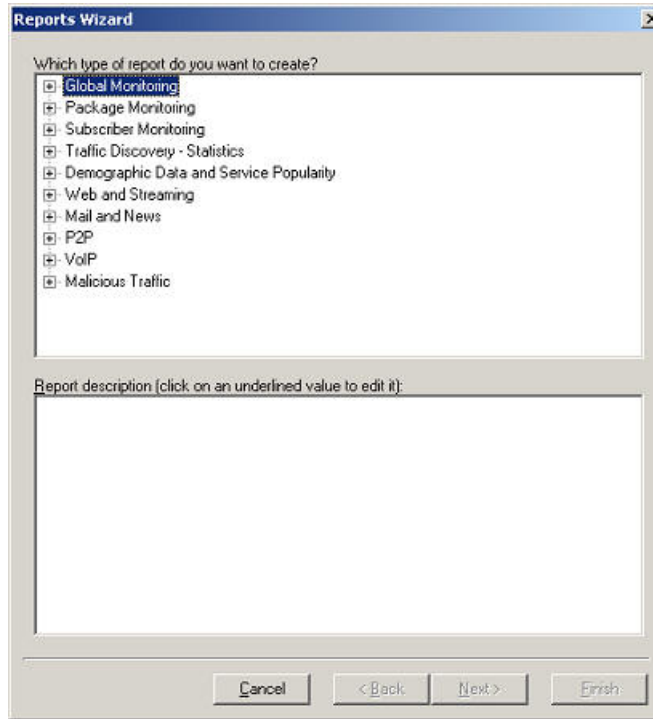
The following example illustrates defining the "Global Bandwidth per service" report.

To create a new report:

Step 1 From the **Reports Wizard**, click **New**.

The following dialog box appears.

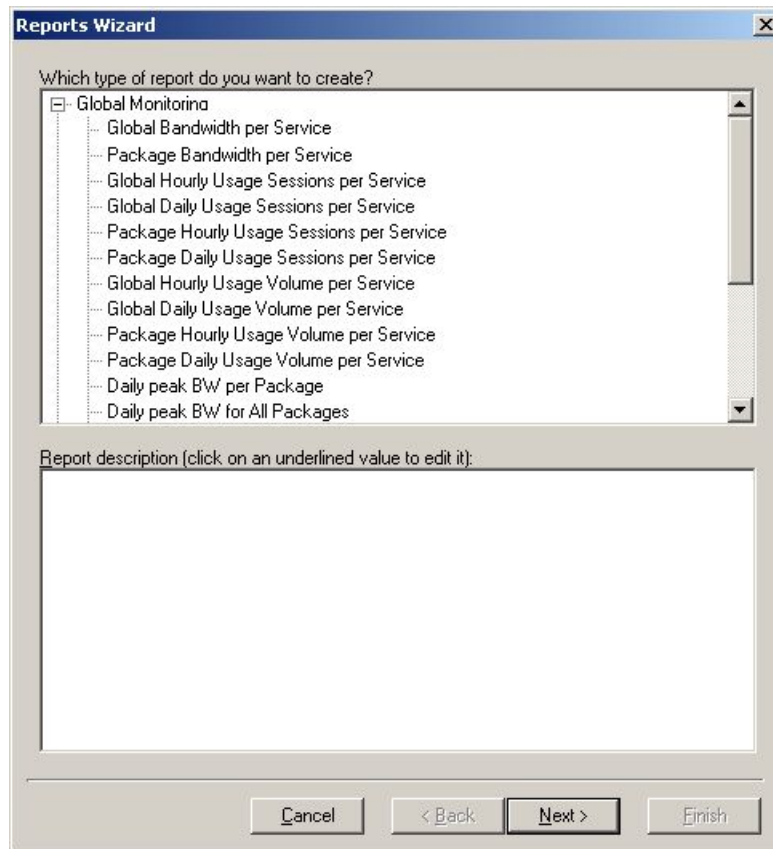
Figure 8-5: Reports Wizard: New



Step 2 Click a report group name (in our example, "Global Monitoring").

The following dialog box appears displaying a list for the selected group.

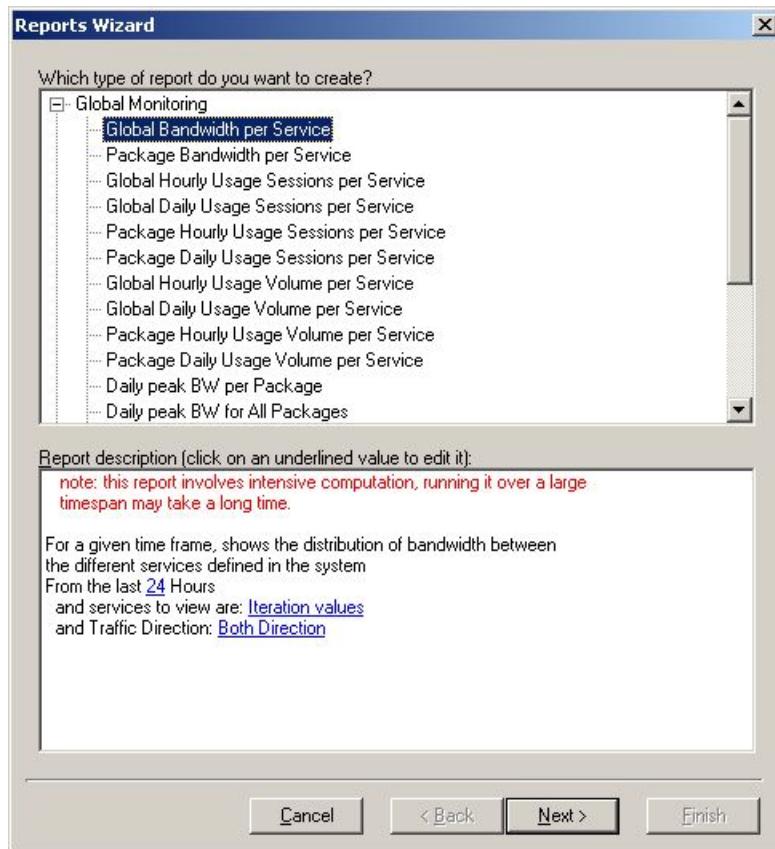
Figure 8-6: Reports Wizard: Displaying the Available Reports



Step 3 Select the desired report (Global Bandwidth per Service).

The description of the selected report appears in the bottom pane titled **Report Description**.

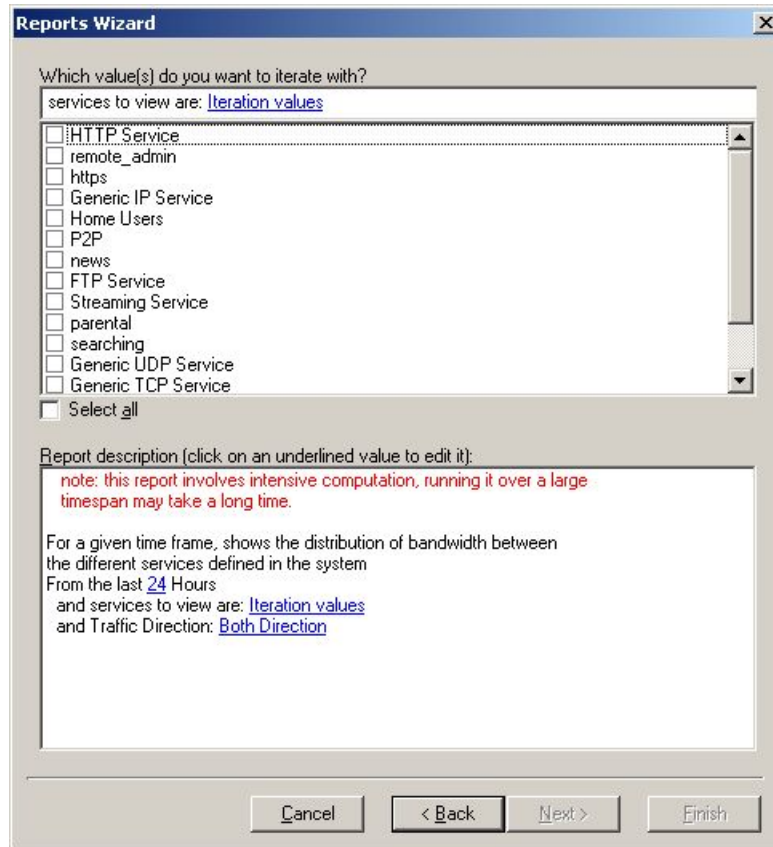
Figure 8-7: Reports Wizard: Report Description



Step 4 Click **Next**.

The next dialog box appears, displaying a list iteration values in the upper pane. Since this report is produced "per service", you must choose which services to include.

Figure 8-8: Reports Wizard: Iteration Value Options

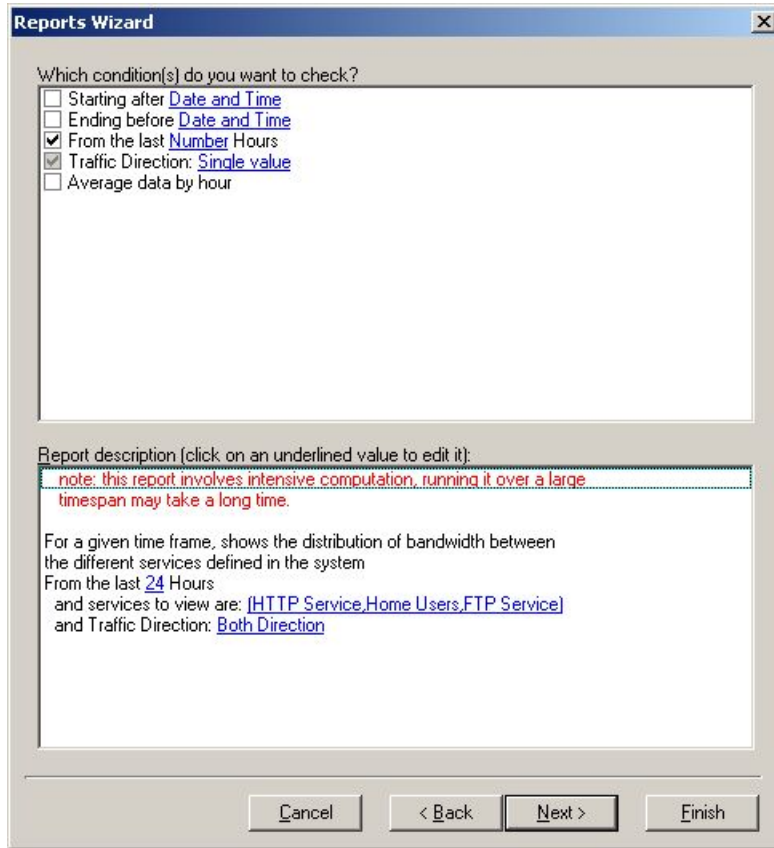


Step 5 Select the iteration values (desired services).

If you want to include all services, check **Select all**.

The selected services appear in the report description (**services to view are**).

Figure 8-9: Reports Wizard: Updated Report Description



Step 6 Click **Next**.

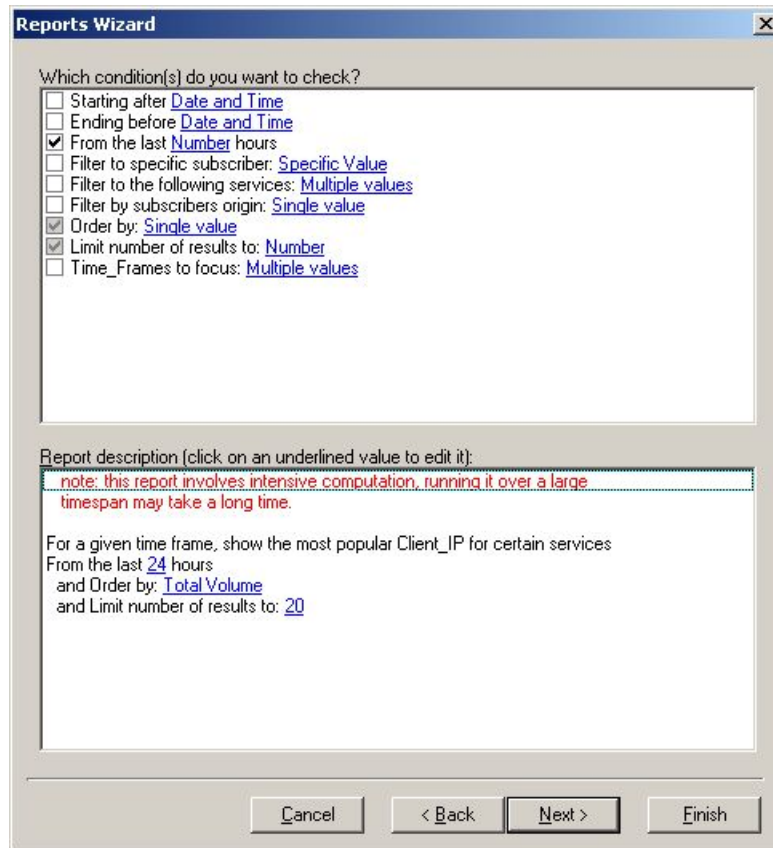
The next dialog box appears, displaying a list of conditions in the upper pane. These represent the report parameters. For every report template, there is a different selection of conditions.

Note the following:

- Grayed boxes indicate required conditions. You cannot clear these conditions.
- All other conditions are optional.

- Some conditions are mutually exclusive. For example, "From the last Number hours" and "Starting after Date and Time" cannot both be selected.

Figure 8-10: Reports Wizard: Choosing Conditions



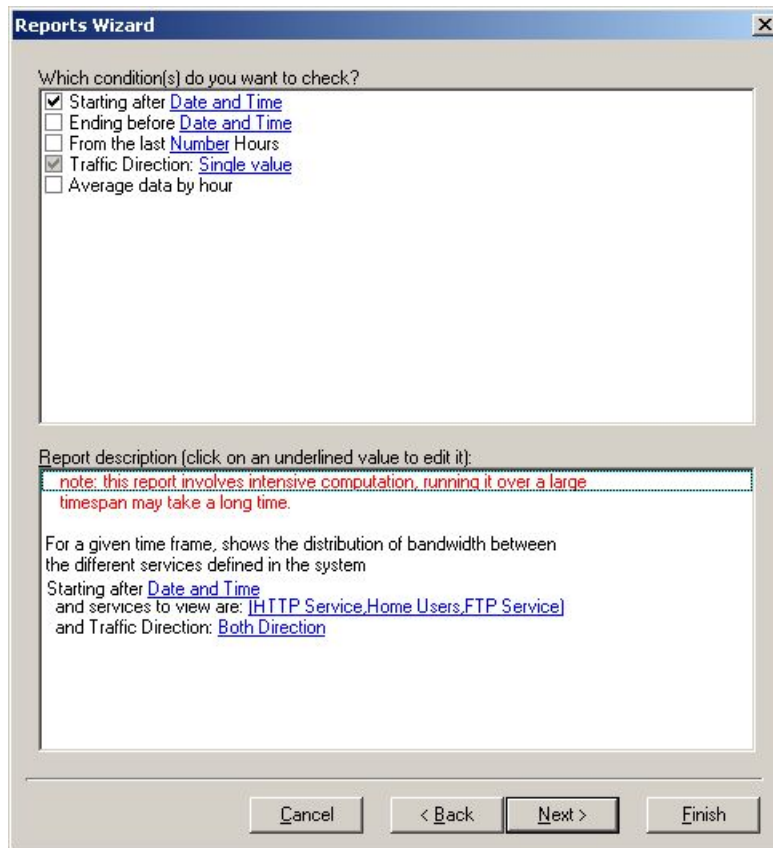
Step 7 Select the desired conditions.

The selected conditions appear in the report description in the bottom pane.

For example, if you want to define the time frame to begin at a specified time, rather than to cover a specified number of hours previous, select "Starting after Date and Time" in the upper pane.

The bottom pane now displays "Starting after Date and Time" rather than "From the last Number hours". The report time frame will be according to the Date and Time values, if selected, even if "From the last 24 hour" still appears.

Figure 8-11: Reports Wizard: Conditions in the Report Description



If you also wanted an average per hour, you would check "Average date per hour" check box in the upper pane, and that condition would appear as an additional condition in the report description.

Step 8 Select the desired value for each selected condition.

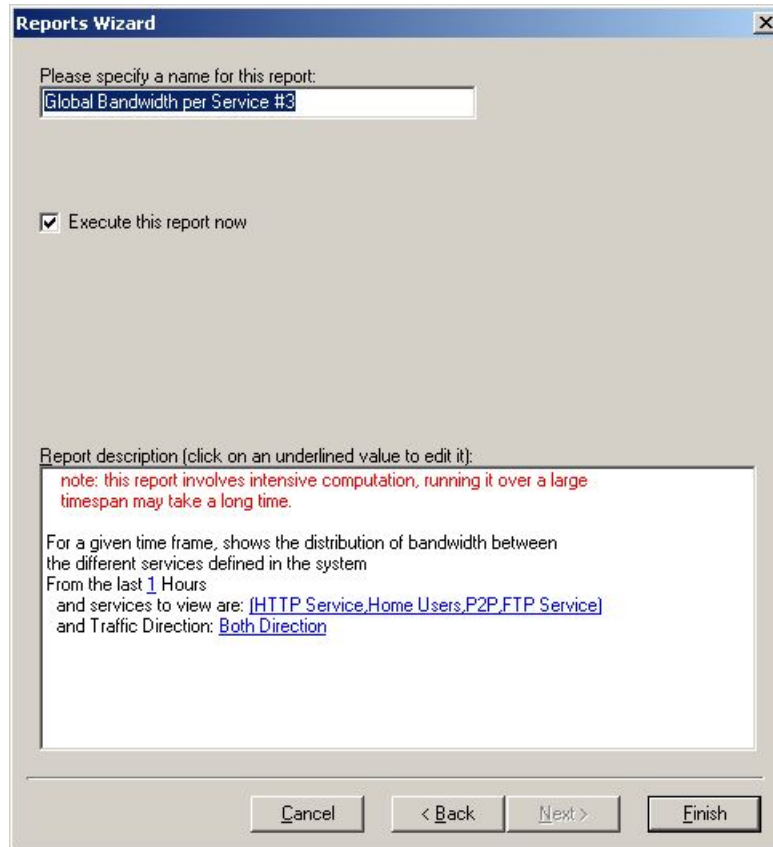
After you have selected the conditions in the upper pane, click on each underlined field type in the lower pane, and either select an appropriate item from a list provided by the wizard or type an entry of your choice. See the table below more information on field types and possible input options.

Step 9 When all conditions have a specific value assigned, click **Next**. (If the **Next** button is not available, you have not specified a value for a required condition.)

The final *Reports Wizard* dialog box appears, allowing you to name the report.

The complete report description appears, allowing you to make additional changes to the condition field values, if desired

Figure 8-12: Reports Wizard: Final Report Description



Step 10 (Optional) In the *Please specify a name for this report* text box, type a meaningful name for the report.


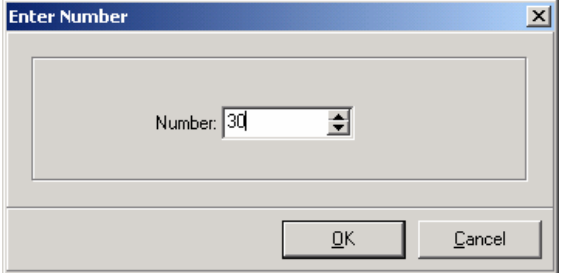
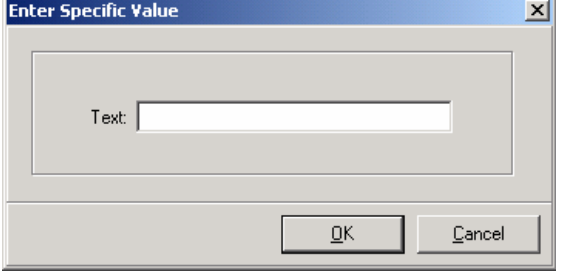
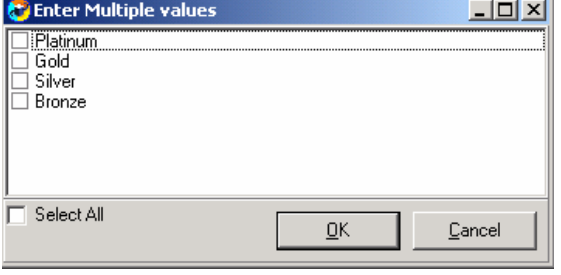
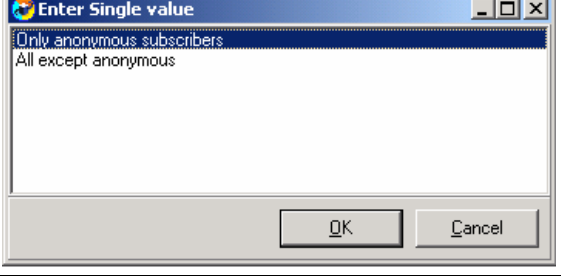
Step 11 If you want to view the report, select the **Execute this report now** check box and click **Finish**.

The report is generated and appears in the *Reporter Main Screen* (see *Working with Reports* (on page 8-19))

-or-

If you want to save the report without viewing it, clear the **Execute this report now** check box and click **Finish**.

Table 8-3 Condition Field Values

Field Type	Examples of associated items	Input Screen
Date and Time	Starting after <i>Date and Time</i> Ending before <i>Date and Time</i>	
Number	From the Last <i>Number</i> days Limit number of results to: <i>Number</i>	
Specific Value	Filter to specific subscriber: <i>Specific Value</i> Where text contains: <i>Specific Value</i>	
Multiple Values	Filter to the following services: <i>Multiple Values</i>	
Single Value	Filter by subscribers origin: <i>Single Value</i>	

Generating a Report

Reports are generated only from the *Reports Wizard*, but they are displayed in the *Reporter Main Screen*.

To generate a report:

Step 1 From the **Reports Wizard**, choose a report.

Step 2 Click **Report**.

The report is generated and appears in the *Reporter Main Screen* (see *Working with Reports* (on page 8-19)).

Duplicating an Existing Report Definition

You can duplicate an existing report definition. Use this feature when you want to create a report that is very similar to a report you have already defined, rather than starting "from scratch".

To create a duplicate report definition:

Step 1 From the **Reports Wizard**, choose a report.

Step 2 Click **Copy**.

The report is created. You can now edit and rename as desired.

Modifying an Existing Report Definition

You can edit a report definition on two levels:

- Edit the specific values only: If a report is run every week, you would simply edit the starting date and time.
- Change the conditions: Change the time frame from a starting date and time to the last number of days.

If you are only changing specific values of already selected conditions, you can do this from the report description that appears when the report is selected (step 1). You can then run the report without any further steps. However, if you wish to change the conditions of the report, you must use the **Modify** button to access the remainder of the wizard.

To modify an existing report definition:

Step 1 From the **Reports Wizard**, choose a report.

The report description appears.

You can edit the specified values of any conditions.

Step 2 Click **Modify**.

The available conditions are displayed.

You can select different conditions.

Step 3 Edit the report as desired. (See *Creating a New Report Definition* (on page 8-7).)

Renaming an Existing Report Definition

You can rename an existing report definition. This is useful when the same report is generated on a regular basis; the date or other identifying information can be included in the name of the report.

To rename a report definition:

Step 1 From the **Reports Wizard**, choose a report.

Step 2 Click **Rename**.

The following dialog box appears.

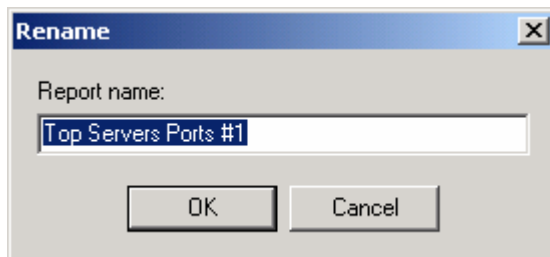


Figure 8-13: Rename a Report Dialog Box

Step 3 Type in a new name.

Step 4 Click **OK**.

The report is now listed under the new name.

Deleting a Report Definition

You can delete a report definition.

To delete a report definition:

Step 1 From the **Reports Wizard**, choose a report.

Step 2 Click **Delete**.

The following confirmation dialog box appears.

**Step 3** Click **Yes**.

The selected report definition is deleted.

Working with Reports

Although you use the *Reports Wizard* to define and generate a report, the generated report appears in the *Reporter Main Screen*. The report can be displayed as a graph or a table. You can edit the graphs, export the graph to a file, and print out the current graph.

Report Options

In addition to the command menus and the toolbar found on the *Reporter Main Screen* ("The [Reporter Main Screen](#)" on page 8-4), the report display has a number of buttons. The buttons are different for the chart (graph) and for the table. The buttons are explained in the table below.

Figure 8-14: Report Display with Report Options

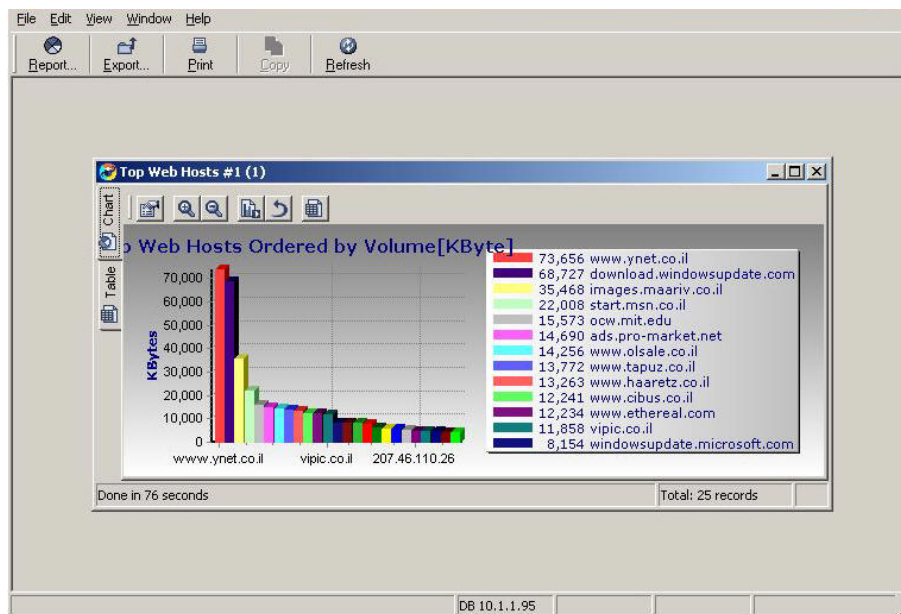
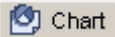






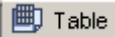



Table 8-4 Report Option Buttons

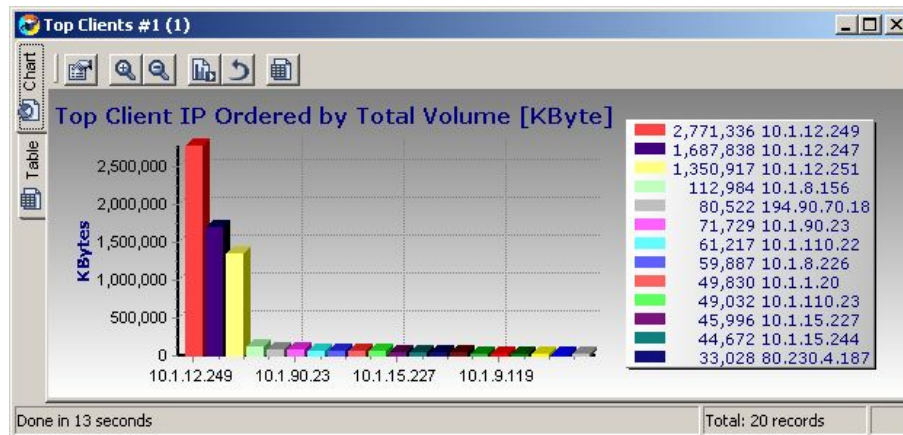
Button	Description
Chart View	 Chart
	Chart Properties: Opens the chart editor dialogs
	Zoom In
	Zoom Out
	Save Look: Saves the current “look” of the chart—all editing selections are saved.
	Remove Saved Look: All editing selections are removed and the default chart look is applied
	Export
Table View	 Table
	Find: find a specific value or text in the report table

Viewing Reports

There are two possible views for each report:

- Table
- Chart

Click the appropriate tab located on the left side of each report to select the desired view.



Client_IP	Hit_Count	Total_Volume	Downstream_Volume	Upstream_Volume
10.1.12.249	7437	2771336	202622	2568713
10.1.12.247	5333	1687838	70630	1617207
10.1.12.251	4800	1350917	1320605	30311
10.1.8.156	4340	112984	106621	6363
194.90.70.18	597	80522	79030	1491
10.1.90.23	15115	71729	9263	62465
10.1.110.22	13325	61217	8140	53077
10.1.8.226	2177	59887	47331	12555
10.1.1.20	1951	49830	904	48925
10.1.110.23	13281	49032	7667	41364
10.1.15.227	265	45996	44787	1208
10.1.15.244	494	44672	43130	1542

Done in 13 seconds Total: 20 records

The table is useful for locating specific information. Use the **Find** option to locate a specific record in the table.

Editing a Chart

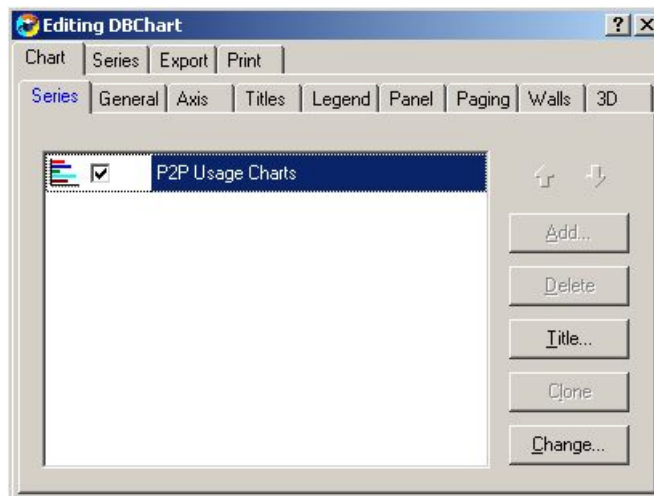
Use the *Chart Properties* option to edit the appearance and type of any report chart. This option allows you to edit almost every feature of the graph, including colors, fonts, line sizes and styles, and type of graph.

To edit a report chart:

Step 1 Click  (*Chart Properties*).

The following dialog box appears.

Figure 8-15: Edit Chart Dialog



This is a complete chart editing application. It has its own **Help** feature that you can access to find out more about how to edit the chart.

Generating a New Report

If you wish to generate a report based on a different report definition, you must return to the *Reports Wizard*.

To generate a different report:

Step 1 In the toolbar, click  **Report...**

The *Reports Wizard* opens.


Step 2 Select the desired report definition or create a new one (see *Defining the Report* (on page 8-6)).

Step 3 Click **Report** or **Finish** in the *Reports Wizard* to generate the report, which will appear in the *Reporter Main Screen*.

Refreshing the Report

If you have been editing the report, you may wish to use this option to make sure the report represents current data before printing it or exporting it. Refreshing updates the report contents without changing the appearance of the report.


To refresh a report:

-
- Step 1** In the toolbar, click  Refresh.
- The report is updated.
-

Printing Reports

Use this option to print reports, both tables and charts. Use the **Print Preview** and **Print Setup** options on the **File** menu to see the chart before printing it and to set a variety of printer options.

To print a report:

-
- Step 1** In the toolbar, click  Print.
- The selected chart is printed.
-

Exporting Reports

Use this option to export a chart to most of the common text and graphic formats.

To export a report chart:

-
- Step 1** In the toolbar, click  Export...

The *Save Report Chart As* browser window appears.

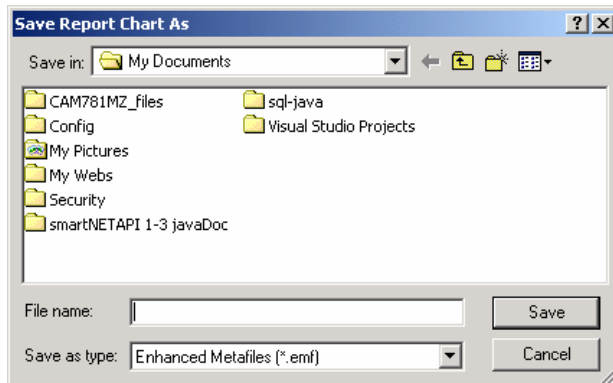


Figure 8-16: Save Report Chart As Browser Window

Step 2 Select the desired file name and type.

Step 3 Click **Save**.

The current report chart is saved to the specified file name and type.



SCAS Reporter Templates

This appendix describes the SCAS Reporter Templates.

Overview of Report Templates

The SCAS Reporter provides groups of templates from which to generate reports. Each template allows you to select the values of the default filter conditions. It is also possible to impose additional constraints by adding filters to the list of active filters.

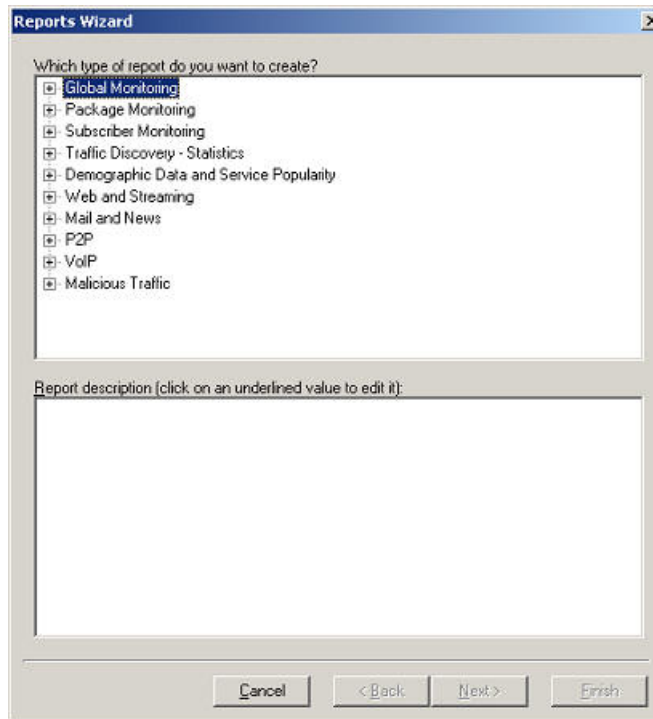


Note

The default filter fields are marked in **red** in the tables for each report type.

The figure below illustrates the wizard screen where you select a template from the list of available groups.

Figure A-1: Reports Wizard: New



At a high level, the system provides two categories of reports:

- **Monitoring reports**, which provide insight as to how network resources are utilized according to the configured services in the system at various granularities (global, package, subscriber).
- **Traffic Discovery reports**, which provide statistical information on network activity and help identify the characteristics of the traffic traversing the network.

The following subsections describe the mainstream reports in each category.

Monitoring Reports

Monitoring reports provide information on the distribution and consumption of network resources. Reports in this category are useful for the understanding of how the network is used at different granularities (such as for the entire link, or for traffic generated by all subscribers in a particular package counter, or for traffic generated by a particular subscriber). These reports are critical for the tuning of the solution's configuration according to the changing network patterns.

Monitoring RDRs are created from the Link, Subscriber, and Package RDRs (that are generated by the SCE device). These RDRs provide periodic usage information (at the various granularities) that is processed according to the selected report template to provide the final report.

Reports of this type typically show a specific *metric* for a set of *service counters* at a selected *granularity*. For example, *bandwidth* for *P2P and Browsing* service counters at a *link* granularity, or *volume* for the *Streaming* service counter for subscribers in the *Gold* package counter.

Selecting the service counters on which to report is done via the report-template wizard. The available service counters are those defined in the service configuration of the SCE device from which the reports are generated.

Granularity

A report's granularity controls what part of the traffic the selected report addresses. The following granularities are supported:

- **Global:** Provide visibility into all traffic processed by the SCE(s) being reported on. Use this global granularity to view the global distribution of network resources (for example, total P2P bandwidth for the last 24 hours)
- **Package:** Reports on traffic mapped to subscribers in a particular package counter. Use package granularity to monitor how network resources are used by subscribers assigned to a particular package counter (for example, the total volume of streaming traffic for all subscribers assigned to the Gold package counter in the last 10 days). Note that to generate package counter reports, subscribers must be defined (in any of the subscriber modes) and assigned to a particular package. See Chapter 7, *Managing Subscribers*, for a description of how to manage subscribers; see Chapter 5, *Constructing Service Configurations*, for a description of defining different packages in the system.
- **Subscriber:** Provides insight into the activity of a single subscriber as defined in the **SCAS BB** solution. Use subscriber granularity to view how a particular subscriber is utilizing network resources (for example, the number of P2P sessions generated by subscriber *xyz* for each hour during the last 12 hours). Subscriber reports are available for those subscribers flagged for real-time reporting. (See Chapter 5, *Constructing Service Configurations*, for a description of managing real-time subscriber reporting.)

Each report template generates a report in a specific granularity (global, package, or subscriber). Global and package reports are accessible through in the "*Global Monitoring* (on page [A-7](#))" report template group (see page [A-8](#) ("*Global Monitoring*" on page [A-7](#))). Subscriber reports are accessible through the "*Subscriber Monitoring* (on page [A-14](#))" report template group (see page [A-13](#) ("*Subscriber Monitoring*" on page [A-14](#))).

Metrics

A metric is the statistic that is being reported on. The following metrics are available:

- **Bandwidth:** Represents the total Kilobits-per-second (Kbps) consumed by the selected service(s). Bandwidth graphs are presented by default as **stacked-area** (where each area/series indicates the bandwidth of a particular service).

When generating a bandwidth report it is possible to select the **direction:** upstream or downstream (to focus on a particular direction), or both (*default*). An additional option is to perform an **hourly average** of samples so as to create a single sample for each hour. This is recommended when generating a report for more than several hours, in which case a single sample per hour is usually sufficient and reduces the number of samples displayed (it also increases performance and improves the visualization of the data).

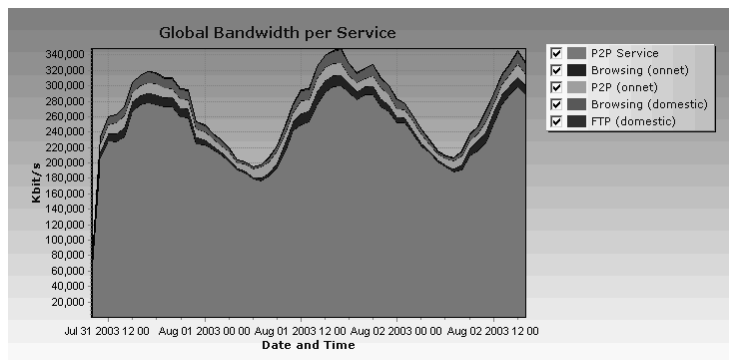


Figure A-1: Global Bandwidth per Service

- **Volume:** Represents the total volume (in kilobytes or megabytes) for a specific period of time, for the selected service counter(s). As opposed to the bandwidth metric (which provides normalized volume over time), volume reports provide the total volume consumed, grouped by specific time durations. Volume graphs are presented by default as **stacked bar-charts** (where each bar/series indicates the volume of a particular service counter).

Volume reports accumulated usage either for specific durations of time (hours or days), or for the entire duration of the report. An example of a report that groups volume by duration is Global Hourly Usage Volume, which generates a bar that accounts for the total volume consumed (by each service counter) during each hour of the selected time frame. As a different example, the Global Aggregated Usage Volume per Service report accounts for all volume of each service counter for the entire time frame of the report.

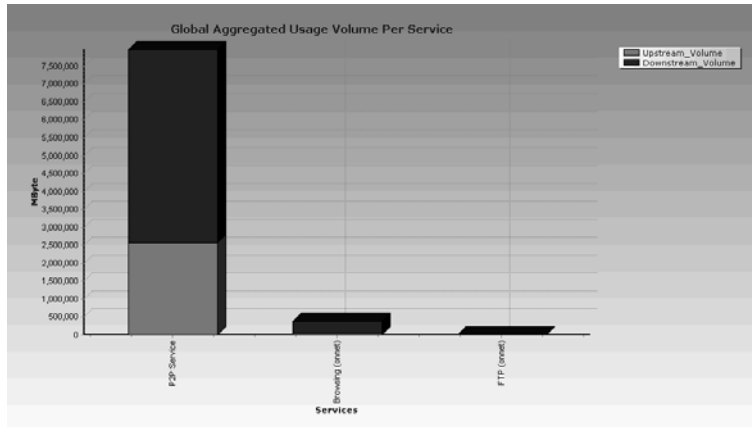


Figure A-2: Global Aggregated Usage Volume per Service

- Sessions:** Counts the number of sessions. A session is a single network transaction (for example, RTSP stream or P2P file download). Sessions graphs are generated by default as **stacked-bar charts** (where each bar/series indicates the total number of sessions of a particular service counter).

Similarly to volume reports, Sessions reports can be grouped into specific durations (hours or days), so as to account for the total number of sessions in a particular hour/day consumed by a particular service counter.

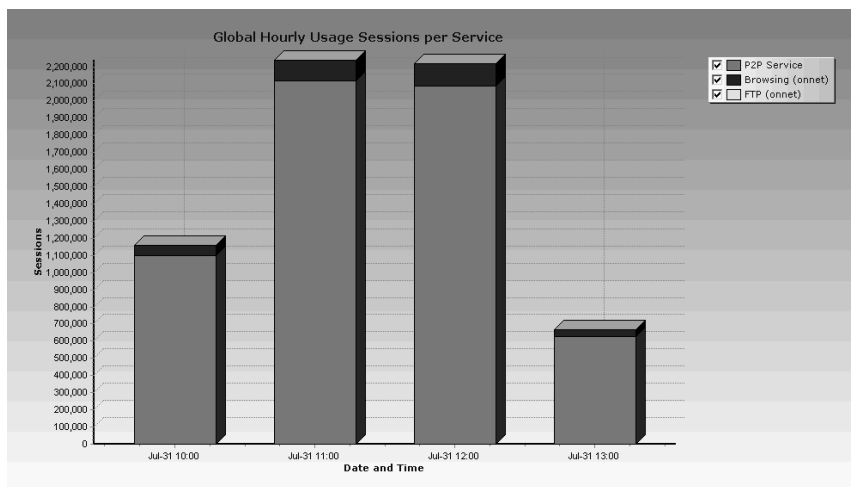


Figure A-3: Global Hourly Usage Sessions per Service

Traffic Discovery Reports

Traffic discovery reports provide raw statistics for analyzing network activities. They are useful for obtaining statistics on the general activity in the IP network, and are the key for the definition of the service configuration of the system.

The generation of traffic discovery reports is based on Transaction RDRs (generated by the SCE device). These sampled RDRs provide the statistical information from which the various Traffic Discovery histograms and charts are created.

Traffic Discovery reports generate histograms and distribution charts that are grouped by the selected *criteria* and ordered by the selected *order-parameter*. For example: Top *Protocols* sorted by *Total Volume*, or Top *Web-hosts* sorted by *Hit-Count*.

Criteria

Each report template focuses on a particular criterion based on layers 3–7, such as:

- Top Servers/Client IP addresses
- Top Server/Client Port numbers
- Top HTTP web-hosts
- Top NNTP news-groups

Report templates focusing on statistics from layers 3 and 4 (for example, IP addresses and port numbers) are found in "[Traffic Discovery - Statistics](#) (on page [A-17](#))". Report templates focusing on application- and protocol-specific information are in "[Traffic Discovery - Application Popularity](#) ("[Email and News Reports](#)" on page [A-31](#))" section.

Order Parameter

The order parameter indicates the parameter that the report will be sorted by. Available parameters are:

- **Total Volume:** Extrapolated total volume (both upstream and downstream)
- **Upstream Volume:** Extrapolated upstream volume
- **Downstream Volume:** Extrapolated downstream volume
- **Hit-Counts:** Extrapolated Number of transactions

Each report can be limited to a specific number of results, which allows focusing on the top areas of activity (according to the selected order-parameter), as illustrated in the following two figures.

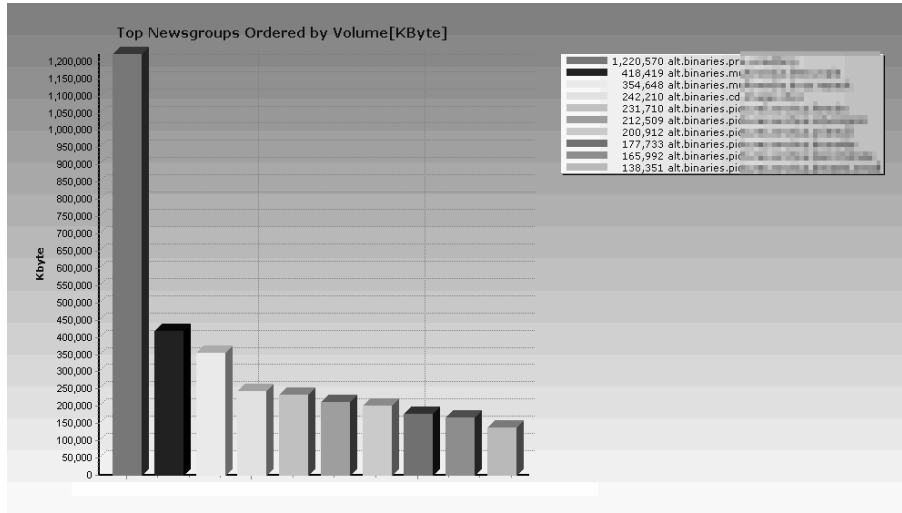


Figure A-4: Top Newsgroups Ordered by Volume

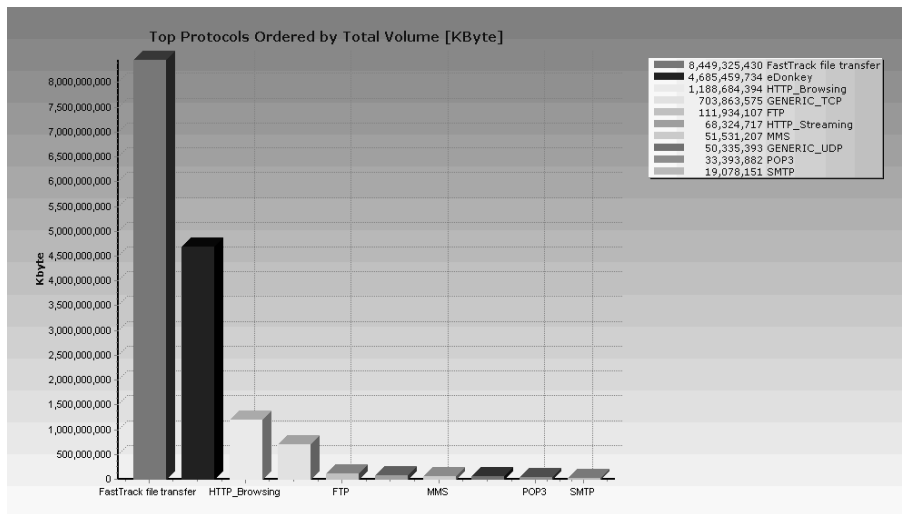


Figure A-5: Top Protocols Ordered by Volume

Global Monitoring

Use the Global Monitoring group of reports to view statistics regarding the traffic bandwidth or volume that was consumed. The bandwidth/volume consumption can be presented per service for the entire link.

Global Bandwidth per Service

For a given time frame, Global Bandwidth per Service shows the distribution of bandwidth between the different services defined in the system for all traffic, regardless of subscriber or package.

Table A-5 Global Bandwidth per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Global Hourly Usage Sessions per Service

For a given time frame, Global Hourly Usage Sessions per Service shows the distribution of sessions between the different service counters defined in the system, grouped by hour.

Table A-6 Global Hourly Usage Sessions per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Global Daily Usage Sessions per Service

For a given time frame, Global Daily Usage Sessions per Service shows the distribution of sessions between the different service counters defined in the system, grouped by day.

Table A-7 Global Daily Usage Sessions per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Global Hourly Usage Volume per Service

For a given time frame, Global Hourly Usage Volume per Service shows the distribution of volume between the different service counters defined in the system, grouped by hour.

Table A-8 Global Hourly Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Global Daily Usage Volume per Service

For a given time frame, Global Daily Usage Volume per Service shows the distribution of volume between the different service counters defined in the system, grouped by day.

Table A-9 Global Daily Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Global Aggregated Usage Volume per Service

For a given time frame, Global Aggregated Usage Volume per Service shows the most popular Service counter. It shows, for the selected time frame, the total amount of traffic volume (upstream and downstream) for each service counter (for all traffic, regardless of subscriber or package).

Table A-10 Global Aggregated Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Package to view <i>Single Value</i>	List	Select one of the packages.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Daily Peak BW for All Packages

For a given time frame, Daily Peak BW for All Packages shows value per day of the max 1hour/2hours BW in Kbps

Table A-11 Daily Peak BW for All Packages

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.

Global Hourly Aggregated Minutes per Service

For a given time frame, Global Hourly Aggregated Minutes per Service shows the total no. of minutes spent for service counters defined in the system, grouped by hour.

Table A-12 Global Hourly Aggregated Minutes per Service

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Global Concurrent Session per Service

For a given time frame, Global Concurrent Session per Service shows the distribution of concurrent sessions between the different service counters defined in the system

Table A-13 Global Hourly Aggregated Minutes per Service

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Package Monitoring

Package Bandwidth per Service

For a given time frame, Package Bandwidth per Service shows the distribution of bandwidth between the different service counters defined in the system for all subscribers belonging to a particular package.

Table A-14 Package Counter Bandwidth per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of services available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Package Hourly Usage Sessions per Service

For a given time frame, Package Hourly Usage Sessions per Service shows the distribution of sessions between the different service counters defined in the system, for the traffic of subscribers in a specific package, grouped by hour.

Table A-15 Package Hourly Usage Sessions per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Package Daily Usage Sessions per Service

For a given time frame, Package Daily Usage Sessions per Service shows the distribution of sessions between the different service counters defined in the system, for the traffic of subscribers in a specific package counter, grouped by day.

Table A-16 Package Daily Usage Sessions per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Condition	Field Type	Comments
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Package Hourly Usage Volume per Service

For a given time frame, Package Hourly Usage Volume per Service shows the distribution of volume between the different service counters defined in the system, for the traffic of subscribers in a specific package counter, grouped by hour.

Table A-17 Package Hourly Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Packagecounter to view <i>Single Value</i>	List	Select one of the package counters.

Package Daily Usage Volume per Service

For a given time frame, Package Daily Usage Volume per Service shows the distribution of volume between the different service counters defined in the system, for the traffic of subscribers in a specific package counter, grouped by day.

Table A-18 Package Daily Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Daily Peak BW per Package

For the given time frame, Daily Peak BW per Package shows the maximum BW value per day for the traffic of subscribers in a specific package counter

Table A-19 Daily peak BW per Package Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.
Peak BW over <i>Single Value</i>	List	List of available time frames.

Package Aggregated Usage Volume per Service

For a given time frame, Package Aggregated Usage Volume per Service shows the most popular Service counter for a specific package counter. It shows, for the selected time frame, the total amount of traffic volume (upstream and downstream) for each service counter (for subscribers in a specific package).

Table A-20 Package Aggregated Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Package Hourly Aggregated Minutes per Service

For a given time frame, Package Hourly Aggregated Minutes per Service shows the total no. of minutes spent for service counters for a specific package counter defined in the system, grouped by hour.

Table A-21 Package Hourly Aggregated Minutes per Service

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Package Concurrent Session per Service

For a given time frame, Package Concurrent Session per Service shows the distribution of concurrent sessions between the different Service Counters for a specific package counter defined in the system

Table A-22 Package Concurrent Session per Service

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Subscriber Monitoring

Use the Subscriber Monitoring group of reports to view statistics regarding the bandwidth or volume of traffic used by the subscriber. The reports are provided per service counter for the total volume consumed by the subscriber. The Top Volume Consumers report identifies the subscribers that consume the largest traffic volume. Subscriber bandwidth and volume reports are available for those subscribers configured for real-time monitoring. (See *Managing Subscribers* (on page 7-1), for a description of how to configure real-time subscribers.)

Subscriber Bandwidth per Service Counter

For a given time frame, Subscriber Bandwidth per Service shows the distribution of bandwidth between the different service counters defined in the system for a particular subscriber.

Table A-23 Subscriber Bandwidth per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Subscriber name is <i>Specific Values</i>	Text	IP address (decimal format) or subscriber name.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Average data by hour	BOOLEAN	Select option or not (default: false).

Subscriber Hourly Usage Volume per Service

For a given time frame, Subscriber Hourly Usage Volume per Service shows the hourly distribution of volume between the different service counters defined in the system for a particular subscriber.

Table A-24 Subscriber Hourly Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Subscriber name is <i>Specific Values</i>	Text	IP address (decimal format) or subscriber name.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Subscriber Daily Usage Volume per Service

For a given time frame, Subscriber Daily Usage Volume per Service shows the daily distribution of volume between the different service counters defined in the system for a particular subscriber.

Table A-25 Subscriber Daily Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.

Condition	Field Type	Comments
Subscriber name is <i>Specific Values</i>	Text	IP address (decimal format) or subscriber name.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Top Subscribers

For a given time frame, Top Subscribers shows a list of the top subscriber volume consumption in a specific hour/day.

Table A-26 Top Subscribers Template

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Filter to Directional Volume <i>Single Value</i>	List	Select one of the directions of the volume.
Aggregation Period <i>Single Value</i>	List	Select one or more packages.
Focus on the services: <i>Multiple Values</i>	List	Select one or more services.
Where Subscriber Id contains: <i>Specific Values</i>	Text	Pattern which represent group of subscribers.

Subscriber Hourly Usage Sessions per Service

For a given time frame, Subscriber Hourly Usage Sessions per Service shows the hourly distribution of sessions between the different service counters defined in the system for a particular subscriber.

Table A-27 Subscriber Hourly Usage Sessions per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Subscriber name is <i>Specific Values</i>	Text	IP address (decimal format) or subscriber name.
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.

Subscriber Daily Usage Sessions per Service

For a given time frame, Subscriber Daily Usage Sessions per Service shows the daily distribution of sessions between the different service counters defined in the system for a particular subscriber.

Table A-28 Subscriber Daily Usage Sessions per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Subscriber name is Specific Values	Text	IP address (decimal format) or subscriber name.
Service counters to view are Iteration Value	List	List of service counters available for this subscriber domain.

Subscriber Aggregated Usage Volume per Service

For a given time frame, Subscriber Aggregated Usage Volume per Service shows the most popular Service counter for a particular subscriber.

Table A-29 Subscriber Aggregated Usage Volume per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Subscriber name is Specific Values	Text	IP address (decimal format) or subscriber name.
Service counters to view are Iteration Value	List	List of service counters available for this subscriber domain.

Daily Peak BW for Specific Subscriber

For the given time frame, Daily Peak BW for Specific Subscriber shows the maximum BW value per day for the traffic of a specific subscriber.

Table A-30 Daily peak BW for Specific Subscriber Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Subscriber name is Specific Values	Text	IP address (decimal format) or subscriber name.
Peak BW over Single Value	List	List of available time frames.

Subscriber Hourly Aggregated Minutes per Service

For a given time frame, Subscriber Hourly Aggregated Minutes per Service shows the total no. of minutes spent for service counters for a specific package counter defined in the system, grouped by hour.

Table A-31 Subscriber Hourly Aggregated Minutes per Service Template

Condition	Field Type	Comments
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Subscriber name is Specific Values	Text	IP address (decimal format) or subscriber name.
Service counters to view are Iteration Value	List	List of service counters available for this subscriber domain.

Traffic Discovery - Statistics

Use the Traffic Discovery - Statistics group of reports to view statistics compiled from the source and destination IP addresses and ports of the system traffic. Note that the reports in this group are not per subscriber; they supply general Port and IP address information.

Top IP Protocol

For a given time frame, Top IP Protocols show the most popular IP protocol for certain services.

Table A-32 Top Signature-Based Protocols Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Servers

For a given time frame, Top Servers shows the most popular servers for certain services.

Table A-33 Top Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Servers TCP Ports

For a given time frame, Top Servers TCP Ports shows the most popular server TCP ports for certain services.

Table A-34 Top Servers TCP Ports Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Servers UDP Ports

For a given time frame, Top Servers UDP Ports shows the most popular server UDP ports for certain services.

Table A-35 Top Servers UDP Ports Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client

For a given time frame, Top Client shows the most popular client IP for certain services.

Table A-36 Top Client Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client IP To Server TCP Port

For a given time frame, Top Client IP To Server TCP Port shows the most popular client IP to server TCP port for certain services.

Table A-37 Top Client IP to Server TCP Port Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client IP To Server UDP Port

For a given time frame, Top Client IP To Server Port shows the most popular client IP to server UDP port for certain services.

Table A-38 Top Client IP to Server UDP Port Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.

Condition	Field Type	Comments
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client IP to Server IP

For a given time frame, Top Client IP to Server IP shows the most popular client IP to server IP for certain services.

Table A-39 Top Client IP To Server IP Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Server IP and Server TCP Port

For a given time frame, Top Server IP and Server TCP Port shows the most popular server IP and server TCP port for certain services.

Table A-40 Top Server IP and Server TCP Port Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).

Condition	Field Type	Comments
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client IP and Server UDP Port

For a given time frame, Top Server IP and Server UDP Port shows the most popular server IP and server UDP port for certain services.

Table A-41 Top Server IP and Server UDP Port Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client IP to Server IP and Server TCP Port

For a given time frame, Top Client IP to Server IP and Server TCP Port shows the most popular server IP and server TCP port for certain services.

Table A-42 Top Client IP To Server IP and Server TCP Port Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.

Condition	Field Type	Comments
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Client IP to Server IP and Server UDP Port

For a given time frame, Top Client IP to Server IP and Server UDP Port shows the most popular server IP and server UDP port for certain services.

Table A-43 Top Client IP To Server IP and Server UDP Port Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Signature-Based Protocols

For a given time frame, Top Signature-Based Protocols show the most popular signature-based protocol for certain services.

Table A-44 Top Signature-Based Protocols Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Service TCP Ports

For a given time frame, Top Service TCP Ports shows the most popular TCP server ports of a certain service(s).

Table A-45 Top TCP Service Ports Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Service UDP Ports

For a given time frame, Top Service UDP Ports shows the most popular UDP server ports of a certain service(s).

Table A-46 Top UDP Service Ports Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Web and Streaming Reports

Use the Web and Streaming group of reports to compile statistics presenting the most popular servers or hosts for the various pre-defined system services (such as Browsing, Streaming, and Downloading) and for user-defined services.

Top Web Hosts

For a given time frame, Top Web Hosts shows the most popular web servers.

Table A-47 Top Web Hosts Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Do not retrieve empty Host Names	BOOLEAN	Select option or not.
Filter to specific subscriber <i>Specific Values</i>	Text	IP address (decimal format) or subscriber name.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.

Condition	Field Type	Comments
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain
Where host contains: <i>Specific Values</i>	Text	Host name.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top HTTP Streaming Hosts

For a given time frame, Top HTTP Streaming Hosts shows the most popular streaming servers.

Table A-48 Top HTTP Streaming Hosts Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Where host contains: <i>Specific Values</i>	Text	Host name.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top RTSP Hosts

For a given time frame, Top RTSP Hosts shows the most popular real-time streaming protocol (RTSP) servers.

Table A-49 Top RTSP Hosts Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Where host contains: <i>Specific Values</i>	Text	Host name.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top MMS Servers

For a given time frame, Top MMS Servers shows the most popular MMS hosts.

Table A-50 Top MMS Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.

Condition	Field Type	Comments
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top FTP Servers

For a given time frame, Top FTP Servers shows the most popular FTP file hosts.

Table A-51 Top FTP Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Service Servers

For a given time frame, Top Service Servers shows the most popular servers of a certain service(s).

Table A-52 Top Service Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.

Condition	Field Type	Comments
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Streaming Host Distribution by Subscriber Packages

For a given time frame, Streaming Host Distribution by Subscriber Packages shows the most popular streaming servers, grouped by the package of the requesting subscriber.

Table A-53 Streaming Host Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

RTSP Host Distribution by Subscriber Packages

For a given time frame, RTSP Host Distribution by Subscriber Packages shows the most popular real-time streaming protocol servers, grouped by the package of the requesting subscriber.

Table A-54 RTSP Host Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.

Condition	Field Type	Comments
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

MMS Server Distribution by Subscriber Packages

For a given time frame, MMS Server Distribution by Subscriber Packages shows the most popular Microsoft Manager Server servers, grouped by the package of the requesting subscriber.

Table A-55 MMS Server Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

FTP Server Distribution by Subscriber Packages

For a given time frame, FTP Server Distribution by Subscriber Packages shows the most popular FTP file servers, grouped by the package of the requesting subscriber.

Table A-56 FTP Server Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.

Condition	Field Type	Comments
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Service Distribution by Subscriber Packages

For a given time frame, Service Distribution by Subscriber Packages shows the distribution of service usage according to the subscriber packages.

Table A-57 Service Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to the following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Email and News Reports

Use the Email and News group of reports to view statistics of the email and news traffic.

Top SMTP Servers

For a given time frame, Top SMTP Servers shows the most popular SMTP hosts.

Table A-58 Top SMTP Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options

Top POP3 Servers

For a given time frame, Top POP3 Servers shows the most popular POP3 hosts.

Table A-59 Top POP3 Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).

Condition	Field Type	Comments
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top NNTP Servers

For a given time frame, Top NNTP Servers shows the most popular NNTP hosts.

Table A-60 Top NNTP Servers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top E-mail Senders

For a given time frame, Top E-mail Senders shows the top e-mail senders.

Table A-61 Top E-mail Senders Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.

Condition	Field Type	Comments
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top E-mail Recipients

For a given time frame, Top E-mail Recipients shows the top e-mail recipients.

Table A-62 Top E-mail Recipients Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top E-mail Account Owners

For a given time frame, Top E-mail Account Owners shows the top e-mail account owners.

Table A-63 Top E-mail Account Owners Template

Condition	Field Type	Comments
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.

Condition	Field Type	Comments
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Newsgroups

For a given time frame, Top Newsgroups shows the most popular newsgroups.

Table A-64 Top Newsgroups Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Subscriber to Newsgroup

For a given time frame, Top Subscriber to Newsgroup shows the top subscriber to newsgroup for certain services.

Table A-65 Top Subscriber to Newsgroup Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.

Condition	Field Type	Comments
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top NNTP Consumers

For a given time frame, Top NNTP Consumers shows the top NNTP Consumers.

Table A-66 Top NNTP Consumers Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

SMTP Server Distribution by Subscriber Packages

For a given time frame, SMTP Server Distribution by Subscriber Packages shows the most popular SMTP servers, grouped by the package of the requesting subscriber.

Table A-67 SMTP Server Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.

Condition	Field Type	Comments
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

POP3 Server Distribution by Subscriber Packages

For a given time frame, POP3 Server Distribution by Subscriber Packages shows the most popular POP3 servers, grouped by the package of the requesting subscriber.

Table A-68 POP3 Server Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

NNTP Server Distribution by Subscriber Packages

For a given time frame, NNTP Server Distribution by Subscriber Packages shows the most popular NNTP servers, grouped by the package of the requesting subscriber.

Table A-69 NNTP Server Distribution by Subscriber Packages Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.

Condition	Field Type	Comments
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

P2P Reports

Use the P2P Reports group of reports to view statistics of the P2P traffic.

Top P2P Consumers

For a given time frame, Top P2P Consumers shows a list of the top P2P subscriber volume consumption.

Table A-70 Top P2P Consumers Template

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Filter to Directional Volume <i>Single Value</i>	List	Select one of the directions of the volume.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	Select one or more packages.
Focus on the services: <i>Multiple Values</i>	List	Select one or more services.
P2P Protocol: <i>Multiple Values</i>	List	Select one or more protocol

Top P2P Downloaders

For a given time frame, Top P2P Downloaders show the the top P2P downloader consumers.

Table A-71 Top P2P Downloaders Template

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	Select one or more packages.
Focus on the services: <i>Multiple Values</i>	List	Select one or more services.

Condition	Field Type	Comments
P2P Protocol: <i>Multiple Values</i>	List	Select one or more protocol

Top P2P Uploaders

For a given time frame, Top P2P Uploaders show the most popular P2P uploader consumers.

Table A-72 Top P2P Uploaders Template

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	Select one or more packages.
Focus on the services: <i>Multiple Values</i>	List	Select one or more services.
P2P Protocol: <i>Multiple Values</i>	List	Select one or more protocol

Top P2P Protocols

For a given time frame, Top P2P Protocols show the most popular P2P protocol for certain services.

Table A-73 Top P2P Protocols Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top P2P Protocols

For a given time frame, Top P2P File Extensions shows the most popular P2P file-extensions

Table A-74 Top P2P File Extensions Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain
Filter to the following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

VoIP Reports

Use the VoIP group of reports to view statistics of the VoIP traffic.

Global Bandwidth per VoIP Service

For a given time frame, Global Bandwidth per VoIP Service shows the distribution of bandwidth between the different VoIP services defined in the system for all traffic, regardless of subscriber or package.

Table A-75 Global Bandwidth per VoIP Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	List	List of VoIP service counters available for this subscriber domain.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Global Hourly Call Minutes per VoIP Service

For a given time frame, Global Hourly Call Minutes per VoIP Service shows the distribution of Call Minutes between the different VoIP service counters defined in the system, grouped by day.

Table A-76 Global Daily Usage Volume per Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	List	List of VoIP service counters available for this subscriber domain.

Package Bandwidth per VoIP Service

For a given time frame, Package Bandwidth per VoIP Service shows the distribution of bandwidth between the different VoIP services defined in the system for the traffic of subscribers in a specific package.

Table A-77 Package Bandwidth per VoIP Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	List	List of VoIP service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Package Hourly Call Minutes per VoIP Service

For a given time frame, Global Hourly Call Minutes per VoIP Service shows the distribution of Call Minutes between the different VoIP service counters defined in the system, grouped by day.

Table A-78 Package Daily Usage Volume per Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	List	List of VoIP service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Subscriber Bandwidth per VoIP Service

For a given time frame, Subscriber Bandwidth per VoIP Service shows the distribution of bandwidth between the different VoIP services defined in the system for the traffic of subscriber in a specific package.

Table A-79 Subscriber Bandwidth per VoIP Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	Text	IP address (decimal format) or subscriber name.
Subscriber name is <i>Specific Values</i>	List	Select one of the package counters.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Subscriber Hourly Call Minutes per VoIP Service

For a given time frame, Subscriber Hourly Call Minutes per VoIP Service shows the distribution of Call Minutes between the different VoIP service counters defined in the system, grouped by day.

Table A-80 Subscriber Daily Usage Volume per Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	Text	IP address (decimal format) or subscriber name.
Subscriber name is <i>Specific Values</i>	List	Select one of the package counters.
Traffic Direction <i>Single Value</i>	List	Select one of the directions of the bandwidth.

Global Concurrent Calls per VoIP Service

For a given time frame, Global Concurrent Calls per VoIP Service shows the distribution of concurrent sessions between the different VoIP service counters defined in the system, grouped by day.

Table A-81 Global Concurrent Calls per VoIP Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	List	List of VoIP service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Packet Concurrent Calls per VoIP Service

For a given time frame, Packet Concurrent Calls per VoIP Service shows the distribution of concurrent sessions between the different VoIP service counters defined in the system, grouped by day.

Table A-82 Packet Concurrent Calls per VoIP Service Template

Condition	Field Type	Comments
VoIP Service counters to view are <i>Iteration Value</i>	List	List of VoIP service counters available for this subscriber domain.
Package counter to view <i>Single Value</i>	List	Select one of the package counters.

Top SIP Domains

For a given time frame, Top SIP Domains shows the most popular SIP Domains.

Table A-83 Top SIP Domains Template

Condition	Field Type	Comments
Order by <i>Single Value</i>	List	Choose a field to determine the listing order.
Limit number of results to: <i>Numbers</i>	Number	Type a number.
Starting after <i>Date and Time</i>	Date	Select date and time from the pop-up window.
Ending before <i>Date and Time</i>	Date	Select date and time from the pop-up window.
From the last <i>Numbers</i> days	Number	Type a number.
Filter to subscribers of following services: <i>Multiple Values</i>	List	List of services available for this domain.
Filter to subscribers of following packages: <i>Multiple Values</i>	List	List of packages available for this domain.
Filter to specific subscriber: <i>Specific Values</i>	Text	Subscriber name or IP address (decimal format).
Filter by subscribers origin: <i>Single Value</i>	List	List of subscriber identification options: anonymous, recognized.
Time_Frames to focus: <i>Multiple Values</i>	List	Select one or more of 4 time frame options.

Top Talkers

For a given time frame, Top Talkers shows a list of the top talker volume/session/minutes consumption in a specific hour/day for a specific/all VoIP services.

Table A-84 Top Talker Template

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Select the number of top subscriber to introduce.
Filter to Metric counter <i>Single Value</i>	List	Select one of the metric counter: Session/Upvolume/Downvolume/Minutes.
Aggregation Period <i>Single Value</i>	List	Select hourly or daily time resolution.
Where Subscriber ID contains: <i>Specific Values</i>	Text	Pattern that represents group of subscribers.

Demographic Data and Service Popularity Reports

Use the Demographic Data and Service Popularity group of reports to view demographic and service statistics.

Global Active Subscriber per Service

For a given time frame, Global Active Subscriber per Service shows the distribution of active subscriber in a single service counters in relative to the Total Active Subscriber defined in the system for all traffic, regardless of package.

Table A-85 Global Active Subscriber per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Link to focus	List	Default is all links.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Service Popularity among Subscribers

For a given time frame, Service popularity among subscribers shows the percentage of subscribers using specific service against all services defined in the system for all traffic, regardless of package.

Table A-86 Service Popularity Among Subscribers Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Link to focus	List	Default is all links.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Package Active Subscriber per Service

For a given time frame, Package Active Subscriber per Service shows the distribution of active subscriber in a single Service counters in relative to the Total Active Subscriber defined in the system for the traffic of subscribers in a specific package counter

Table A-87 Package Active Subscriber per Service Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view are <i>Iteration Value</i>	List	Select one of the package counters
Link to focus	List	Default is all links.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Service Popularity among Subscribers of a Specific Package

For a given time frame, Service Popularity Among Subscribers of Specific Package shows the percentage of subscribers using specific service against all services defined in the system for all traffic.

Table A-88 Service Popularity Among Subscribers of Specific Package Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view are <i>Iteration Value</i>	List	Select one of the package counters
Link to focus	List	Default is all links.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Service Popularity among Subscribers of a Specific Package

For a given time frame, Service Popularity Among Subscribers of Specific Package (Average) shows the percentage of subscribers using a specific service against all services defined in the system for all traffic.

Table A-89 Service Popularity Among Subscribers of Specific Package (Average) Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Package counter to view are <i>Iteration Value</i>	List	Select one of the package counters
Link to focus	List	Default is all links.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Service Popularity among Subscribers of a Specific Package

For a given time frame, Service Popularity Among Subscribers (Average) shows the percentage of subscribers using specific service against all services defined in the system for all traffic, regardless of package.

Table A-90 Service Popularity Among Subscribers (Average) Template

Condition	Field Type	Comments
Service counters to view are <i>Iteration Value</i>	List	List of service counters available for this subscriber domain.
Link to focus	List	Default is all links.
Average data by hour	BOOLEAN	Select option or not (default: false). If this option is selected, a single value is used for each hour (average of all samples). This option is recommended when generating the report for more than several (24) hours.

Relative Consumption Consumptions of Top Subscribers

For a given time frame, Relative Consumption Consumptions of Top Subscribers shows a list of the top subscriber volume consumption in specific service or for all services in a specific hour/day. The consumption will be presented as relative to all subscriber consumption. (For example, this report might show that the total volume consumption of the top 50 subscribers in P2P service represents 25% of the total consumption for all subscribers in P2P service.)

Table A-91 Relative Consumption Consumptions of Top Subscribers Template

Condition	Field Type	Comments
Limit number of results to: <i>Numbers</i>	Number	Select the number of top subscriber to introduce.
Filter to Directional Volume <i>Single Value</i>	List	Select one of the directions of the volume.
Aggregation Period <i>Single Value</i>	List	Select hourly or daily time resolution.
Focus on the services: <i>Multiple Values</i>	List	Select one or more services.
Where Subscriber ID contains: <i>Specific Values</i>	Text	Pattern that represents group of subscribers.

Malicious Traffic Reports

Use the Malicious Traffic group of reports to view reports on the amount of security events detected by the OS.

Global Scan/Attack Rate

For a given time frame, Global Scan/Attack Rates shows the rate (session/sec) of scan/attacks originating from hosts (typically due to worm / zombie).

Table A-92 Global Scan/Attack Rate Template

Condition	Field Type	Comments
<i>IP-Protocol Single Value</i>	List	List of IP-Protocols (TCP,UDP,ICMP,Other).
<i>Initiating Side Single Value</i>	List	List of initiating sides (subscriber/network).

Global DoS Rate

For a given time frame Global DoS Rate shows the distribution of DoS between the different IP protocols defined in the system.

Table A-93 Global DoS Rate Template

Condition	Field Type	Comments
<i>IP-Protocol Single Value</i>	List	List of IP-Protocols (TCP,UDP,ICMP,Other).
<i>Initiating Side Single Value</i>	List	List of initiating sides (subscriber/network).

Top Scanning/Attacking Hosts

For a given time frame Top Scanning/Attacking Hosts, shows the top hosts identified as DoS attacked per initiating side (User/Network) and per protocol.

Table A-94 Top Scanning/Attacking Hosts Template

Condition	Field Type	Comments
<i>IP-Protocol Single Value</i>	List	List of IP-Protocols (TCP,UDP,ICMP,Other).
<i>Aggregate Metric Single Value</i>	List	List of Aggregated metrics (Attacks,Sessions,Duration)
<i>Initiating Side Single Value</i>	List	List of initiating sides (subscriber/network).

Top Scanning/Attacking Hosts

For a given time frame, Top Scanning/Attacking Subscribers shows the top subscribers identified as scanning / attacking. These subscribers typically have machines infected by worms / zombies.

Table A-95 Top Scanning/Attacking Subscribers Template

Condition	Field Type	Comments
Ordering Metric <i>Single Value</i>	List	List of Metric (Number of Attacks, Number of Malicious Sessions, Attack Duration [Minutes])
IP-Protocol <i>Single Value</i>	List	List of IP-Protocols (TCP,UDP,ICMP,Other).

Top DoS Attacked Hosts

For a given time frame Top DoS Attacked Hosts, shows the top hosts identified as DoS per initiating side (User/Network) and per protocol.

Table A-96 Top DoS Attacked Hosts Template

Condition	Field Type	Comments
<i>IP-Protocol Single Value</i>	List	List of IP-Protocols (TCP,UDP,ICMP,Other).
<i>Aggregate Metric Single Value</i>	List	List of Aggregated metrics (Attacks,Sessions,Duration)
<i>Initiating Side Single Value</i>	List	List of initiating sides (subscriber/network).

Top Scanning/Attacking Hosts

For a given time frame, Top DoS Attacked Subscribers shows the top subscribers identified as DoS attacked

Table A-97 Top DoS Attacked Subscribers Template

Condition	Field Type	Comments
Ordering Metric Single Value	List	List of Metric (Number of Attacks, Number of Malicious Sessions, Attack Duration [Minutes])

Infected Subscribers

For a given time frame, Infected Subscribers shows the distribution of suspected infected subscribers between the different IP protocol defined in the system.

Table A-98 Infected Subscribers Template

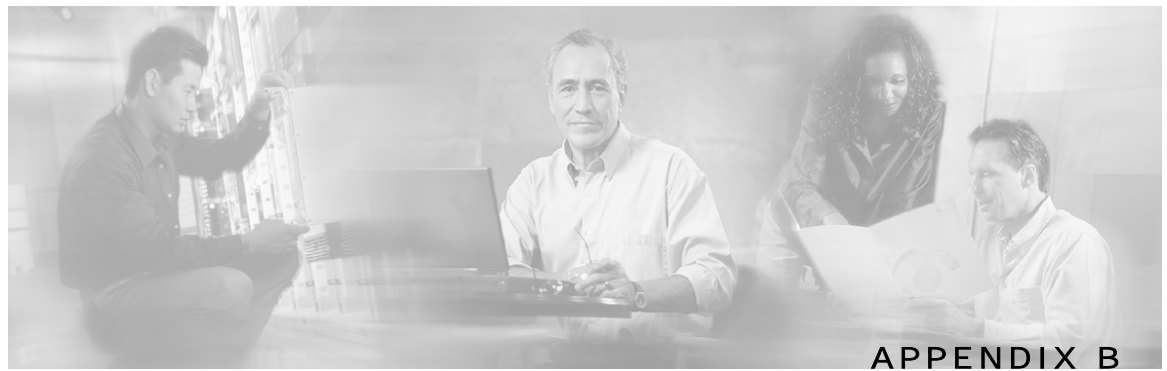
Condition	Field Type	Comments
IP-Protocol Single Value	List	List of IP-Protocols (TCP,UDP,ICMP,Other).

DoS Attacked Subscribers

For a given time frame, DoS Attacked Subscribers shows the distribution of DoS attacked Subscribers between the different IP protocol defined in the system

Table A-99 DoS Attacked Subscribers Template

Condition	Field Type	Comments
IP-Protocol Single Value	List	List of IP-Protocols (TCP,UDP,ICMP,Other).



Protocol Reference Tables

This chapter contains reference tables that relate to protocols in *SCAS BB* Service Configuration.

Generic Protocols

The three generic protocols (IP, TCP and UDP) serve as default containers for classifying transactions of the relevant type (IP, TCP or UDP) that were not classified to a more specific protocol.

A transaction is classified as belonging to one of the generic protocols if:

- Step 1** It was not classified as one of the signature-based protocols, **and**
- Step 2** It was not classified as one of the IP protocols or port-based protocols that were specifically mapped to a service.

Table B-1 **Generic Protocols**

Protocol name	Description
Generic IP	Holds for any non-TCP/UDP transaction, where the related IP protocol is not specifically mapped to a service.
Generic TCP	Holds for any TCP transaction, which does not match any signature-based protocol, and where the related port-based protocol (if exists) is not specifically mapped to a service.
Generic UDP	Holds for any UDP transaction, which does not match any signature-based protocol, and where the related port-based protocol (if exists) is not specifically mapped to a service.

Signature-based Protocols

A transaction is classified as belonging to one of the signature-based protocols if it is carried on the protocol's well-known port, and matches the protocol's signature.

Table B-2 **Signature-based Protocols**

Protocol Name	TCP Ports	UDP Ports
FTP	21	

HTTP Browsing	8080;80	
HTTP Streaming		
MMS	1755	
NNTP	119	
POP3	110	
RTSP Streaming	554;7070;1554	
SIP	5060;5061	5060;5061
Vonage		
SMTP	25	
H323	1720	
DHCP Sniff		
MGCP		2427;2727

In addition to the protocol's well-known ports, the sub-group of P2P signature-based protocols are also detected (according to their signature) on a configurable range of TCP/UDP ports:

Table B-3 Signature-based P2P Protocols

Protocol Name	TCP Ports	UDP Ports
BitTorrent	6881-6889;6969	
DirectConnect	413;412;411	
eDonkey	4672;4673;4661-4665;4711;5662;5773;5783	same as TCP
FastTrack KaZaA File Transfer		
FastTrack KaZaA Networking	1214	
Filetopia		
Gnutella File Transfer		
Gnutella Networking	6347;6346	
Hotline	5498;5503;5502;5501;5500	
iTunes		
Manolito		
Napster		
Share		
Skype	33033	
Soulseek		
WinMX/OpenNap	6699	6699
Winnie	7742-7745;7773	

Mute
 NodeZilla
 Waste
 NeoNet
 Ares/Warez

IP Protocols

This section lists the IP protocols supported by Service Control Application Suite for Broadband:

Table B-4 IP Protocols

IP protocol number (ascending order)	Protocol name
0	HOPOPT
1	ICMP
2	IGMP
3	GGP
4	IP
5	ST
6	TCP
7	CBT
8	EGT
9	IGP
10	BBN-RCC-MON
11	NVP-II
12	PUP
13	ARGUS
14	EMCON
15	XNET
16	CHAOS
18	MUX
19	DCN-MEAS
20	HMP
21	PRM
22	XNS-IDP
23	TRUNK-1
24	TRUNK-2

IP protocol number (ascending order)	Protocol name
25	LEAF-1
26	LEAF-2
27	RDP
28	IRTP
29	ISO-TP4
30	NETBLT
31	MFE-NSP
32	MERIT-INP
33	SEP
34	3PC
35	IDPR
36	XTP
37	DDP
38	IDPR-CMTP
39	TP++
40	IL
41	IPv6
42	SDRP
43	IPv6-ROUTE
44	IPv6-FRAG
45	IDRP
46	RSVP
47	GRE
48	MHRP
49	BNA
50	ESP
51	AH
52	I-NLSP
53	SWIPE
54	NARP
55	MOBILE
56	TLSP
57	SKIP
58	IPv6-ICMP

IP protocol number (ascending order)	Protocol name
59	IPv6-NONXT
60	IPv6-OPTS
62	CFTP
64	SAT-EXPAK
65	KRYPTOLAN
66	RVD
67	IPPC
69	SAT-MON
70	VISA
71	IPCV
72	CPNX
73	CPHB
74	WSN
75	PVP
76	BR-SAT-MON
77	SUN-ND
78	WB-MON
79	WB-EXPAK
80	ISO-IP
81	VMTP
82	SECURE-VMTP
83	VINES
84	TTP
85	NSFNET-IGP
86	DGP
87	TCF
88	EIGRP
89	OSPFIGP
90	SPRITE-RPC
91	LARP
92	MTP
93	AX.20
94	IPIP
95	MICP

IP protocol number (ascending order)	Protocol name
96	SCC-SP
97	ETHERIP
98	ENCAP
100	GMTP
101	IFMP
102	PNNI
103	PIM
104	ARIS
105	SCPS
106	QNX
107	A/N
108	IPCOMP
109	SNP
110	COMPAQ-PEER
111	IPX-IN-IP
112	VRRP
113	PGM
115	L2TP
116	DDX
117	IATP
118	STP
119	SRP
120	UTI
121	SMP
122	SM
123	PTP
124	ISIS
125	FIRE
126	C RTP

Port-Based Protocols

This section lists the TCP/UDP port-based protocols supported by Service Control Application Suite for Broadband default service configuration. Note that the existing port-based protocols can be modified and more port-based protocols can be added.

Table B-5 Port-based Protocols

Protocol Name	TCP Ports	UDP Ports
compressnet	3, 2	3, 2
rje	5	5
echo	7	7
discard	9	9
systat	11	11
daytime	13	13
qotd	17	17
misp	18	18
chargen	19	19
ftp-data	20	20
ssh	22	22
telnet	23	23
nsw-fe	27	27
msg-icp	29	29
msg-auth	31	31
dsp	33	33
time	37	37
rap	38	38
rlp	39	39
graphics	41	41
name	42	42
nickname	43	43
mpm-flags	44	44
mpm	45	45
mpm-snd	46	46
ni-ftp	47	47
auditd	48	48
tacacs	49	49
re-mail-ck	50	50

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
la-maint	51	51
xns-time	52	52
dns	53	53
xns-ch	54	54
isi-gl	55	55
xns-auth	56	56
xns-mail	58	58
ni-mail	61	61
acas	62	62
whois	63	63
covia	64	64
tacaacs-ds	65	65
sql*net	66	66
bootps	67	67
bootpc	68	68
tftp	69	69
gopher	70	70
netrjs-1	71	71
netrjs-2	72	72
netrjs-3	73	73
netrjs-4	74	74
deos	76	76
finger	79	79
hosts2-ns	81	81
xfer	82	82
mit-ml-dev	85, 83	85, 83
ctf	84	84
mfcobol	86	86
kerberos	88	88
su-mit-tg	89	89
dnsix	90	90
mit-dov	91	91
npp	92	92
dcp	93	93
objcall	94	94

Protocol Name	TCP Ports	UDP Ports
supdup	95	95
dixie	96	96
swift-rvf	97	97
tacnews	98	98
metagram	99	99
newacct	100	
hostname	101	101
iso-tsap	102	102
gppitnp	103	103
acr-nema	104	104
csnet-ns	105	105
3com-tsmux	106	106
rtelnet	107	107
snagas	108	108
pop2	109	109
sunrpc	111	111
mcidas	112	112
auth	113	113
audionews	114	114
sftp	115	115
ansanotify	116	116
uucp-path	117	117
sqlserv	118	118
cfdpkt	120	120
erpc	121	121
smakynet	122	122
ntp	123	123
ansatrader	124	124
locus-map	125	125
nxedit	126	126
locus-con	127	127
gss-xlicen	128	128
pwdgen	129	129
cisco-fna	130	130
cisco-tna	131	131

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
cisco-sys	132	132
statsrv	133	133
ingres-net	134	134
epmap	135	135
profile	136	136
netbios-ns	137	137
netbios-dgm	138	138
netbios-ssn	139	139
emfis-data	140	140
emfis-ctrl	141	141
bl-idm	142	142
imap	143	143
uma	144	144
uaac	145	145
iso-tp0	146	146
iso-ip	147	147
jargon	148	148
aed-512	149	149
sql-net	150	150
hems	151	151
bftp	152	152
sgmp	153	153
netsc-prod	154	154
netsc-dev	155	155
sqlsrv	156	156
knet-cmp	157	157
pcmail-srv	158	158
nss-routing	159	159
sgmp-traps	160	160
snmp	161	161
snmptrap	162	162
cmip-man	163	163
cmip-agent	164	164
xns-courier	165	165
s-net	166	166

Protocol Name	TCP Ports	UDP Ports
namp	167	167
rsvd	168	168
send	169	169
print-srv	170	170
multiplex	171	171
cl/1	172	172
xplex-mux	173	173
mailq	174	174
vmnet	175	175
genrad-mux	176	176
xmcp	177	177
nextstep	178	178
bgp	179	179
ris	180	180
unify	181	181
audit	182	182
ocbinder	183	183
ocserver	184	184
remote-kis	185	185
kis	186	186
aci	187	187
mumps	188	188
qft	189	189
gacp	190	190
prospero	191	191
osu-nms	192	192
srmp	193	193
irc	194	194
dn6-nlm-aud	195	195
dn6-smm-red	196	196
dls	197	197
dls-mon	198	198
smux	199	199
src	200	200
at-rtmp	201	201

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
at-nbp	202	202
at-3	203	203
at-echo	204	204
at-5	205	205
at-zis	206	206
at-7	207	207
at-8	208	208
qmtp	209	209
z39.50	210	210
914c/g	211	211
anet	212	212
ipx	213	213
vmpwscs	214	214
softpc	215	215
CAllic	216	216
dbase	217	217
mpp	218	218
uarps	219	219
imap3	220	220
fln-spx	221	221
rsh-spx	222	222
cdc	223	223
masqdiabler	224	224
direct	242	242
sur-meas	243	243
inbusiness	244	244
link	245	245
dsp3270	246	246
subntbcst_tftp	247	247
bhfh	248	248
set	257	257
yak-chat	258	258
esro-gen	259	259
openport	260	260
nsiiops	261	261

Protocol Name	TCP Ports	UDP Ports
arcisdms	262	262
hdap	263	263
bgmp	264	264
x-bone-ctl	265	265
sst	266	266
td-service	267	267
td-replica	268	268
http-mgmt	280	280
personal-link	281	281
cableport-ax	282	282
rescap	283	283
corerjd	284	284
fxp-1	286	286
k-block	287	287
novastorbakcup	308	308
entrusttime	309	309
bhmds	310	310
asip-webadmin	311	311
vslmp	312	312
magenta-logic	313	313
opalis-robot	314	314
dpsi	315	315
decauth	316	316
zannet	317	317
pkix-timestamp	318	318
ptp-event	319	319
ptp-general	320	320
pip	321	321
rtsps	322	322
texar	333	333
pdap	344	344
pawserv	345	345
zserv	346	346
fatserv	347	347
csi-sgwp	348	348

Protocol Name	TCP Ports	UDP Ports
mftp	349	349
matip-type-a	350	350
matip-type-b	351	351
dtag-ste-sb	352	352
ndsauth	353	353
bh611	354	354
datex-asn	355	355
cloanto-net-1	356	356
bhevent	357	357
shrinkwrap	358	358
nsrmp	359	359
scoi2odialog	360	360
semantix	361	361
srssend	362	362
rsvp_tunnel	363	363
aurora-cmgr	364	364
dtk	365	365
odmr	366	366
mortgageware	367	367
qbikgdp	368	368
rpc2portmap	369	369
codaaauth2	370	370
clearcase	371	371
ulistproc	372	372
legent-1	373	373
legent-2	374	374
hassle	375	375
nip	376	376
tnETOS	377	377
dsETOS	378	378
is99c	379	379
is99s	380	380
hp-collector	381	381
hp-managed-node	382	382
hp-alarm-mgr	383	383

Protocol Name	TCP Ports	UDP Ports
arns	384	384
ibm-app	385	385
asa	386	386
aurp	387	387
unidata-ldm	388	388
ldap		389
uis	390	390
synotics-relay	391	391
synotics-broker	392	392
meta5	393	393
embl-ndt	394	394
netware-ip	396	396
mptn	397	397
kryptolan	398	398
iso-tsap-c2	399	399
work-sol	400	400
ups	401	401
genie	402	402
decap	403	403
nced	404	404
nclD	405	405
imsp	406	406
timbuktu	407	407
prm-sm	408	408
prm-nm	409	409
decladebug	410	410
rmt		411
synoptics-trap		412
smsp		413
infoseek	414	414
bnet	415	415
silverplatter	416	416
onmux	417	417
hyper-g	418	418
ariell	419	419

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
smpte	420	420
ariel2	421	421
ariel3	422	422
opc-job-start	423	423
opc-job-track	424	424
icad-el	425	425
smartsdp	426	426
svrloc	427	427
ocs_cmu	428	428
ocs_amu	429	429
utmpsd	430	430
utmpcd	431	431
iasd	432	432
nnsd	433	433
mobileip-agent	434	434
mobilip-mn	435	435
dna-cml	436	436
comscm	437	437
dsfgw	438	438
dasp	439	439
sgcp	440	440
decvms-sysmgt	441	441
cvc_hostd	442	442
https	443	443
snpp	444	444
microsoft-ds	445	445
ddm-rdb	446	446
ddm-dfm	447	447
ddm-ssl	448	448
as-servermap	449	449
tserver	450	450
sfs-smp-net	451	451
sfs-config	452	452
creativeserver	453	453
contentserver	454	454

Protocol Name	TCP Ports	UDP Ports
creativepartnr	455	455
scohelp	457	457
appleqt	458	458
ampr-rcmd	459	459
skronk	460	460
datasurfsrv	461	461
datasurfsrvsec	462	462
alpes	463	463
kpasswd	464	464
url-rendezvous	465	465
digital-vrc	466	466
mylex-mapd	467	467
photuris	468	468
rcp	469	469
scx-proxy	470	470
mondex	471	471
ljk-login	472	472
hybrid-pop	473	473
tn-tl-w1	474	
tn-tl-w2		474
tn-tl-fd1	476	476
ss7ns	477	477
spsc	478	478
iafserver	479	479
iafdbase	480	480
ph	481	481
bgs-nsi	482	482
ulpnet	483	483
integra-sme	484	484
powerburst	485	485
avian	486	486
saft	487	487
gss-http	488	488
nest-protocol	489	489
micom-pfs	490	490

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
go-login	491	491
ticf-1	492	492
ticf-2	493	493
pov-ray	494	494
intecourier	495	495
pim-rp-disc	496	496
dantz	497	497
siam	498	498
iso-ill	499	499
isakmp	500	500
stmf	501	501
asa-appl-proto	502	502
intrinsic	503	503
citadel	504	504
mailbox-lm	505	505
ohimsrv	506	506
crs	507	507
xvttp	508	508
snare	509	509
fcp	510	510
passgo	511	511
exec	512	
biff		512
login	513	
who		513
shell	514	
syslog		514
printer	515	515
videotex	516	516
talk	517	517
ntalk	518	518
utime	519	519
efs	520	
router		520
ripng	521	521

Protocol Name	TCP Ports	UDP Ports
ulp	522	522
ibm-db2	523	523
ncp	524	524
timed	525	525
tempo	526	526
stx	527	527
custix	528	528
irc-serv	529	529
courier	530	530
conference	531	531
netnews	532	532
netwall	533	533
mm-admin	534	534
iiop	535	535
opalis-rdv	536	536
nmsp	537	537
gdomap	538	538
apertus-ldp	539	539
uucp	540	540
uucp-rlogin	541	541
commerce	542	542
klogin	543	543
kshell	544	544
appleqtcsrvr	545	545
dhcpv6-client	546	546
dhcpv6-server	547	547
idfp	549	549
new-rwho	550	550
cybercash	551	551
deviceshare	552	552
pirp	553	553
remotefs	556	556
openvms-sysipc	557	557
sdnskmp	558	558
teedtap	559	559

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
rmonitor	560	560
monitor	561	561
chshell	562	562
nntps	563	563
9pfs	564	564
whoami	565	565
streettalk	566	566
banyan-rpc	567	567
ms-shuttle	568	568
ms-rome	569	569
meter	571, 570	571, 570
sonar	572	572
banyan-vip	573	573
ftp-agent	574	574
vemmi	575	575
ipcd	576	576
vnas	577	577
ipdd	578	578
decbsrv	579	579
sntp-heartbeat	580	580
bdp	581	581
scc-security	582	582
philips-vc	583	583
keyserver	584	584
imap4-ssl	585	585
password-chg	586	586
submission	587	587
cal	588	588
eyelink	589	589
tns-cml	590	590
http-alt	591	591
eudora-set	592	592
http-rpc-epmap	593	593
tpip	594	594
cab-protocol	595	595

Protocol Name	TCP Ports	UDP Ports
smsd	596	596
ptenameservice	597	597
sco-websrvrmg3	598	598
acp	599	599
ipcserver	600	600
urm	606	606
nqs	607	607
sift-uft	608	608
npmp-trap	609	609
npmp-local	610	610
npmp-gui	611	611
hmmp-ind	612	612
hmmp-op	613	613
sshell	614	614
sco-inetmgr	615	615
sco-sysmgr	616	616
sco-dtmgr	617	617
dei-icda	618	618
digital-evm	619	619
sco-websrvrmgr	620	620
escp-ip	621	621
collaborator	622	622
aux_bus_shunt	623	623
cryptoadmin	624	624
dec_dlm	625	625
asia	626	626
passgo-tivoli	627	627
qmqp	628	628
3com-amp3	629	629
rda	630	630
ipp	631	631
bmpp	632	632
servstat	633	633
ginad	634	634
rlzdbase	635	635

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
ldaps	636	636
lanserver	637	637
mcns-sec	638	638
msdp	639	639
entrust-sps	640	640
repcmd	641	641
esro-emsdp	642	642
sanity	643	643
dwr	644	644
pssc	645	645
ldp	646	646
dhcp-failover	647	647
rrp	648	648
aminet	649	649
obex	650	650
ieee-mms	651	651
hello-port	652	652
repscmd	653	653
aodv	654	654
tinc	655	655
spmp	656	656
rmc	657	657
tenfold	658	658
mac-srvr-admin	660	660
hap	661	661
pftp	662	662
purenoise	663	663
secure-aux-bus	664	664
sun-dr	665	665
doom	666	666
disclose	667	667
mecomm	668	668
meregister	669	669
vacdsm-sws	670	670
vacdsm-app	671	671

Protocol Name	TCP Ports	UDP Ports
vpps-qua	672	672
cimplex	673	673
acap	674	674
dctp	675	675
vpps-via	676	676
vpp	677	677
ggf-ncp	678	678
mrm	679	679
entrust-aaas	680	680
entrust-aams	681	681
xfr	682	682
corba-iiop	683	683
corba-iiop-ssl	684	684
mdc-portmapper	685	685
hcp-wismar	686	686
asipregistry	687	687
realm-rusd	688	688
nmap	689	689
vatp	690	690
msexch-routing	691	691
hyperwave-isp	692	692
connendp	693	693
ha-cluster	694	694
ieee-mms-ssl	695	695
rushd	696	696
uuidgen	697	697
olsr	698	698
accessnetwork	699	699
elcsd	704	704
agentx	705	705
silc	706	706
borland-dsj	707	707
entrust-kmsh	709	709
entrust-ash	710	710
cisco-tdp	711	711

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
netviewdm1	729	729
netviewdm2	730	730
netviewdm3	731	731
netgw	741	741
netrcs	742	742
flexlm	744	744
fujitsu-dev	747	747
ris-cm	748	748
kerberos-adm	749	749
rfile	750	
kerberos-iv		750
pump	751	751
qrh	752	752
rrh	753	753
tell	754	754
nlogin	758	758
con	759	759
ns	760	760
rx	761	761
quotad	762	762
cycleserv	763	763
omserv	764	764
webster	765	765
phonebook	767	767
vid	769	769
cadlock	770	770
rtip	771	771
cycleserv2	772	772
submit	773	
notify		773
rpasswd	774	
acmaint_dbd		774
entomb	775	
acmaint_transd		775
wpages	776	776

Protocol Name	TCP Ports	UDP Ports
multiling-http	777	777
wpgs	780	780
concert	786	786
qsc		787
mdb_s_daemon	800	800
device	801	801
itm-mcell-s	828	828
pkix-3-ca-ra	829	829
dhcp-failover2	847	847
rsync	873	873
iclnet-locate	886	886
iclnet_svinfo	887	887
accessbuilder	888	888
omginitialrefs	900	900
smpnameres	901	901
ideafarm-chat	902	902
ideafarm-catch	903	903
xact-backup	911	911
ftps-data	989	989
ftps	990	990
nas	991	991
telnets	992	992
imaps	993	993
ircs	994	994
pop3s	995	995
vsinet	996	996
maitrd	997	997
busboy	998	
puparp		998
garcon	999	
applix		999
surf	1010	1010
iMesh	4326	4326
rmiactivation	1098	1098
rmiregistry	1099	1099

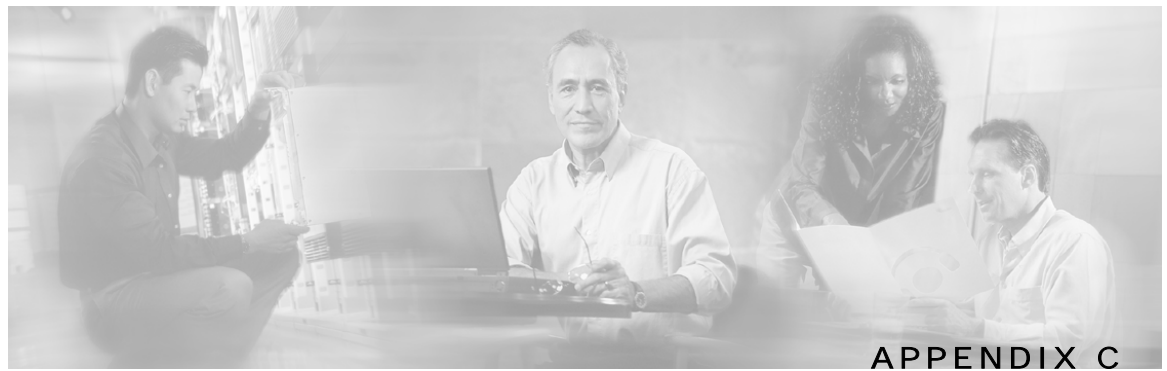
Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
ms-sql-s	1433	1433
ms-sql-m	1434	1434
ms-olap	2382, 2383, 2393, 2394	2382, 2383, 2393, 2394
msft-gc	3268	3268
msft-gc-ssl	3269	3269
ms-term-services	3389	3389
oracle	1521	1521
orasrv	1525	1525
tlisrv	1527	1527
coauthor	1529	1529
rdb-dbs-disp	1571	1571
oraclenames	1575	1575
oraclenet&cman	1630	1630
net&cman	1830	1830
citrixima	2512	2512
citrixadmin	2513	2513
citrix-rtmp	2897	2897
citriximaclient	2598	2598
micromuse-lm	1534	1534
orbixd	1570	1570
orbix-locator	3075	3075
orbix-config	3076	3076
orbix-loc-ssl	3077	3077
shockwave	1626	1626
sitaraserver	2629	2629
sitaramgmt	2630	2630
sitaradir	2631	2631
mysql	3306	3306
net-assistant	3283	3283
msnp	1836	1836
aim	5190, 5191, 5192, 5193	
groove	2492	2492
directplay	2234	2234
directplay8	6073	6073
kali	2213	2213

Protocol Name	TCP Ports	UDP Ports
worldfusion	2595, 2596	2595, 2596
directv-web	3334	3334
directv-soft	3335	3335
directv-tick	3336	3336
directv-catlg	3337	3337
sip-tls	5061	5061
wta-wsp-s	2805	2805
wap-push	2948	2948
wap-pushsecure	2949	2949
wap-push-http	4035	4035
wap-push-https	4036	4036
wap-wsp	9200	9200
wap-wsp-wtp	9201	9201
wap-wsp-s	9202	9202
wap-wsp-wtp-s	9203	9203
wap-vcard	9204	9204
wap-vcal	9205	9205
wap-vcard-s	9206	9206
wap-vcal-s	9207	9207
ibprotocol	6714	6714
radius	1812, 1813	1812, 1813
pptp	1723	1723
gtp-user	2152	2152
xctp	3088	3088
l2tp	1701	1701
fsgs	6112	6112
parsec-game	6582	6582
UnReal_UT	7778	7778
SiN	22450	22450
halflife		27015
tribes	28001	28001
heretic2	28910	
starsiege		29001, 29002, 29003, 29004, 29005, 29006, 29007, 29008, 29009
game-search	29001	

Port-Based Protocols

Protocol Name	TCP Ports	UDP Ports
KingPin	31510	31510
runescape	43594	
quake-server	27960	27960, 27910
game-spy	29000, 28900, 6500	6515, 27900



RDR Format and Field Content

Raw Data Records (RDRs), are the collection of fields that are sent by the SCE Platforms to the Collection Manager. This chapter contains a list of the RDRs produced by the SCE Platform and a full description of the fields contained in each RDR. This chapter also contains field-content information for those fields that are generated by Service Control components; for example, tags.

For brevity, fields that are common to many of the RDRs are described at the start of this chapter (see *Universal RDR Fields* (on page C-1)), prior to the description of the individual RDRs.

Universal RDR Fields

This section contains descriptions of the fields, in alphabetic order, that are common to many of the RDRs. However, the first two fields, `SUBSCRIBER_ID` and `PACKAGE_ID`, are universal fields that appear in almost all the RDRs.

- Step 1** `SUBSCRIBER_ID`: The subscriber identification string that was introduced through the subscriber management interfaces. It may contain up to 40 characters.
- Step 2** `PACKAGE_ID`: The ID of the Package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between **0** and **maximum number of packages**. The value **maximum number of packages** is reserved for unknown subscribers.
- Step 3** `ACCESS_STRING`: Layer 7 property extracted from the transaction. For possible values, see *PROTOCOL_ID (int16)* (on page C-24) in the per protocol `ACCESS_STRING` column.
- Step 4** `BREACH_STATE`: This field indicates whether the subscriber breached its quota: not breached (0) or breached (1).
- Step 5** `CLIENT_IP`: Contains the IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format.
- Step 6** `CLIENT_PORT`: For TCP/UDP-based sessions, this field contains the port number of the client side (initiator) of the networking session. For non-TCP/UDP sessions, this field has the value zero (0).
- Step 7** `CONFIGURED_DURATION`: For periodic RDRs, indicates the configured period, in seconds, between successive RDRs.
- Step 8** `INFO_STRING`: Layer 7 property extracted from the transaction. For possible values, see *PROTOCOL_ID (int16)* (on page C-24), in the per protocol `ACCESS_STRING` column.
- Step 9** `INITIATING_SIDE`: On which side of the SCE the initiator of the transaction resides: the subscriber side (0) or the network side (1).

Step 10 PROTOCOL_ID: This field contains a unique ID indicating the Protocol associated with the reported session. For field values, see *PROTOCOL_ID (int16)* (on page C-24), in the per protocol ACCESS_STRING column.



Note For Port-based protocols (for example, TCP port 666 for DOOM) and for IP-protocol-based protocols (for example, IP protocol 1 for ICMP), the PROTOCOL_ID will be of the TCP_GENERIC / UDP_GENERIC / IP_PROTOCOL values, according to the specific base protocol of the transaction.

Step 11 SERVER_IP: Contains the destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format.

Step 12 SERVER_PORT: For TCP/UDP-based sessions, this field contains the destination port number of the networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.

Step 13 SERVICE_ID: This field indicates the Service classification of the reported session. For example, in the Transaction RDR this field indicates which Service has been accessed, and in the Breaching RDR this field indicates which Service has been breached. Positive values specify the related Service Index as the ID.

Step 14 TIME_FRAME: The system supports time-dependent policies, by using different Rules for different time frames. This field indicates the time frame during which the RDR was generated. The field's value can be in the range 0 to 3, indicating which of the four possible time frames was used.

Step 15 TIMESTAMP: RDR timestamp. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

Transaction RDR

The TRANSACTION_RDR is generated at the end of an admitted session, according to a sampling mechanism configurable by the user. Configuring *number-of-transaction-RDRs-per-second* sets the number of transaction RDRs generated per-service per-second.

The RDR tag is **0xf0f0f010 / 4042321936**.

The following table lists the RDR fields and their descriptions.

Table C-1 Transaction RDR Fields

RDR Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1). For unknown-subscriber this field contains an empty string.
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVICE_ID	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Name	Type	Description
PROTOCOL_ID	INT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since last report.
SERVER_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
ACCESS_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INFO_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INITIATING_SIDE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
REPORT_TIME	UINT32	Ending timestamp of the report(GMT time). transaction reported in this RDR. The field is a UNIX time_t format, that is, the number of seconds since 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	UINT8	Indicates the time frame during which the RDR was generated.
SESSION_UPSTREAM_VOLUME	UINT32	Upstream volume of the admitted transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_VOLUME	UINT32	Downstream volume of the admitted transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Each service is mapped to a counter. There are 32 subscriber counters.
GLOBAL_COUNTER_ID	UINT16	Each service is mapped to a counter. There are 64 global counters.
PACKAGE_COUNTER_ID	UINT16	Each package is mapped to a counter. There are 64 counters.
IP_PROTOCOL	UINT8	IP Protocol Type

Transaction Usage RDR

The TRANSACTION_USAGE_RDR is generated at the end of an admitted session, for all transactions on packages and services that are configured to generate such an RDR (note that by default they are *disabled* from generating this RDR).



Note

This RDR is designed for services and packages where specific per transaction RDRs are required (for example, transaction level billing). As such, the characteristics of this RDR's generation scheme make it very sensitive to inadvertent, erroneous configuration: this RDR can be configured for generation upon each and every transaction, which may result in an excessive RDR rate. *Therefore, the generation scheme for this RDR should be configured with extra care.*

The RDR tag is **0xf0f0f012 / 4042321938**.

The following table lists the RDR fields and their descriptions.

Table C-2 Transaction Usage RDR Fields

RDR Fields	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVICE_ID	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PROTOCOL_ID	INT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since last report.
SERVER_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
ACCESS_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INFO_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INITIATING_SIDE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
REPORT_TIME	UINT32	Ending Timestamp of the report(GMT time). transaction reported in this RDR. The field is a UNIX time_t format, that is, the number of seconds since 1 January 1970.

RDR Fields	Type	Description
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	UINT8	Indicates time frame during which RDR was generated.
SESSION_UPSTREAM_VOLUME	UINT32	Upstream volume of the admitted transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_VOLUME	UINT32	Downstream volume of the admitted transaction, in bytes. The volume refers to the aggregated stream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Each service is mapped to a counter. there are 32 subscriber counters.
GLOBAL_COUNTER_ID	UINT16	Each service is mapped to a counter. there are 64 global counters.
PACKAGE_COUNTER_ID	UINT16	Each package is mapped to a counter. There are 64 counters.
IP_PROTOCOL	UINT8	IP protocol type

VoIP Transaction Usage RDR

The VOIP_TRANSACTION_USAGE_RDR is generated at the end of an admitted session, for all transactions on packages and services that are configured to generate such an RDR (note that by default they are disabled from generating this RDR). The VoIP Transaction Usage RDR is enabled automatically when the Transaction Usage RDR is enabled, therefore if triggered, both a Transaction Usage RDR and a VoIP Transaction Usage RDR will be generated when the session ends. Currently this RDR is generated for H323 sessions.



Note

This RDR is designed for services and packages where specific per transaction RDRs are required (for example, transaction level billing). As such, the characteristics of this RDR generation scheme make it very sensitive to inadvertent, erroneous configuration: this RDR can be configured for generation upon each and every transaction, which may result in an excessive RDR rate. Therefore, the generation scheme for this RDR should be configured with extra care.

The RDR tag is **0xf0f0f01 / 4042321940**.

The following table lists the RDR fields and their descriptions.

Table C-3 VoIP Transaction RDR Fields

RDR Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1). For unknown-subscriber this field contains an empty string.
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Name	Type	Description
SERVICE_ID	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PROTOCOL_ID	INT176	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
ACCESS_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INFO_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INITIATING_SIDE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
REPORT_TIME	UINT32	Ending Timestamp of the report(GMT time). transaction reported in this RDR. The field is a UNIX time_t format, that is, the number of seconds since 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	UINT8	Indicates the time frame during which the RDR was generated.
SESSION_UPSTREAM_VOLUME	UINT32	Upstream volume of the admitted transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_VOLUME	UINT32	Downstream volume of the admitted transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Each service is mapped to a counter. There are 32 subscriber counters.
GLOBAL_COUNTER_ID	UINT16	Each Service is mapped to a counter. There are 64 global counters.
PACKAGE_COUNTER_ID	UINT16	Each package is mapped to a counter. There are 64 counters.
APPLICATION_ID	UINT32	The ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.

RDR Name	Type	Description
UPSTREAM_PACKET_LOSS	UINT16	The average fractional upstream packet loss for the session. A value of 0xFFFF indicates that this field was not available (no RTCP flows were opened).
DOWNSTREAM_PACKET_LOSS	UINT16	The average fractional downstream packet loss for the session. A value of 0xFFFF indicates that this field was not available (no RTCP flows were opened).
UPSTREAM_AVERAGE_JITTER	UINT32	The average upstream jitter for the session in milliseconds. A value of 0xFFFFFFFF indicates that this field was not available (no RTCP flows were opened).
DOWNSTREAM_AVERAGE_JITTER	UINT32	The average downstream jitter for the session in milliseconds. A value of 0xFFFFFFFF indicates that this field was not available (no RTCP flows were opened).
CALL_DESTINATION	STRING	The Q931 Alias address of the session destination. A value of N/A indicates that this field was not found in the traffic.
CALL_SOURCE	STRING	The Q931 Alias address of the session source. A value of N/A indicates that this field was not found in the traffic.
UPSTREAM_PAYLOAD_TYPE	UINT8	The upstream RTP payload type for the session. A value of 0xFF indicates that this field was not available (no RTP flows were opened).
DOWNSTREAM_PAYLOAD_TYPE	UINT8	The downstream RTP payload type for the session. A value of 0xFF indicates that this field was not available (no RTP flows were opened).
CALL_TYPE	UINT8	The call type. A value of 0xFF indicates that this field was not available (no RTP flows were opened).
MEDIA_CHANNELS	UINT8	The number of data flows that were opened during the session.
IP_PROTOCOL	UINT8	IP Protocol Type

Subscriber Usage RDR



Note

A Subscriber Usage RDR will be generated *only* for those subscribers **whose policy requires the generation of such an RDR**.

At fixed, user-configurable time intervals (for example, every 30 minutes), there is a periodic SUBSCRIBER_USAGE_RDR generation point in time. Whether or not a Subscriber Usage RDR *for a particular subscriber* is actually generated depends on the following:

- If the subscriber consumed resources associated with the Service since the previous RDR generation point in time, a Subscriber Usage RDR is generated now at this current generation point in time.
- If the subscriber did *not* consume resources associated with the Service since the previous RDR generation point in time, *no* Subscriber Usage RDR is generated now.

Note, however, that the generation logic for Subscriber Usage RDRs uses zeroing methodology (as described in *Periodic RDR Zero Adjustment Mechanism* (on page C-27)).

Therefore, if the subscriber consumes resources associated with the Service at some later time, this will cause the *immediate* generation of either one or two zero-consumption Subscriber Usage RDRs. (This is in addition to the eventual generation of the Subscriber Usage RDR associated with this latest occurrence of subscriber consumption of resources).

- If there was only one time interval (for example, 0830–0900) for which there was no subscriber consumption of resources, only one zero-consumption Subscriber Usage RDR is generated.
- If there were multiple consecutive time intervals (for example, 0830–0900, 0900–0930, 0930–1000, 1000–1030) for which there was no subscriber consumption of resources, two zero-consumption Subscriber Usage RDR are generated: one for the first such time interval (0830–0900) and one for the last (1000–1030).

In addition, a Subscriber Usage RDR may be generated in the following situation:

- The subscriber performed a logout in a subscriber-integrated installation or was un-introduced from the SCE Platform. If the subscriber consumed resources associated with the Service since the previous Subscriber Usage RDR, a Subscriber Usage RDR is generated now. If the subscriber did not consume resources since the previous RDR, no RDR is generated for that Service.

The RDR tag is **0xf0f0f000 / 4042321920**.

The following table lists the RDR fields and their descriptions.

Table C-4 Subscriber Usage RDR

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	INT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Field Name	Type	Description
SERVICE_USAGE_COUNTER_ID	UINT16	Each service is mapped to a counter. There are 32 counters in the subscriber scope.
BREACH_STATE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1). Holds the breach state of a service. However, NUR reports usage counters, which cannot be breached.
REASON	UINT8	Reason for RDR generation: <ul style="list-style-type: none"> • 0- Period time passed • 1- Subscriber Logout • 2- Package Switch • 3- Wraparound • 4- End of aggregation period
CONFIGURED_DURATION	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
DURATION	UINT32	Indicates the number of seconds that have passed since the previous SUBSCRIBER_USAGE_RDR. (Always the same as CONFIGURED_DURATION)
END_TIME	UINT32	Ending timestamp (GMT time) of the period during which aggregated information is reported in this RDR. The field is in UNIX time_t format, that is, the number of seconds since 1 January 1970.
UPSTREAM_VOLUME	UINT32	Change from the last report in aggregated upstream volume on both links of all sessions, in kilobytes.
DOWNSTREAM_VOLUME	UINT32	Change from the last report in aggregated downstream volume on both links of all sessions, in kilobytes.
SESSIONS	UINT16	Change from the last report in aggregated number of sessions for the reported Service.
SECONDS	UINT16	Change from the last report in aggregated number of session seconds for the reported Service.

Real-time Subscriber Usage RDR



Note

A Real-time Subscriber Usage RDR will be generated only for those subscribers who are identified by the system as being currently online.

At fixed, user-configurable time intervals (for example, every 5 minutes), there is a periodic `REALTIME_SUBSCRIBER_USAGE_RDR` generation point in time. The `REALTIME_SUBSCRIBER_USAGE_RDR` reports the same usage numbers as the `SUBSCRIBER_USAGE_RDR`, but is generated more frequently to provide a more detailed picture of the subscriber activity.

Whether or not a Real-time Subscriber Usage RDR *for a particular subscriber* is actually generated depends on the following:

- If the subscriber consumed resources associated with the Service since the previous RDR generation point in time, a Real-time Subscriber Usage RDR is generated now at this current generation point in time.
- If the subscriber did *not* consume resources associated with the Service since the previous RDR generation point in time, *no* Real-time Subscriber Usage RDR is generated now.

Note, however, that the generation logic for Real-time Subscriber Usage RDRs uses zeroing methodology (as described in *Periodic RDR Zero Adjustment Mechanism* (on page C-27)).

Therefore, if the subscriber consumes resources associated with the Service at some later time, this will cause the *immediate* generation of either one or two zero-consumption Real-time Subscriber Usage RDRs. (This is in addition to the eventual generation of the Real-time Subscriber Usage RDR associated with this latest occurrence of subscriber consumption of resources).

- If there was only one time interval (for example, 0805–0810) for which there was no subscriber consumption of resources, only one zero-consumption Real-time Subscriber Usage RDR is generated.
- If there were multiple consecutive time intervals (for example, 0805–0810, 0810–0815, 0815–0820, 0820–0825) for which there was no subscriber consumption of resources, two zero-consumption Real-time Subscriber Usage RDR are generated: one for the first such time interval (0805–0810) and one for the last (0820–0825).

In addition, a Real-time Subscriber Usage RDR may be generated in the following situation:

- The subscriber performed a logout in a subscriber-integrated installation or was un-introduced from the SCE Platform. If the subscriber consumed resources associated with the Service since the previous Real-time Subscriber Usage RDR, a Real-time Subscriber Usage RDR is generated now. If the subscriber did not consume resources since the previous RDR, no RDR is generated for that Service.

The RDR tag is `0xf0f0f002 / 4042321922`.

The following table lists the RDR fields and their descriptions.

Table C-5 Real-time Subscriber Usage RDR Fields

RDR Field Name	Type	Description
<code>SUBSCRIBER_ID</code>	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
<code>PACKAGE_ID</code>	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
<code>SERVICE_USAGE_COUNTER_ID</code>	UINT16	Each service is mapped to a counter. There are 32 counters in the subscriber scope.

RDR Field Name	Type	Description
AGGREGATION_OBJECT_ID	INT16	Externally assigned <ul style="list-style-type: none"> • 0: Offline subscriber • 1: Online subscribers
BREACH_STATE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1). Holds the breach state of a service. However, NUR reports usage counters, which cannot be breached.
REASON	UINT8	Reason for RDR generation: <ul style="list-style-type: none"> • 0- Period time passed • 1- Subscriber Logout • 2- Package Switch • 3- Wraparound • 4- End of aggregation period
CONFIGURED_DURATION	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
DURATION	UINT32	Indicates the number of seconds that have passed since the previous SUBSCRIBER_USAGE_RDR. (Always the same as CONFIGURED_DURATION.)
END_TIME	UINT32	Ending timestamp (GMT time) of the period during which aggregated information is reported in this RDR. The field is in UNIX time_t format, that is, the number of seconds since 1 January 1970.
UPSTREAM_VOLUME	UINT32	Change from the last report in aggregated upstream volume on both links of all sessions, in kilobytes.
DOWNSTREAM_VOLUME	UINT32	Change from the last report in aggregated downstream volume on both links of all sessions, in kilobytes.
SESSIONS	UINT16	Change from the last report in aggregated number of sessions for the reported Service.
SECONDS	UINT16	Change from the last report in aggregated number of session seconds for the reported Service

Link Usage RDR

At fixed, user-configurable time intervals (for example, every 30 minutes), there is a periodic LINK_USAGE_RDR generation point in time. Whether or not a Link Usage RDR is actually generated depends on the following:

- If network resources associated with the Service have been consumed since the previous RDR generation point in time, a Link Usage RDR is generated now at this current generation point in time.

- If network resources associated with the Service have *not* been consumed since the previous RDR generation point in time, *no* Link Usage RDR is generated now.

Note, however, that the generation logic for Link Usage RDRs uses zeroing methodology (as described in *Periodic RDR Zero Adjustment Mechanism* (on page C-27)).

Therefore, if network resources associated with the Service are once again consumed at some later time, this will cause the *immediate* generation of either one or two zero-consumption Link Usage RDRs. (This is in addition to the eventual generation of the Link Usage RDR associated with this latest consumption of network resources).

- If there was only one time interval (for example, 0830–0900) for which there was no consumption of network resources, only one zero-consumption Link Usage RDR is generated.
- If there were multiple consecutive time intervals (for example, 0830–0900, 0900–0930, 0930–1000, 1000–1030) for which there was no consumption of network resources, two zero-consumption Link Usage RDR are generated: one for the first such time interval (0830–0900) and one for the last (1000–1030).



Note

A *separate* RDR is generated for *each link* (on a single traffic processor) within the SCE device, where each RDR represents the total traffic processed and analyzed by that processor. To compute the total traffic in any given time frame, take the sum of the RDRs of all the processors. (A traffic processor that did not process traffic of a certain type will not generate the corresponding RDR.)

The RDR tag is **0xf0f0f005 / 4042321925**.

The following table lists the RDR fields and their descriptions.

Table C-6 Link Usage RDR Fields

RDR Field Name	Type	Description
LINK_ID	INT8	A numeric value associated with the reported network link. Possible values are 0 and 1 (referring to physical links 1 and 2 respectively). For future use.
GENERATOR_ID	UINT32	A numeric value identifying the processor generating the RDR. Possible values are 0 through 3.
SERVICE_USAGE_COUNTER_ID	UINT16	Each service is mapped to a counter. There are 64 global counters.
CONFIGURED_DURATION	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
DURATION	UINT32	Indicates the number of seconds that have passed since the previous LINK_USAGE_RDR.
END_TIME	UINT32	Ending timestamp (GMT time) of the period during which aggregated information is reported in this RDR. The field is in UNIX time_t format, that is, the number of seconds since 1 January 1970.

RDR Field Name	Type	Description
UPSTREAM_VOLUME	UINT32	Change from the last report in aggregated upstream volume of all sessions, in kilobytes.
DOWNSTREAM_VOLUME	UINT32	Change from the last report in aggregated downstream volume of all sessions, in kilobytes.
SESSIONS	UINT32	Change from the last report in aggregated number of sessions for the reported Service.
SECONDS	UINT32	Change from the last report in aggregated number of session seconds for the reported Service.
CONCURRENT_SESSIONS	UINT32	Concurrent number of sessions
ACTIVE_SUBSCRIBERS	UINT32	Concurrent number of subscribers using the reported Service at this point in time
TOTAL_ACTIVE_SUBSCRIBERS	UINT32	Concurrent number of subscribers in the system at this point in time

Package Usage RDR

The PACKAGE_USAGE_RDR aggregates network usage information for all subscribers of the same package.



Note

A Package Usage RDR will be generated *only* for those packages **that are configured to generate such an RDR**.

At fixed, user-configurable time intervals (for example, every 5 minutes), there is a periodic PACKAGE_USAGE_RDR generation point in time. Whether or not a Package Usage RDR is actually generated depends on the following:

- If network resources associated with the Service have been consumed by a subscriber of the Package since the previous RDR generation point in time, a Package Usage RDR is generated now at this current generation point in time.
- If a subscriber of the Package has not consumed network resources associated with the Service since the previous RDR generation point in time, *no* Package Usage RDR is generated now.

Note, however, that the generation logic for Package Usage RDRs uses zeroing methodology (as described in *Periodic RDR Zero Adjustment Mechanism* (on page [C-27](#))).

Therefore, if network resources associated with the Service are once again consumed by a subscriber of the Package at some later time, this will cause the *immediate* generation of either one or two zero-consumption Package Usage RDRs. (This is in addition to the eventual generation of the Package Usage RDR associated with this latest consumption of network resources by a subscriber of the Package).

- If there was only one time interval (for example, 0805–0810) for which there was no consumption of network resources by a subscriber of the Package, only one zero-consumption Package Usage RDR is generated.
- If there were multiple consecutive time intervals (for example, 0805–0810, 0810–0815, 0815–0820, 0820–0825) for which there was no consumption of network resources by a subscriber of the Package, two zero-consumption Package Usage RDR are generated: one for the first such time interval (0805–0810) and one for the last (0820–0825).

**Note**

Each traffic processor within the SCE platform generates a separate RDR, where each RDR represents the total traffic processed and analyzed by that processor. To compute the total traffic (for a package) in any given time frame, take the sum of the RDRs of all the processors. (A traffic processor that did not process traffic of a certain type will not generate the corresponding RDR.)

The RDR tag is **0xf0f0f004 / 4042321924**.

The following table lists the RDR fields and their descriptions.

Table C-7 Package Usage RDR Fields

RDR Field Name	Type	Description
PACKAGE_ID	UINT16	A universal field; see “ <i>Universal RDR Fields</i> (on page C-1).
GENERATOR_ID	UINT32	A numeric value identifying the processor generating the RDR.
SERVICE_USAGE_COUNTER_ID	UINT16	Each service is mapped to a counter. There are 64 global counters.
CONFIGURED_DURATION	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
DURATION	UINT32	Indicates the number of seconds that have passed since the previous PACKAGE_USAGE_RDR. (Always the same as CONFIGURED_DURATION.)
END_TIME	UINT32	Ending timestamp (GMT time) of the period during which aggregated information is reported in this RDR. The field is in UNIX time_t format, that is, the number of seconds since 1 January 1970.
UPSTREAM_VOLUME	UINT32	Change from the last report in aggregated upstream volume on both links (for a single processor) of all sessions, in kilobytes.

RDR Field Name	Type	Description
DOWNSTREAM_VOLUME	UINT32	Change from the last report in aggregated downstream volume on both links (for a single processor) of all sessions, in kilobytes.
SESSIONS	UINT32	Change from the last report in aggregated number of sessions for the reported Service.
SECONDS	UINT32	Change from the last report in aggregated number of session seconds for the reported Service.
CONCURRENT_SESSIONS	UINT32	Concurrent number of sessions
ACTIVE_SUBSCRIBERS	UINT32	Concurrent number of subscribers using the reported Service at this point in time
TOTAL_ACTIVE_SUBSCRIBERS	UINT32	Concurrent number of subscribers in the system at this point in time

Blocking RDR

The `SERVICE_BLOCK_RDR` is generated each time a transaction is blocked, and the profile and rate/quota limitations indicate that this RDR should be generated.

Note the following regarding RDR generation:

- This RDR is generated when a session is blocked. A session can be blocked for various reasons; for example, access is blocked or concurrent session limit has been reached.
- Generation of this RDR is subject to two requirements—a quota and a rate—as follows:
 - Quota. Each subscriber has a maximum quota of Block RDRs that can be generated for that subscriber in a specific aggregation period (day, week, month, etc.). The quota is package-dependent; that is, its value is set according to the Package assigned to the subscriber.
 - Rate. The rate is a global, per-box, maximum number of Block RDRs that can be generated per second. The rate is a global value that sets an upper limit for the total number of RDRs to be generated for all subscribers.

The RDR tag is **0xf0f0f040 / 4042321984**.

The following table lists the RDR fields and their descriptions.

Table C-8 Blocking RDR (`SERVICE_BLOCK_RDR`) Fields

RDR Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Name	Type	Description
SERVICE_ID	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PROTOCOL_ID	INT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INITIATING_SIDE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
ACCESS_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INFO_STRING	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
BLOCK_REASON	UINT8	Indicates the reason why this session was blocked. See, in <i>Block Reason (uint8)</i> (on page C-23), the table Block Reason Field Bit Values, for possible values and their interpretation.
BLOCK_RDR_COUNT	UINT32	Total number of blocked flows reported so far (from the beginning of the current time frame).
REDIRECTED	UINT8	Indicates whether the flow has been redirected (1) or not (0), after being blocked. Redirection will take place only for HTTP and RTSP flows, which were mapped to a Rule ordering to block and redirect them.
REPORT_TIME	UINT32	Ending timestamp of the report(GMT time).

Quota Provision RDR

The QUOTA_PROVISION_RDR is generated each time a bucket is breached for the first time in a session.

This RDR is directed to the non-default RDR category. It is important to note that one must configure the RDR destination of this category in order to get the RDRs

```
(SE1000(config)#> RDR-formatter destination x.x.x.x <port number> category 2
```

This RDR is not limited by a rate limit; it is generated whenever a quota breach occurs, provided that the RDR is enabled.

This RDR is generated subject to the following conditions:

- One of the Subscriber's buckets was depleted.
- Quota Breach RDRs are enabled.
- This is the first time this subscriber has breached this bucket.

The RDR tag is **0xf0f0f022 / 4042321954**.

The following table lists the RDR fields and their descriptions.

Table C-9 Quota Breach RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
BUCKET_BREACHED_ID	UINT8	1-16, according to the number of the breached bucket
END_TIME	UINT32	Time stamp of the report generation (GMT time)
BUCKET_QUOTA	INT32	The remaining quota in the indicated bucket: <ul style="list-style-type: none"> • Volume bucket: in Kbytes • Number of sessions bucket: integer
AGGREGATION_PERIOD_TYPE	UINT8	Defines how often the bucket is refilled. See, <i>Aggregation period</i> (" Aggregation Period (uint8) " on page C-25) for possible values and their interpretation.

Remaining Quota RDR



Note

A Quota Threshold RDR will be generated only for those subscribers **whose policy requires the generation of such an RDR**

At fixed, user-configurable time intervals (for example, every 30 minutes), there is a periodic REMAINING_QUOTA_RDR generation point in time. If the REMAINING_QUOTA_RDRs are enabled, they will be generated at the specified points in time.

The user can set total limit enforcement on the number of these RDRs per second.

This RDR is also generated after a subscriber performed a logout in a subscriber-integrated installation or was un-introduced from the SCE Platform, or when the subscriber's packag-ID is changed.

This RDR is directed to the non-default RDR category. It is important to note that one must configure the RDR destination of this category in order to get the RDRs

```
(SE1000(config)#> RDR-formatter destination x.x.x.x <port number> category 2
```

The RDR tag is **0xf0f0f030 / 4042321968**.

The following table lists the RDR fields and descriptions.

Table C-10 Remaining Quota RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Field Name	Type	Description
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
RDR_REASON	UINT8	<ul style="list-style-type: none"> • 0- Period time passed • 1- Logout • 2- Package Switch • 3- Wraparound • 4- End of aggregation period
END_TIME	UINT32	Timestamp of RDR generation.
REMAINING_QUOTA_1	INT32	The remaining quota in the bucket that was breached, in Kbytes.
REMAINING_QUOTA_16		There are sixteen Remaining Quota fields, one for each bucket.
TOTAL_VOLUME_USAGE	UINT32	Change from the last report in Total Volume Usage for all services that are not quota provisioned, in Kbytes.

Threshold Breach RDR

The THRESHOLD BREACH_RDR is generated each time a bucket exceeds the global threshold.

This RDR is directed to the non-default RDR category. It is important to note that one must configure the RDR destination of this category in order to get the RDRs

```
(SE1000(config)#> RDR-formatter destination x.x.x.x <port number> category 2
```

This RDR is not limited by a rate limit; it is generated whenever a threshold is exceeded, provided that the RDR is enabled.

The RDR tag is **0xf0f0f022 / 4042321969**.

The following table lists the RDR fields and their descriptions.

Table C-11 Threshold Breach RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
BUCKET_BREACHED_ID	UINT8	1-16, according to the number of the breached bucket
GLOBAL_THRESHOLD	UINT32	The globally configured threshold in Kbytes
END_TIME	UINT32	Time stamp of the report generation (GMT time)
BUCKET_QUOTA	INT32	The remaining quota in the indicated bucket in Kbytes.

DHCP RDR



Note

DHCP RDRs are generated only if DHCP ports (67 and 68 UDP) are assigned to the DHCP Sniff Protocol in the current service configuration.

To activate DHCP RDRs in the SCAS BB Console:

Step 1. Go to **Configuration à Protocols**

Step 2. Remove the port numbers 67 and 68 from the protocols 'bootps' and 'bootpc'.

Step 3. Find the protocol "DHCP Sniff".

Step 4. Assign the UDP ports 67 and 68 to the DHCP Sniff Protocol.

Step 5. Close the dialog.

Step 6. Apply the modified service configuration.

DHCP RDR is generated each time a DHCP message of certain type is intercepted. What DHCP message types will be intercepted is configurable.

For each message read, Service Control Application Suite for Broadband extracts several option fields. Again, the options to extract are configurable. RDR will be generated even if none of the options were extracted.

This RDR is directed to the non-default RDR category. It is important to note that one must configure the RDR destination of this category in order to get the RDRs

```
SE(config)#> RDR-formatter destination x.x.x.x <port number> category 3
```

The RDR tag is **0xf0f0f042 / 4042321986**

The following table lists the RDR fields and descriptions.

Table C-12 DHCP RDR Fields

RDR Field Name	Type	Description
CPE_MAC	STRING	A DHCP protocol field
CMTS_IP	UINT32	A DHCP protocol field
ASSIGNED_IP	UINT32	A DHCP protocol field
RELEASED_IP	UINT32	A DHCP protocol field
TRANSACTION_ID	UINT32	A DHCP protocol field
MESSAGE_TYPE	UINT8	DHCP message type
OPTION_TYPE_0/ through OPTION_TYPE_7/	UINT8	A list of DHCP options extracted from the message.
OPTION_VALUE_0 through OPTION_VALUE_7	STRING	The values associated with the above DHCP options.
END_TIME	UINT32	Timestamp of RDR generation.

QOS Request RDR

The QOS_REQUEST_RDR is generated at the beginning of a flow for all flows on packages and services that are configured to generate such an RDR. The QOS_REQUEST_RDR will be generated for services that are configured to generate TRANSACTION_USAGE_RDR. It is possible to decide if both RDRs are generated or just one of them. (By default only TRANSACTION_USAGE_RDR is generated).

This RDR is directed to the non-default RDR category. It is important to note that one must configure the RDR destination of this category in order to get the RDRs

```
SE(config)#> RDR-formatter destination x.x.x.x <port number> category 2
```



Note

This RDR is designed for services and packages where specific per transaction RDRs are required (for example, higher Quality of Service). As such, the characteristics of this RDR's generation scheme make it very sensitive to inadvertent erroneous configuration: this RDR can be configured for generation upon each and every transaction, which may result in an excessive RDR rate. *Therefore, the generation scheme for this RDR should be configured with extra care.*

The RDR tag is **0xf0f0f016 / 4042321942**.

The following table lists the RDR fields and their descriptions.

Table C-13 QOS Request RDR Fields

RDR Fields	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVICE_ID	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PROTOCOL_ID	INT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INITIATING_SIDE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
START_TIME	UINT32	Flow start time

RDR Fields	Type	Description
REPORT_TIME	UINT32	Timestamp of the report (GMT time).

QOS Delete RDR

The QOS_DELETE_RDR is generated at the end of a flow, for all flows that had generated QOS_REQUEST_RDR in their beginning.

This RDR is directed to the non-default RDR category. It is important to note that one must configure the RDR destination of this category in order to get the RDRs.

```
SE(config)#> RDR-formatter destination x.x.x.x <port number> category 2
```



Note

This RDR is designed for services and packages where specific per transaction RDRs are required (for example, higher Quality of Service). As such, the characteristics of this RDR's generation scheme make it very sensitive to inadvertent, erroneous configuration: this RDR can be configured for generation upon each and every transaction, which may result in an excessive RDR rate. *Therefore, the generation scheme for this RDR should be configured with extra care.*

The RDR tag is **0xf0f0f018 / 4042321944**.

The following table lists the RDR fields and their descriptions.

Table C-14 QOS Delete RDR Fields

RDR Fields	Type	Description
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PACKAGE_ID	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVICE_ID	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
PROTOCOL_ID	INT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
SERVER_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_IP	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
CLIENT_PORT	UINT16	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
INITIATING_SIDE	UINT8	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Fields	Type	Description
START_TIME	UINT32	Flow start time
REPORT_TIME	UINT32	Timestamp of the report (GMT time).

Malicious Traffic Periodic RDR

At fixed, user-configurable time intervals (for example, every 5 minutes), there is a periodic MALICIOUS_TRAFFIC_PERIODIC_RDR generation point in time. The MALICIOUS_TRAFFIC_PERIODIC_RDR reports the details of a certain attack or malicious traffic every period in time.

Before the first report of the attack, a zeroing report will be initiated. When an attack ends, a report of the consumed resources since last report is sent, and then a zeroing report, indicating the attack ended.

The RDR tag is **0xf0f0f050 / 4042322000**.

The following table lists the RDR fields and their descriptions.

Table C-15 Malicious Traffic Periodic RDR Fields

RDR Field Name	Type	Description
ATTACK_ID_HIGH	UINT32	Unique attack ID. A 64 bit field divided into two UINT32 fields.
ATTACK_ID_LOW	UINT32	
SUBSCRIBER_ID	STRING	A universal field; see <i>Universal RDR Fields</i> (on page C-1).
ATTACK_IP	UINT32	The IP address related to this attack.
ATTACK_TYPE	UINT32	Whether the IP address in the previous field is: <ul style="list-style-type: none"> • attacker: 1 • attacked: 0
SIDE	UINT32	The relevant IP address side: <ul style="list-style-type: none"> • Network: 1 • Subscriber: 0
IP_PROTOCOL	UINT8	IP Protocol Type: <ul style="list-style-type: none"> • 0 – ICMP • 1 – UDP • 2 – TCP • 3 – OTHER
CONFIGURED_DURATION	UINT32	A universal field; see <i>Universal RDR Fields</i> (on page C-1).

RDR Field Name	Type	Description
DURATION	UINT32	Indicates the number of seconds that have passed since the previous MALICIOUS_TRAFFIC_RDR. (will differ from the configured-duration at the end of the attack, since the handler will be invoked)
END_TIME	UINT32	Ending timestamp (GMT time) of the period during which aggregated information is reported in this RDR.
ATTACKS	UINT8	Change from the last report in attacks number. Since this report is per attack, can be 0 or 1.
MALICIOUS_SESSIONS	UINT32	Change from the last report in aggregated number of sessions for the reported Attack.

RDR Enumeration Fields

Following is a description of possible values for the RDR enumeration fields.

Block Reason (uint8)

The BLOCK_REASON field can be interpreted as a bit field. The following table lists the possible values of the field separated into bits.

Table C-16 Block Reason Field Bit Values

Bits number	Value Description
7 (msb)	Always ON.
6	0: Indicates the block is an admitted block. 1 : Indicates concurrent sessions limit block.
5	0: Indicates the effective Rule was in pre-breach state. 1: Indicates the effective Rule was in post-breach state.
4	Indicates the number of the breached bucket (1-16).
3	Indicates the number of the breached bucket (1-16).
2	Indicates the number of the breached bucket (1-16).
1	Indicates the number of the breached bucket (1-16).
0 (lsb)	Indicates the number of the breached bucket (1-16).

PROTOCOL_ID (int16)

The following table contains the PROTOCOL_ID field values. For additional information, see the *Protocol Support* appendix.

Table C-17 PROTOCOL_ID Field Values

Name	ID Value	TR ACCESS_STRIN G	TR INFO_STRIN G	Description
PROTOCOL_TCP_GENERIC	0	Null	Null	
PROTOCOL_UDP_GENERIC	1	Null	Null	
PROTOCOL_HTTP_BROWSI NG	2	Host name	URL	
PROTOCOL_HTTP_STREAMI NG	3	Host Name	URL	
PROTOCOL_FTP	4	Null	Null	
PROTOCOL_RTSP	5	Host name	Null	
PROTOCOL_MMS	6	Null	Null	
PROTOCOL_PROXY_HTTP	7	Host name	Null	
PROTOCOL_SMTP	8	Server IP	Sender	
PROTOCOL_POP3	9	Server name	Login name	
PROTOCOL_IP_GENERIC	10	Null	Null	Non-TCP/UDP transaction
PROTOCOL_GNUTELLA_ NETWORKING	11	Null	Null	Peer to peer
PROTOCOL_GNUTELLA_FIL E_ TRANSFER	12	Null	Null	Peer to peer
PROTOCOL_FASTTRACK_ NETWORKING	13	Null	Null	Peer to peer
PROTOCOL_FASTTRACK_ TRANSFER	14	Network Name	Null	Peer to peer
PROTOCOL_NNTP	15	Null	Group Name	
PROTOCOL_NAP_WINMX_ TRANSFER	16	Null	Null	Peer to peer
PROTOCOL_WINNY	17	Null	Null	Peer to peer
PROTOCOL_EDONKEY	18	Null	Null	Peer to peer
PROTOCOL_DIRECT_CONN ECT	19	Null	Null	Peer to peer
PROTOCOL_HOTLINE	20	Null	Null	Peer to peer
PROTOCOL_DYNAMIC_ SIGNATURE	21	Null	Null	

Name	ID Value	TR ACCESS_STRIN G	TR INFO_STRIN G	Description
PROTOCOL_MANOLITO	22	Null	Null	Peer to peer
PROTOCOL_SIP	23	SIP Method	SIP Domain	
PROTOCOL_BITTORRENT	24	Null	Null	Peer to peer
PROTOCOL_SKYPE	25	Null	Null	Peer to peer
PROTOCOL_VONAGE	26	SIP Method	SIP Subscriber ID	
PROTOCOL_SHARE	27	Null	Null	Peer to peer
PROTOCOL_H323	28	Null	Is FastStart	
PROTOCOL_SOULSEEK	29	Null	Null	Peer to peer
PROTOCOL_ITUNES	30	Null	Null	Peer to peer
PROTOCOL_FILETOPIA	31	Null	Null	Peer to peer
PROTOCOL_NAPSTER	32	Null	Null	Peer to peer
PROTOCOL_DHCP	33	Null	Null	
PROTOCOL_MUTE	34	Null	Null	Peer to peer
PROTOCOL_NODEZILLA	35	Null	Null	Peer to peer
PROTOCOL_WASTE	36	Null	Null	Peer to peer
PROTOCOL_NEONET	37	Null	Null	Peer to peer
PROTOCOL_MGCP	38	Null	Null	
PROTOCOL_WAREZ	39	Null	Null	Peer to peer

Aggregation Period (uint8)

The following table lists the AGG_PERIOD field values.

Table C-18 AGG_PERIOD Field Values

Name	Value	Description
AGGREGATE_HOURLY	0	Hourly aggregate: every hour, on the hour.
AGGREGATE_DAILY	1	Daily aggregate: every day at midnight.
AGGREGATE_WEEKLY	2	Weekly aggregate: every week at midnight between Saturday and Sunday.
AGGREGATE_MONTHLY	3	Monthly aggregate: every month at midnight of the last day of each calendar month.
EXTERNAL_QUOTA_PROVISION	4	The quota is externally provisioned and managed by a third party source.

Time Frames (uint16)

The following table lists the TIME_FRAME field values:

Table C-19 Time Frame Field Values

Name	Value	Description
TIME_FRAME_0 to TIME_FRAME_3	0–3	ID of active time frame. A number from 0 to 3 that indicates the time frame internal index.

RDR Tag Assignment Summary

Following is a summary of the RDR tag assignments, ordered by tag value.

Table C-20 RDR Tag Assignments

RDR name	Tag Value (decimal)
SUBSCRIBER_PERIODIC_USAGE_RDR	4042321920
ONLINE_SUBSCRIBER_PERIODIC_USAGE_RDR	4042321922
PACKAGE_PERIODIC_USAGE_RDR	4042321924
LINK_PERIODIC_USAGE_RDR	4042321925
TRANSACTION_RDR	4042321936
TRANSACTION_USAGE_RDR	4042321938
VOIP_TRANSACTION_USAGE_RDR	4042321940
BLOCKING_RDR	4042321984
SUBSCRIBER_QUOTA_BREACH_RDR	4042321954
SUBSCRIBER_REMAINING_QUOTA_RDR	4042321968
SUBSCRIBER_QUOTA_THRESHOLD_BREACH_RDR	4042321969
DHCP_RDR	4042321986
QOS_REQUEST_RDR	4042321942
QOS_DELETE_RDR	4042321944
MALICIOUS_TRAFFIC_PERIODIC_RDR	4042322000

Periodic RDR Zero Adjustment Mechanism

The Periodic RDRs, also called Network Usage RDRs, include the Link Usage, Package Usage, Subscriber Usage, and Online Subscriber Usage RDRs. When there is traffic for a particular service or package, the appropriate Network Usage RDRs are generated periodically, according to user-configured intervals (for example, once every 5 minutes for Link Usage RDRs, once every 30 minutes for Subscriber Usage RDRs, etc.). The RDR reports the timestamp of the end of the interval during which that service's or package's traffic has been observed.

When there is *no* traffic (and therefore no consumed resources) for a particular service or package during a given period of time, the **SCAS BB** application uses the Periodic RDR Zero Adjustment Mechanism, also called the *zeroing methodology*, for reducing the number of Network Usage RDRs generated for that service or package. This technique also simplifies collection for external systems by reducing the number of RDRs that they need to handle.

The zeroing methodology algorithm works as follows: for any number of consecutive time intervals having no traffic for a particular service or package, zero-consumption RDRs are generated for the first and last zero-consumption time intervals, but not for the intermediate time intervals. These two zero-consumption RDRs are generated when the next traffic arrives.

EXAMPLE 1

The Subscriber Usage RDR (for a given subscriber) has a generation period of 30 minutes. There is subscriber traffic during the interval 1200–1230, no subscriber traffic during the following five intervals (1230–1300, 1300–1330, 1330–1400, 1400–1430, 1430–1500), and the next subscriber traffic occurs at 1522. The following Subscriber Usage RDRs are generated:

- At 1230, one RDR with the values of the consumed resources and the timestamp (1230) for the interval 1200–1230.
- At 1522, one zero-consumption RDR having the timestamp (1300) of the *first* interval with no traffic for that subscriber, 1230–1300.
- At 1522, one zero-consumption RDR having the timestamp (1500) of the *last* interval with no traffic for that subscriber, 1430–1500.

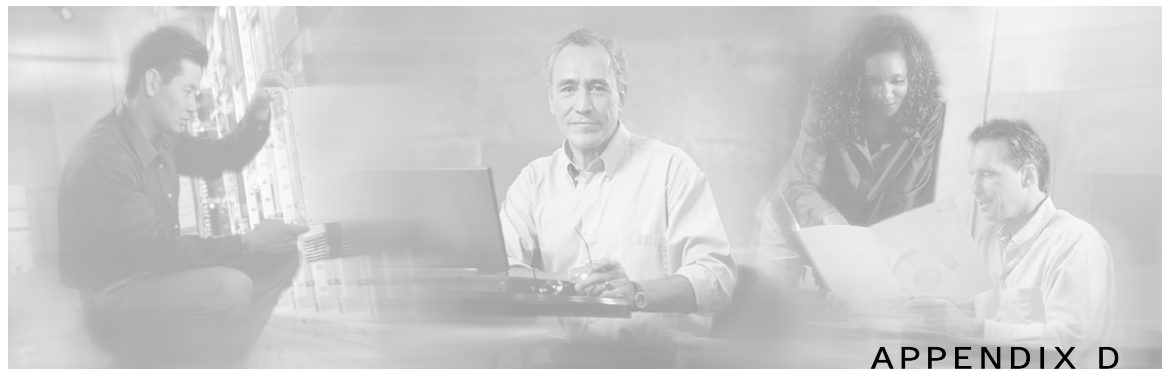
Note that for the three intermediate zero-consumption intervals (1300–1330, 1330–1400, and 1400–1430), no RDR is generated.

- At 1530, one RDR with the values of the consumed resources and the timestamp (1530) for the interval 1500–1530.

EXAMPLE 2

The Subscriber Usage RDR (for a given subscriber) has a generation period of 30 minutes. There is subscriber traffic during the interval 1200–1230, no subscriber traffic during the following interval 1230–1300, and the next subscriber traffic occurs at 1322. The following Subscriber Usage RDRs are generated:

- At 1230, one RDR with the values of the consumed resources and the timestamp (1230) for the interval 1200–1230.
- At 1322, one zero-consumption RDR having the timestamp (1300) of the single interval with no traffic for that subscriber, 1230–1300.
- At 1330, one RDR with the values of the consumed resources and the timestamp (1330) for the interval 1300–1330.



Database Tables

Each Raw Data Record (RDR) is routed to an Adapter, converted, and stored in a database table. There is a separate table for each RDR type. This chapter presents these tables and their columns (field names and types).

For additional information, such as RDR structure, RDR column and field descriptions, and how the RDRs are generated, see *RDR Format and Field Content* (on page [C-1](#)).

Overview

Each RDR is routed to the appropriate Adapter—the Database Adapter (JDBC Adapter or DB Adapter) or the Topper/Aggregator (TA Adapter)—converted, and read into a database table row. There is a separate table for each RDR type, with a column designated for each RDR field.

In addition to the RDR fields that are specific to each RDR type, the tables RPT_NUR, RPT_SUR, RPT_PUR, RPT_LUR, and RPT_TR contain two universal columns: **RECORD_SOURCE** and **TIME_STAMP**. The following values are placed in these two universal columns (field numbers 0 and 1, respectively):

- **RECORD_SOURCE**: Contains the IP address of the SCE that generated the RDR.
The IP address is in 32-bit binary format.
- **TIME_STAMP**: The RDR timestamp assigned by the CM. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

Database Tables

This section contains the following database tables:

- RPT_NUR
- RPT_SUR
- RPT_PUR
- RPT_LUR
- RPT_TR
- RPT_MALUR
- RPT_TOPS_PERIOD0

- RPT_TOPS_PERIOD1
- VALUES_INI_ENG
- INI_VALUES

Table RPT_SUR

Database table RPT_SUR stores the REALTIME_SUBSCRIBER_USAGE_RDRs. These RDRs have the tag 4042321922.

Table D-1 Columns for Table RPT_SUR

Field Number	Field Name	Type
0	TIME_STAMP	DateTime
1	RECORD_SOURCE	Integer
2	SUBSCRIBER_ID	String
3	PACKAGE_ID	Integer
4	SUBS_USG_CNT_ID	Integer
5	MONITORED_OBJECT_ID	Integer
6	BREACH_STATE	Integer
7	REASON	Integer
8	CONFIGURED_DURATION	Integer
9	DURATION	Integer
10	END_TIME	Integer
11	UPSTREAM_VOLUME	Integer
12	DOWNSTREAM_VOLUME	Integer
13	SESSIONS	Integer

Table RPT_PUR

Database table RPT_PUR stores the PACKAGE_USAGE_RDRs. These RDRs have the tag 4042321924.

Table D-2 Columns for Table RPT_PUR

Field Number	Field Name	Type
0	TIME_STAMP	DateTime
1	RECORD_SOURCE	Integer
2	PKG_USG_CNT_ID	Integer
3	GENERATOR_ID	Integer
4	GLBL_USG_CNT_ID	Integer
5	CONFIGURED_DURATION	Integer

Field Number	Field Name	Type
6	DURATION	Integer
7	END_TIME	Integer
8	UPSTREAM_VOLUME	Integer
9	DOWNSTREAM_VOLUME	Integer
10	SESSIONS	Integer

Table RPT_LUR

Database table RPT_LUR stores the LINK_USAGE_RDRs. These RDRs have the tag 4042321925.

Table D-3 Columns for Table RPT_LUR

Field Number	Field Name	Type
0	TIME_STAMP	DateTime
1	RECORD_SOURCE	Integer
2	LINK_ID	Integer
3	GENERATOR_ID	Integer
4	GLBL_USG_CNT_ID	Integer
5	CONFIGURED_DURATION	Integer
6	DURATION	Integer
7	END_TIME	Integer
8	UPSTREAM_VOLUME	Integer
9	DOWNSTREAM_VOLUME	Integer
10	SESSIONS	Integer

Table RPT_TR

Database table RPT_TR stores the TRANSACTION_RDRs. These RDRs have the tag 4042321936.

Table D-4 Columns for Table RPT_TR

Field Number	Field Name	Type
0	TIME_STAMP	DateTime
1	RECORD_SOURCE	Integer
2	SUBSCRIBER_ID	String
3	PACKAGE_ID	Integer
4	SERVICE_ID	Integer
5	PROTOCOL_ID	Integer

Field Number	Field Name	Type
6	SAMPLE_SIZE	Integer
7	PEER_IP	Integer
8	PEER_PORT	Integer
9	ACCESS_String	String
10	INFO_String	String
11	SOURCE_IP	Integer
12	SOURCE_PORT	Integer
13	INITIATING_SIDE	Integer
14	END_TIME	Integer
15	MILISEC_DURATION	Integer
16	TIME_FRAME	Integer
17	UPSTREAM_VOLUME	Integer
18	DOWNSTREAM_VOLUME	Integer
19	SUBS_CNT_ID	Integer
20	GLBL_CNT_ID	Integer
21	PKG_USG_CNT_ID	Integer

Table RPT_MALUR

Database table RPT_MALUR stores the MALICIOUS TRAFFIC_RDRs.

These RDRs have the tag **4042322000**.

Table D-5 Columns for Table RPT_MALUR

Field Number	Field Name	Type
0	TIME_STAMP	DateTime
1	RECORD_SOURCE	Integer
2	ATTACK_ID_HIGH	Integer
3	ATTACK_ID_LOW	Integer
4	SUBSCRIBER-ID	String
5	ATTACK_IP	Integer
6	ATTACK_TYPE	Integer
7	SIDE	Integer
8	IP_PROTOCOL	Integer
9	CONFIGURED_DURATION	Integer
10	DURATION	Integer
11	END_TIME	Integer

Field Number	Field Name	Type
12	ATTACKS	Integer
13	MALICIOUS_SESSIONS	Integer

Table RPT_TOPS_PERIOD0

Database table RPT_TOPS_PERIOD0 is generated by the TA Adapter for the shorter aggregation period, typically an hour.

Table D-6 Columns for Table RPT_TOPS_PERIOD0

Field Number	Field Name	Type
0	RECORD_SOURCE	Integer
1	Metric_ID	Integer
2	SUBS_USG_CNT_ID	Integer
3	Timestamp	DateTime
4	Agg_Period	Integer
5	Subscriber_ID	VARCHAR(64)
6	Consumption	Integer

The possible values for *Metric_ID* are presented in the following table.

Table D-7 Metric_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume
2	Combined Volume
3	Sessions
4	Seconds

Table RPT_TOPS_PERIOD1

Database table RPT_TOPS_PERIOD1 is generated by the TA Adapter for the longer aggregation period, typically 24 hours.

Table D-8 Columns for Table RPT_TOPS_PERIOD1

Field Number	Field Name	Type
0	RECORD_SOURCE	Integer
1	Metric_ID	Integer
2	Service_ID	Integer
3	Timestamp	DateTime

Field Number	Field Name	Type
4	Agg_Period	Integer
5	Subscriber_ID	VARCHAR(64)
6	Consumption	Integer

The possible values for *Metric_ID* are the same as for RPT_TOPS_PERIOD0. Refer to the table of values in the previous section.

Table VALUES_INI_ENG

Database table VALUES_INI_ENG is updated whenever a policy is applied in the SCAS BB Console. This table contains, per SE_IP, the mappings between numeric identifiers and their textual representation for services, packages, etc. The mapping is represented as a standard properties file in string form, where each mapping file is stored in one row. The mappings contained in this table are used in the SCAS Reporter for display.

See also table INI_VALUES, which contains the same information as this table, but where the individual items within each VALUES_INI are placed in separate rows.

Table D-9 Columns for Table VALUES_INI_ENG

Field Number	Field Name	Type
0	TIME_STAMP	DateTime
1	SE_IP	VARCHAR(20)
2	VALUES_INI	TEXT

Table INI_VALUES

Database table INI_VALUES contains the same information as table VALUES_INI_ENG, but the individual items within each VALUES_INI are placed in rows.

Table D-10 Columns for Table INI_VALUES

Field Number	Field Name	Type	Description
0	TIME_STAMP	DateTime	
1	SE_IP	VARCHAR(20)	Identification of the SCE Platform where these values were applied

Field Number	Field Name	Type	Description
2	VALUE_T YPE	Integer	Key/Value family type The possible values are: 1: service id / service name 2: package id / package name 3: tcp port number / port name 4: time frame id / time frame name 5: se address 32bit / dotted notation 6: ip protocol number / ip protocol name 7: signature protocol id / protocol name 8: p2p signature protocol id / protocol name 11: global service counter id / counter name 12: subscriber service counter id / counter name 13: package counter id / counter name 15: udp port number / port name 1002: voip signature protocol id / protocol name 2001: p2p subscriber service counter id / counter 2002: voip subscriber service counter id / counter 3001: p2p global service counter id to counter 3002: voip global service counter id to counter
3	VALUE_K EY	VARCHAR(80)	Key name For example, Gold, Silver, Adult Browsing
4	VALUE	Integer	Numeric reference



Glossary of Terms

A

Anonymous subscriber mode

A mode in which entities defined as an IP address(es) or VLAN(s) are treated as subscribers. The correlation to actual subscriber IDs is not performed by the system, but can be done externally by the collection system. Anonymous subscriber mode does not require an SM.

B

Bump-in-the-wire topology

The SCE Platform physically resides on the data link between the subscriber side and the network side, and can both receive and transmit traffic.

C

Collection Manager (CM)

A software application running on the SCE Platform that is responsible for receiving RDRs from SCE Platforms and processing them.

Command Line Interface (CLI)

One of the management interfaces to the SCE Platform. It is accessed through a Telnet session or directly via the console port on the front panel of the SCE Platform.

D

Downstream traffic

Traffic entering the SCE Platform from the network side (that is, toward the subscribers).

Dynamic Signature

A dynamic signature is a signature that can be loaded to a running application, and once loaded the application knows to identify the protocol associated with this signature.

Dynamic Subscriber-aware mode

A mode in which the actual subscriber ID is associated with an IP address when the subscriber logs onto the network and is assigned an IP address. To operate in this mode, the system must be integrated with the OSS system that assigns IP addresses to subscribers (typically based on RADIUS or DHCP)

E**External Quota Management**

Provisioning of per-service quotas for individual subscribers by an external system, such as a pre-paid server or a policy-controller.

In External Quota Provisioning, usage counters are not automatically reset at the end of an aggregation period, nor is a certain quota limit provided uniformly to all subscribers as part of the package parameters. Rather the quotas are provisioned individually via the external Quota Management system.

F**Filter Rules**

The part of the Service Configuration that lets you direct the SCE Platform to ignore some types of transactions based on Layer 3 and Layer 4 properties, and transmit them unchanged, bypassing the solution service.

G**Global Controllers**

Global Controllers are used for controlling the total bandwidth percentage for a selected protocol or package for all subscribers. See also *Subscriber BW Controllers* ("[Subscriber BW Controllers \(Bandwidth Controllers\)](#)" on page 4).

I**Inline connection mode**

The *SCAS BB* physically resides on the data link between the subscriber side and the network side, and can both receive and transmit traffic.

L**List**

An IP address range or list of web addresses used to define a service.

N**Network-initiated transactions**

Transactions that were initiated by a host, on the network side, toward a subscriber.

P**Package**

A collection of business policy rules, defining access levels to various services, charging parameters, and traffic control actions to be taken upon certain events. Subscribers are assigned packages (plans) that determine how their network transactions are controlled and charged.

PQI (Cisco Installation) File

An application package file that is installed on the network SCE Platforms and Collection Managers.

Q**Quota**

A (subscriber's) limit for a specific metric, such as bandwidth or volume.

Quota Buckets

When the external quota management mode is selected, subscriber usage of a certain service is consumed from a certain subscriber-quota-bucket. Each subscriber has four subscriber quota buckets. When a quota-bucket is depleted, services that try to consume from that bucket are regarded as "breached".

Replenishment of quota-buckets is done by a quota manager that is external to the Service Control system.

R

RDR (Raw Data Record)

A data record produced by the SCE Platform that reports on events in the traffic. RDRs produced by the SCE Platform are sent to the Collection Manager and then stored in the Collection Manager database or forwarded to third-party systems. The RDR typically contains quota (see Quota) request or reports service usage.

RDR Formatter

An internal component of the SCE Platform that gathers the Raw Data Records (RDRs), formats them, and sends them to an external Collection Manager.

Real-time subscriber usage monitoring

Subscribers which are monitored in detail and usage information is frequently reported by the SCE device to facilitate detailed reports.

Receive-only connection mode

The SCE Platform does not reside physically on the data link, and therefore can only receive data and not transmit.

S

SCAS BB Console

The user interface used for controlling the Service Control Application Suite for Broadband system, used to create, modify, and apply the service configuration.

SCE Platform

The SCE Platform is a purpose-built service component and active enforcing system designed for enhancing service providers and backbone carrier networks. By identifying, classifying, and manipulating complex traffic flows at wire-speed, the SCE Platform transforms simple transport networks into differentiated service delivery infrastructures for a wide variety of value-added IP applications, such as video streaming, VoIP, tiered services, and bilateral application-level SLAs.

The SCE Platform seamlessly interfaces with existing network elements—including routers, switches, aggregators, subscriber management devices, and operational support systems—using industry standard interfaces and communications protocols.

The need to guarantee that packets passing through the network are processed at the rate they arrive makes it necessary to provide a custom-made hardware solution.

The SCE Platform comes in three models: SCE 1000, SCE 2000 4xGBE, and SCE 2000 4/8xFE. There may be one or more of the SCE Platforms in the provider network. Within the SCE Platforms, network transactions are analyzed and mapped to services that enforce the provider's policies.

In addition, the SCE Platform implements the business logic of the system solution and performs the transaction analysis in real time. When so instructed, the SCE Platform creates a Raw Data Record (RDR) to be sent for storage to the system's data repository, the Collection Manager (CM); or carries out some other operation such as bandwidth and volume control.

SCMS Application

An SML program that determines how the *SCAS BB* operates.

Service

A value-added offering given by the service provider to its subscribers on top of its access network.

For each such commercial service the providers offer to their subscribers, a corresponding service is defined in the **SCAS BB** solution for classifying and identifying network transaction associated with the service, reporting on its usage, and controlling its traffic according to the business policy

Service Configuration

The definition of services within the **SCAS BB** solution, the mapping of network transactions to their corresponding services, and the behavior of the SCE Platform on them. The service configuration includes the definition of Services, Packages, Bandwidth Controllers, Filter Rules, etc.

Service Control

The Cisco basic concept for enabling service providers to differentiate subscribers, detect real-time events, create premium services, actively control applications, and leverage their existing infrastructure.

Service Rule

A Service is assigned to a Package by defining a Service Rule for the Package.

Session (also called Transaction)

An instance of communication between network hosts. A precise definition of a session is application protocol (Layer 7) dependent

Signature

A set of parameters that uniquely identify a protocol.

smartSUB Manager (SM)

A middleware software component used in cases where dynamic binding of subscriber information and service configurations is required. The SM manages subscriber information and provisions it in real time to multiple SCE Platforms. The SM can store subscriber service configurations information internally, and act as a state-full bridge between the AAA system (for example, RADIUS and DHCP) and the SCE Platforms.

Static Subscriber-aware mode

A mode in which a specific IP address is bound to each subscriber. This mode is useful when controlling enterprise customers, or when controlling subscribers in groups of predefined subnets (such as users of a specific CMTS/BRAS).

Subscriber

A Service Provider's client. There are two types of subscribers:

- **Introduced Subscriber:** A specific customer with an externally generated name. Maybe mapped to more than one IP address.
- **Anonymous subscriber group:** A subscriber with an internally generated name, generated automatically by the **SCAS BB** according to an anonymous subscriber group specification. Always mapped to a single IP address. The actual identity of the customer(s) is unknown to the system.

Subscriber aware mode

A mode in which actual subscribers are defined in the system, thus requiring no external correlation to actual subscriber IDs.

Subscriber BW Controllers (Bandwidth Controllers)

Subscriber Bandwidth Controllers (BW Controllers) controls traffic bandwidth for an individual subscriber. See also *Global Controllers* (on page 2).

Subscriber-initiated transactions

Transactions that are initiated by a host of a subscriber.

Subscriber-less mode

A mode of the solution that requires no integration, so that the SM component is not required. This mode is not influenced by the number of subscribers or inbound IP addresses, therefore the total amount of subscribers utilizing the monitored link is unlimited from the perspective of the SCE Platform. It is the choice for sites where control and level analysis functions are required only at a global device resolution.

T

Time Based Rule

An added-value Service Rule that can be attached to either a Total Traffic Rule or to a Service Rule. A time based rule is applied for one of the user-defined Weekly Time Frames.

Traffic-Discovery Reports

Statistics reports on network activity based on transaction usage records.

Transaction (also called Session)

An event in traffic that is recognized by the application and is distinguished according to its L3, L4, or L7 characteristics. Different protocols may have different transaction types.

U

Upstream traffic

Traffic entering the SCE Platform from the subscriber side.



Index

A

- Accessing the Global Controller Settings • 33-5
- Accessing the SCAS BB SM GUI • 13-4, -7
2
- Accessing the SCAS Reporter • 13-4, 2-8
- Activating a Filter Rule • 97-5
- Activating the Network Traffic Band • 41-5
- Adding a Filter Rule • 89-5
- Adding a Global Controller • 36-5
- Adding a List • 27-5
- Adding a List Item • 29-5
- Adding a New Package • 42-5
- Adding a New Rule to a Package • 54-5
- Adding a New Service • 6-5
- Adding a New Service Name and Description • 7-5
- Adding a Service Element • 11-5
- Adding a Set of Redirection URLs • 5-6
- Adding a Subscriber • 9-7
- Adding a Time Based Rule • 63-5
- Adding Protocol Data • 24-5
- Adding Protocols • 24-5
- Aggregation Period (uint8) • C-25
- Aggregation Period field values • C-25
- Allowed URL List • 15-6
- Anonymous Group csv files • 25-7
- Anonymous subscriber mode • 1
- Anonymous subscriber-mode • 4-2
- Anonymous-Subscriber Mode • 18-7
- Applying a Service Configuration • 2-4
- Applying and Retrieving Service Configurations • 1-4
- Assigning Services to Packages • 53-5
- Attack Filtering and Subscriber Notification • 13-6
- Audience • xi

B

- Bandwidth Control Revisited • 72-5
- Block Reason (uint8) • C-23
- Block Reason bit values • C-23
- Blocking RDR • C-15
fields • C-15
- Bump-in-the-wire topology • 1

C

- CIR (Committed Information Rate) • 46-5
- Cisco TAC Website • xiii
- Closing the SCAS BB Console • 11-3
- Collection • 6-1
- Collection Manager (CM) • 1
- Command Line Interface (CLI) • 1
- Configuring Subscriber Notifications • 15-6
- Configuring the Redirection Parameters • -6
4
- Configuring the System Mode Parameter • 1-6
- Configuring Weekly Time-Frames • 70-5
- Connecting and Disconnecting • 4-7
- Constructing a Filter Rule • 89-5
- Constructing and Modifying Services • 6-5
- Constructing Packages • 41-5
- Constructing Service Configurations • 1-5
- Controlling Traffic in Two Levels
Total and Internal • 32-5
- Creating a New Report Definition • 7-8
- Creating a New Service Configuration • 6-4
- Criteria • A-6

D

- Daily Peak BW for All Packages • A-10
- Daily Peak BW for Specific Subscriber • A-16
- Daily Peak BW per Package • A-12

- Database tables
 - list of • D-1
 - Database Tables • D-1
 - Deactivating a Filter Rule • 97-5
 - Defining Global Controllers for a Dual Link System • 38-5
 - Defining Service Elements for Services • -5
11
 - Defining the Global Controllers • 33-5
 - Defining the Report • 6-8
 - Defining the Service Usage Counters • 8-5
 - Deleting a Report Definition • 18-8
 - Demographic Data and Service Popularity Reports • A-44
 - Description Tail • 14-6
 - Destination URL • 13-6
 - DHCP RDR • C-19
 - Displaying the Services Affected by a Rule • 66-5
 - Document Content • xii
 - Document Conventions • xii
 - DoS Attacked Subscribers • A-49
 - Downstream traffic • 1
 - Duplicating a Package • 51-5
 - Duplicating an Existing Report Definition • 17-8
 - Dynamic Signature • 1
 - Dynamic Signature Management • 10-6
 - Dynamic Subscriber-aware mode • 1
- E**
- Editing a Chart • 21-8
 - Editing a Filter Rule • 95-5
 - Editing a Global Controller • 37-5
 - Editing a List • 28-5
 - Editing a List Item • 29-5
 - Editing a Service Element • 15-5
 - Editing a Service Rule • 65-5
 - Editing Multiple Subscribers • 14-7
 - Editing Package Parameters • 51-5
 - Editing Protocol Data • 25-5
 - Editing Protocols • 21-5
 - Editing Service Parameters • 10-5
 - Editing Subscribers • 12-7
 - Editing the Protocol name and description • 21-5
 - Editing the Protocol supported list type • -5
22
 - Editing the Upstream/Downstream Total Link Limit • 36-5
- Email and News Reports • A-31
 - Exiting the Reporter • 3-8
 - Exiting the SCAS BB SM GUI • 5-7
 - Exporting Packages, Services, Protocols and Lists • 11-4
 - Exporting Reports • 23-8
 - Exporting Subscriber Files • 17-7
 - External Quota Management • 2
- F**
- Filter Rules • 2
 - Filtering the Traffic Flows • 89-5
 - Finding Subscribers • 8-7
 - FTP Server Distribution by Subscriber Packages • A-30
- G**
- Generating a New Report • 22-8
 - Generating a Report • 17-8
 - Generating Reports • 1-8
 - Generic Protocols • B-1
 - Global Active Subscriber per Service • A-44
 - Global Aggregated Usage Volume per Service • A-9
 - Global Bandwidth per Service • A-8
 - Global Bandwidth per VoIP Service • A-40
 - Global Concurrent Calls per VoIP Service • A-42
 - Global Concurrent Session per Service • A-10
 - Global Control • 30-5
 - Global Controllers • 2
 - accessing • 33-5
 - adding • 36-5, 37-5
 - total link limit • 36-5
 - Global Daily Usage Sessions per Service • A-8
 - Global Daily Usage Volume per Service • A-9
 - Global DoS Rate • A-48
 - Global Hourly Aggregated Minutes per Service • A-10
 - Global Hourly Call Minutes per VoIP Service • A-41
 - Global Hourly Usage Sessions per Service • A-8
 - Global Hourly Usage Volume per Service • A-9
 - Global Monitoring • A-7
 - Global Scan/Attack Rate • A-48

Granularity • A-3

I

Import/Export file
 mappings field format • 24-7
 Importing Packages, Services, Protocols or
 Lists • 12-4
 Importing Subscriber Files • 15-7
 Infected Subscribers • A-49
 Inline connection mode • 2
 Introducing the SCAS BB SM GUI • 2-7
 Introducing the SCAS Reporter • 1-8
 Introduction • xi, 1-1
 IP Protocols • B-3

L

Link Usage RDR • C-11
 fields • C-11
 List • 2
 List Types • 26-5
 Lists • 1-5
 editing • 28-5
 list item
 adding • 29-5
 editing • 29-5
 removing • 30-5
 managing • 26-5
 removing • 29-5
 working with • 27-5
 Locating and Selecting Subscribers • 8-7

M

Malicious Traffic Periodic RDR • C-22
 Malicious Traffic Reports • A-47
 Management and Collection • 4-1
 Managing Calendars • 68-5
 Managing csv Files • 23-7
 Managing Lists • 26-5
 Managing Protocols • 17-5
 Managing RDR Settings • 75-5
 Managing Real-time Subscriber Usage
 RDRs • 21-7
 Managing Service Configurations • 1-4
 Managing Subscriber Monitoring via the
 SCE Platform • 22-7
 Managing Subscriber Monitoring via the SM
 • 21-7
 Managing Subscribers • 1-7

Managing Subscribers via Other System
 Components • 18-7
 Managing the System Settings • 1-6
 Menu Bar and Toolbar • 2-3
 Message Band • 9-3, 7-7
 Metrics • A-4
 MMS Server Distribution by Subscriber
 Packages • A-30
 Modifying an Existing Report Definition •
 17-8
 Monitoring Reports • A-3
 Moving a Service Element • 16-5

N

Network Management • 5-1
 Network Traffic Band • 5-3
 Network Traffic/Services Band • 5-3
 Network-initiated transactions • 2
 NNTP Server Distribution by Subscriber
 Packages • A-37
 Notification Dismissal • 15-6

O

Obtaining Technical Assistance • xiii
 Opening a TAC Case • xiv
 Opening an Existing Service Configuration •
 10-4
 Opening the SCAS BB Console • 10-3
 Order Parameter • A-6
 Overview • 1-1, D-1
 Overview of Bandwidth Control • 30-5
 Overview of Report Templates • A-1

P

P2P Reports • A-38
 Package • 2
 Package Active Subscriber per Service • A-
 45
 Package Aggregated Usage Volume per
 Service • A-13
 Package Bandwidth per Service • A-11
 Package Bandwidth per VoIP Service • A-41
 Package Concurrent Session per Service •
 A-13
 Package Counters • 4-5
 Package Daily Usage Sessions per Service •
 A-11
 Package Daily Usage Volume per Service •
 A-12

- Package Hourly Aggregated Minutes per Service • A-13
 - Package Hourly Call Minutes per VoIP Service • A-41
 - Package Hourly Usage Sessions per Service • A-11
 - Package Hourly Usage Volume per Service • A-12
 - Package Monitoring • A-11
 - Package Usage RDR • C-13
 - fields • C-13
 - Packages • 1-5, 40-5
 - adding • 42-5
 - using Advanced tab • 49-5
 - using Aggregation Period tab • 44-5
 - using Bandwidth Controller tab • 46-5
 - using General tab • 42-5
 - constructing • 41-5
 - duplicating • 51-5
 - editing parameters • 51-5
 - removing • 53-5
 - Packages and Services • 5-5
 - Packet Concurrent Calls per VoIP Service • A-43
 - Periodic RDR Zero Adjustment Mechanism • C-27
 - PIR (Peak Information Rate) • 46-5
 - POP3 Server Distribution by Subscriber Packages • A-37
 - Port-Based Protocols • B-7
 - PQI (Cisco Installation) File • 2
 - Printing Reports • 23-8
 - Protocol Data • 19-5
 - Protocol Reference Tables • B-1
 - Protocol Settings Screen • 18-5
 - PROTOCOL_ID (int16) • C-24
 - PROTOCOL_ID field values • C-24
 - Protocols • 1-5, 17-5
 - adding • 24-5
 - editing
 - managing • 17-5
 - Protocol Settings screen • 18-5
 - reference tables • B-1
 - removing • 23-5
 - working with • 20-5
 - list type • 22-5
 - name and description • 21-5
 - supported list type • 22-5
 - Purpose • xi
- Q**
- QOS Delete RDR • C-21
 - QOS Request RDR • C-20
 - Quota • 2
 - Quota Buckets • 2
 - Quota Provision RDR • C-16
- R**
- RDR (Raw Data Record) • 3
 - RDR Enumeration Fields • C-23
 - RDR Format and Field Content • C-1
 - RDR Formatter • 3
 - RDR Tag Assignment Summary • C-26
 - Real-time subscriber usage monitoring • 3
 - Real-time Subscriber Usage RDR • C-9
 - fields • C-9
 - Receive-only connection mode • 3
 - Refreshing the Report • 23-8
 - Related Publications • xiii
 - Relative Consumption Consumptions of Top Subscribers • A-47
 - Remaining Quota RDR • C-17
 - Removing a Filter Rule • 96-5
 - Removing a Global Controller • 37-5
 - Removing a List • 29-5
 - Removing a List Item • 30-5
 - Removing a Package • 53-5
 - Removing a Service • 10-5
 - Removing a Service Element • 16-5
 - Removing a Service Rule • 66-5
 - Removing a Set of Redirection URLs • 6-6
 - Removing Port Numbers • 26-5
 - Removing Protocols • 23-5
 - Removing Subscribers • 15-7
 - Renaming an Existing Report Definition • -8
18
 - Report Options • 19-8
 - Reporter
 - Main Screen • 4-8
 - Reports

- editing a chart • 21-8
 - exporting • 23-8
 - generating new report • 22-8
 - printing • 23-8
 - refreshing • 23-8
 - viewing • 20-8
 - working with • 19-8
- Retrieving the Current Service Configuration • 3-4
- RTSP Host Distribution by Subscriber Packages • A-29
- Running the SCAS BB Console • 1-3
- S**
- Saving the Current Service Configuration • 8-4
- SCAS BB Console • 6-2, 1-3, 3
 - closing • 11-3
 - main screen • 2-3
- main window • 5-3
- message band • 9-3
- Network Traffic/Services band • 5-3
- status bar • 9-3
 - menu • 2-3
- SCAS BB Licenses • 13-4
- SCAS BB Subscriber Manager
 - accessing • 13-4
- SCAS Reporter Templates • A-1
- SCE Platform • 3
- SCE Platform Subscriber CLI • 19-7
- SCE Platforms • 3
- SCE Subscriber files • 24-7
- SCMS Application • 3
- Selecting a Group of Subscribers • 8-7
- Selecting a Protocol for a Service Element • 11-5
- Selecting an Initiating Side • 12-5
- Selecting Lists • 13-5
- Service • 4
- Service Configuration • 5-2, 4
 - applying • 2-4
 - managing • 1-4
 - opening • 10-4
 - retrieving • 3-4
 - validating • 9-4
- Service Configuration API • 7-2
- Service Configuration Management • 6-1
- Service Configuration Overview • 2-5
- Service Configuration Utility • 6-2
- Service Configurations Utility
 - using • 4-4
- Service Control • 4
- Service Control Application Suite for Broadband - Service Control for Broadband Service Providers • 2-1
- Service Control Capabilities • 2-1
- Service Counters • 3-5
- Service Distribution by Subscriber Packages • A-31
- Service Popularity among Subscribers • A-45
- Service Popularity among Subscribers of a Specific Package • A-46, A-47
- Service Rule • 53-5, 4
 - adding to a Package using Breach Handling tab • 61-5
 - using Control tab • 56-5
 - using General tab • 54-5
 - using Usage Limits tab • 60-5
- Services • 1-5
 - adding • 6-5
- name and description • 7-5
 - definition • 2-5
 - editing parameters • 10-5
 - removing • 10-5
 - setting the advanced options • 9-5
- Services Band • 8-3
- Session (also called Transaction) • 4
- Setting BW Management Parameters • 9-6
- Setting Ongoing Policy Check Parameters • 7-6
- Setting P2P Detection Parameters • 8-6
- Setting Redirection Parameters • 3-6
- Setting the Service Advanced Options • 9-5
- Signature • 4
- Signature-based Protocols • B-1
- SM Subscriber files • 24-7
- smartSUB Manager (SM) • 4
- smartSUB Manager CLU • 20-7
- SMTP Server Distribution by Subscriber Packages • A-36
- Static Subscriber Mode • 4-2
- Static Subscriber-aware mode • 4
- Status Bar • 9-3, 8-7
- Streaming Host Distribution by Subscriber Packages • A-29

- Subscriber • 4
 - Subscriber Aggregated Usage Volume per Service • A-16
 - Subscriber aware mode • 4
 - Subscriber Bandwidth Control • 31-5
 - Subscriber Bandwidth per Service Counter • A-14
 - Subscriber Bandwidth per VoIP Service • A-42
 - Subscriber BW Controllers (Bandwidth Controllers) • 5
 - Subscriber CSV File Formats • 24-7
 - Subscriber Daily Usage Sessions per Service • A-16
 - Subscriber Daily Usage Volume per Service • A-14
 - Subscriber Hourly Aggregated Minutes per Service • A-17
 - Subscriber Hourly Call Minutes per VoIP Service • A-42
 - Subscriber Hourly Usage Sessions per Service • A-15
 - Subscriber Hourly Usage Volume per Service • A-14
 - Subscriber Listing • 7-7
 - Subscriber Management • 6-1
 - Subscriber Manager
 - accessing • 2-7
 - Main Window • 5-7
 - managing subscribers • 8-7
 - Subscriber listing • 7-7
 - Subscriber Modes – Summary • 5-2
 - Subscriber Monitoring • A-14
 - Subscriber Notification • 85-5
 - Subscriber Notification on Network Attack • 13-6
 - Subscriber Usage RDR • C-8
 - fields • C-8
 - Subscriber-Aware Mode • 19-7
 - Subscriber-aware mode – Dynamic Subscribers • 4-2
 - Subscriber-initiated transactions • 5
 - Subscriber-less mode • 3-2, 5
 - Subscribers
 - anonymous-subscriber mode • 18-7
 - managing anonymous via SE CLI • 18-7
 - managing via other system components • 18-7
 - managing via SCE CLI • 19-7
 - subscriber-aware mode • 19-7
 - Subscribers and Subscriber-Modes • 3-2
 - System Components • 1-2
 - System Overview • 1-2
 - System Settings
 - configuring the System State parameter • 1-6
- T**
- Table INI_VALUES • D-6
 - Table RPT_LUR • D-3
 - Table RPT_MALUR • D-4
 - Table RPT_PUR • D-2
 - Table RPT_SUR • D-2
 - Table RPT_TOPS_PERIOD0 • D-5
 - Table RPT_TOPS_PERIOD1 • D-5
 - Table RPT_TR • D-3
 - Table VALUES_INI_ENG • D-6
 - TAC Case Priority Definitions • xiv
 - Templates
 - overview • A-1
 - The Breach Handling Tab (Service Rule) • 61-5
 - The Cisco Service Control Concept • 1-1
 - The Control Tab (Service Rule) • 56-5
 - The Package Hierarchy • 3-5
 - The Reporter Main Screen • 4-8
 - The Reports Wizard • 5-8
 - The SCAS BB Console • 2-3
 - The SCE Platform • 3-1
 - The Service Hierarchy • 2-5
 - The SM Command Menus and Toolbar • 6-7
 - The SM GUI Main Window • 5-7
 - The Usage Limits Tab (Service Rule) • 60-5
 - Threshold Breach RDR • C-18
 - Time Based Rule • 53-5, 5
 - Time Frames (uint16) • C-26
 - Time Frames field values • C-26
 - Top Client • A-19
 - Top Client IP and Server UDP Port • A-22
 - Top Client IP to Server IP • A-21
 - Top Client IP to Server IP and Server TCP Port • A-22
 - Top Client IP to Server IP and Server UDP Port • A-23

- Top Client IP To Server TCP Port • A-20
 - Top Client IP To Server UDP Port • A-20
 - Top DoS Attacked Hosts • A-49
 - Top E-mail Account Owners • A-34
 - Top E-mail Recipients • A-34
 - Top E-mail Senders • A-33
 - Top FTP Servers • A-28
 - Top HTTP Streaming Hosts • A-26
 - Top IP Protocol • A-17
 - Top MMS Servers • A-27
 - Top Newsgroups • A-35
 - Top NNTP Consumers • A-36
 - Top NNTP Servers • A-33
 - Top P2P Consumers • A-38
 - Top P2P Downloaders • A-38
 - Top P2P Protocols • A-39, A-40
 - Top P2P Uploaders • A-39
 - Top POP3 Servers • A-32
 - Top RTSP Hosts • A-27
 - Top Scanning/Attacking Hosts • A-48, A-49
 - Top Server IP and Server TCP Port • A-21
 - Top Servers • A-18
 - Top Servers TCP Ports • A-18
 - Top Servers UDP Ports • A-19
 - Top Service Servers • A-28
 - Top Service TCP Ports • A-24
 - Top Service UDP Ports • A-25
 - Top Signature-Based Protocols • A-23
 - Top SIP Domains • A-43
 - Top SMTP Servers • A-32
 - Top Subscriber to Newsgroup • A-35
 - Top Subscribers • A-15
 - Top Talkers • A-44
 - Top Web Hosts • A-25
 - Total Traffic Rule • 53-5, 54-5
 - Traffic Classification • 6-5
 - Traffic Control • 30-5
 - Traffic Discovery - Statistics • A-17
 - Traffic Discovery Reports • A-6
 - Traffic Rules • 54-5
 - Traffic-Discovery Reports • 5
 - Transaction (also called Session) • 5
 - Transaction RDR • C-2
 - fields • C-2
 - Transaction Usage RDR • C-4
 - fields • C-4
- U**
- Understanding the System Settings • 1-6
 - Universal RDR Fields • C-1
- Unknown Subscribers Traffic • 67-5
 - definition • 67-5
 - Upstream traffic • 5
 - Using and Filtering The Protocols View • -5
20
 - Using the Advanced Tab (Packages) • 49-5
 - Using the General Tab (Packages) • 42-5
 - Using the Log RDRs Tab (RDR Settings) •
79-5
 - Using the Quota Management Tab
(Packages) • 44-5
 - Using the Quota RDRs Tab (RDR Settings)
• 82-5
 - Using the Realtime RDRs Tab (RDR
Settings) • 84-5
 - Using the Service Configuration Utility • 4-4
 - Using the Subscriber BW Controller Tab
(Packages) • 46-5
 - Using the Traffic Discovery Tab (RDR
Settings) • 81-5
 - Using the Transaction Usage RDRs Tab
(RDR Settings) • 78-5
 - Using the Usage RDRs Tab (RDR Settings)
• 76-5
- V**
- Validating the Current Service
Configuration • 9-4
 - Viewing Reports • 20-8
 - VoIP Reports • A-40
 - VoIP Transaction Usage RDR • C-5
- W**
- Web and Streaming Reports • A-25
 - Weekly Time-Frames • 68-5
 - Working with Individual Subscribers • 8-7
 - Working with Lists • 27-5
 - Working with Protocols • 20-5
 - Working with Reports • 19-8
 - Working with Subscriber csv Files • 15-7