



System Release 4.0

Release Notes

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

CableCARD, OCAP, and OpenCable are trademarks of Cable Television Laboratories, Inc.

DOCSIS is a registered trademark of Cable Television Laboratories, Inc.

Rovi is a trademark of Rovi Corporation.

Other third party trademarks mentioned 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. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing **or** later issued patent.

Copyright

© 2006, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

ROVI CORPORATION COPYRIGHT NOTICE

This product incorporates copyright protection technology that is protected by U.S. patents and other intellectual property rights of Rovi Corporation. Use of this copyright protection technology must be authorized by Rovi Corporation, and is intended for home and other limited viewing uses only unless otherwise authorized by Rovi Corporation. Reverse engineering and disassembly are prohibited.

Contents

About This Guide.....	V
Chapter 1	Why Choose System Release 4.0?
Overview	1-1
DSG: New DOCSIS Option Can Consolidate Administration of the Data Network	1-3
CableCARD: New Features Bring the CableCARD Module to the Next Level ..	1-10
Logging: New Logging Utility Makes Troubleshooting Even Easier.....	1-12
Instastaging: Stage On Demand in the Subscriber's Home	1-15
UI Servers: New GUIs Make It Easier to Monitor UI Servers.....	1-18
Sessions: UI Enhancements Increase Usability of the Session List	1-21
More DNCS Enhancements: Improvements Make Familiar Tasks Easier	1-25
OCAP: Support for OCAP-Based Applications Increases Options for You and Your Subscribers	1-29
Additional DNCS Behavior Change in SR 4.0	1-30
Chapter 2	What Are the New Optional Features in SR 4.0?
Overview	2-1
Direct ASI: Direct ASI Replaces the BIG.....	2-2
Regional Control System: A New Solution for Geographic Challenges	2-3
Overlay: Deploy Cisco Set-Tops in Other Networks	2-4
Chapter 3	What Are the Site Requirements?
Overview	3-1
Hardware and Software Requirements	3-2
Scheduling Requirements	3-5
Chapter 4	What CRs Are Included in SR 4.0?
Overview	4-1
Issues Corrected in SR 4.0: The Short Story	4-2
Want to Know More?	4-3
Chapter 5	What Are the Known Issues for Standard SR 4.0?
Overview	5-1
Known Issues in the Standard Version of SR 4.0	5-2
Chapter 6	What Are the Known Issues for Optional Features in SR 4.0?
Overview	6-1

Contents, Continued

	Known Issues for RCS in SR 4.0.....	6-2
Chapter 7	Customer Information	
Appendix A	What’s Installed with SR 4.0?	
	Overview	A-1
	A Snapshot of Your System Post-Upgrade	A-2

About This Guide

About This Guide

Introduction

System Release 4.0 (SR 4.0) is a major release built on System Release 2.2 (SR 2.2). These release notes contain the following information:

- Descriptions of the standard new features introduced with this system release
- Brief descriptions of new optional features for SR 4.0
- Information you need to prepare your site for an upgrade to SR 4.0
- Change requests (CRs) that were found in previous system releases and corrected in SR 4.0
- A summary of open issues for the standard version of SR 4.0
- A summary of open issues associated with optional features for SR 4.0
- General information on contacting Cisco
- A list of software versions installed with the base SR 4.0 system

Audience

These release notes are written for system operators, sales and program managers, and field technicians.

Scope

These release notes provide an executive overview of SR 4.0. If you have questions about this release or require more detailed information, refer to the documents listed in the **Related Publications** section of this Preface, or contact Cisco Services.

About This Guide, Continued

Software Product Offering

In addition to system releases, Cisco currently offers several other types of software products that enable the cable service provider to better manage their Digital Broadband Delivery System (DBDS) networks:

- Client Releases (Application Platforms) offer a bundled software package that includes both the SARA and PowerTV® Operating System (OS). Client releases are compatible with multiple system releases.
 - Client Maintenance Releases address a group of specific change requests that are required before the next client release is available.
- System Releases are software releases that are designed to improve or enhance the functionality of the Digital Network Control System (DNCS). A system release can be categorized as one of the following product types:
 - Major Releases and Minor Releases introduce new DBDS functionality while fixing known issues in the network.
 - Service Packs are executable files that are an accumulation of fixed change requests since the last major or minor release. After a service pack is issued for a specific major or minor release, each subsequent service pack includes all previously fixed change requests.
 - Patch Releases are a single, executable file that address an urgent customer issue before the next system release.
 - Maintenance Releases incorporate patch releases and service packs into one software release.
- Headend Software Releases are software releases designed specifically for headend components to enhance hardware functionality.

About This Guide, Continued

Related Publications

You may find the following documents useful as you read these release notes. The publish dates for these documents are valid as of this printing. Some of these documents may have since been revised and have newer publish dates.

- *Configuring Simulcast Services at a Sub-Hub Level Technical Bulletin* (part number 4011503, expected publish date: spring 2006)
- *DBDS Utilities 5.1 Configuration Guide* (part number 4000828, expected publish date: spring 2006)
- *DBDS Utilities 5.1 Installation Instructions and DNCS Utilities User's Guide* (part number 740020, expected publish date: spring 2006)
- *DBDS Utilities Version 5.1 Release Notes* (part number 749636, expected publish date: spring 2006)
- *Setting Up Dual Sources and Hiding Services from CableCARD Hosts Configuration Guide* (part number 4011367, expected publish date: spring 2006)
- *Configuring the DBDS System for Using the Common Download Process With OpenCable™ Hosts Application Guide* (part number 4011041, published January 2006)
- *OCAP Architecture Guide* (part number 738184, published January 2006)
- *OCAP Installation and Upgrade Instructions* (part number 732578, published January 2006)
- *QAM Modulator Software Version 2.4 Release Notes and Installation Instructions* (part number 4003389, published January 2006)
- *Recovered IPPV Purchases After SR 2.5 Upgrade Operations Alert Bulletin* (part number 4013346, published January 2006)
- *Setting Up the PowerKey CableCARD Module on the DNCS for SR 2.5/3.5 and SR 4.0* (part number 4011765, published January 2006)
- *TSBROADCASTER User's Guide Cisco's OCAP™ Object Carousel Solution* (part number 4011043, published January 2006)
- *GQAM Software Version 1.2 Release Notes and Installation Instructions* (part number 4012452, published December 2005)
- *DBDS Backup and Restore Procedures for SR 2.2/3.2, SR 2.5/3.5, SR 2.6/3.6, SR 3.3, CV SR 3.4, and SR 4.0* (part number 4011040, published September 2005)
- *Enabling Content Protection for Broadcast Programming* (part number 4005893, published September 2005)
- *MQAM Modulator Software Version 2.5.0 Release Notes and Installation Instructions* (part number 4011045, published September 2005)
- *Program and System Protocol Information Configuration for System Releases 2.5, 3.5, and 4.0* (part number 4011319, published September 2005)

About This Guide, Continued

- *Instastaging Guide* (part number 4010008, published August 2005)
- *SARA Application Server 3.1.5 Release Notes and Installation Instructions* (part number 4005271, published August 2005)
- *SARA Application Server 3.1.5 User's Guide* (part number 4009747, published August 2005)
- *DNCS Report Writer Version 3.5 User's Guide* (part number 734347, published July 2005)
- *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377, published June 2005)
- *Basic DOCSIS Set-Top Gateway (No Straddle)* (part number 4004319, published March 2005)
- *Connecting the Explorer® 8300HD Digital Video Recorder* (part number 4003986, published February 2005)
- *QPSK (Release C70) Software Upgrade and Installation Instructions* (part number 4000919, published February 2005)
- *Getting Started With the Explorer® 8300 and 8300HD DVR* (part number 4004007, published August 2004)
- *Configuring and Troubleshooting the Digital Emergency Alert System, For Use With All System Releases*, part number 4004455, published January 2004)
- *Maintenance Recommendations for the DBDS System Guide* (part number 4002341, published March 2003 [Note: A new revision of this document is in process. Expected publish date: mid-year 2006.])

The SR 4.0 version of the DNCS includes online Help which you can access from the DNCS. However, if you would like to order a CD of the online Help separately, you can order the following PC version:

Digital Network Control System Online Help (PC) Version 3.5.0.3 (part number 4002881, released November 2005)

Document Version

This is the second release of these release notes.

Chapter 1

Why Choose System Release 4.0?

Overview

Introduction

SR 4.0 includes many features and enhancements implemented at the request of our customers. Review this chapter to learn more about these exciting changes.

Notes:

- This chapter describes features and enhancements for the standard version of this software release. If you want information on the optional features available for this software release, see Chapter 2, **New Optional Features**.
- If your DBDS is not currently upgraded to SR 4.0, you may want to review documentation from Cisco's two previous system releases, SR 2.5 and 3.5. Refer to the following documents for information about features and enhancements included in SR 2.5 and 3.5.

System Release 2.5

- *System Release 2.5 Release Notes*, part number 749253
- Complete System Release Binder including media, part number 4008019

System Release 3.5

- *System Release 3.5 Release Notes*, part number 4001159
- Complete System Release Binder including media, part number 4008034

In This Chapter

This chapter contains the following topics.

Topic	See Page
DSG: New DOCSIS Option Can Consolidate Administration of the Data Network	1-3
CableCARD: New Features Bring the CableCARD Module to the Next Level	1-10
Logging: New Logging Utility Makes Troubleshooting Even Easier	1-12
Instagaging: Stage On Demand in the Subscriber's Home	1-15
UI Servers: New GUIs Make It Easier to Monitor UI Servers	1-18
Sessions: UI Enhancements Increase Usability of the Session List	1-21

Overview, Continued

More DNCS Enhancements: Improvements Make Familiar Tasks Easier	1-25
OCAP: Support for OCAP-Based Applications Increases Options for You and Your Subscribers	1-29
Additional DNCS Behavior Change in SR 4.0	1-30

DSG: New DOCSIS Option Can Consolidate Administration of the Data Network

Overview

In addition to the previously supported DAVIC* and mixed DAVIC/DOCSIS® modes, SR 4.0 introduces the new DOCSIS* (DSG) mode for transporting all set-top data over the DOCSIS infrastructure. While the DOCSIS option is a standard DNCS feature included with the SR 4.0 release, this option requires the appropriate network infrastructure to function within your system.

The DOCSIS option may be beneficial for systems wanting to consolidate data traffic onto their DOCSIS network. As an added potential benefit, the DOCSIS option may allow you to use one common out-of-band (OOB) network for multiple set-top vendors.

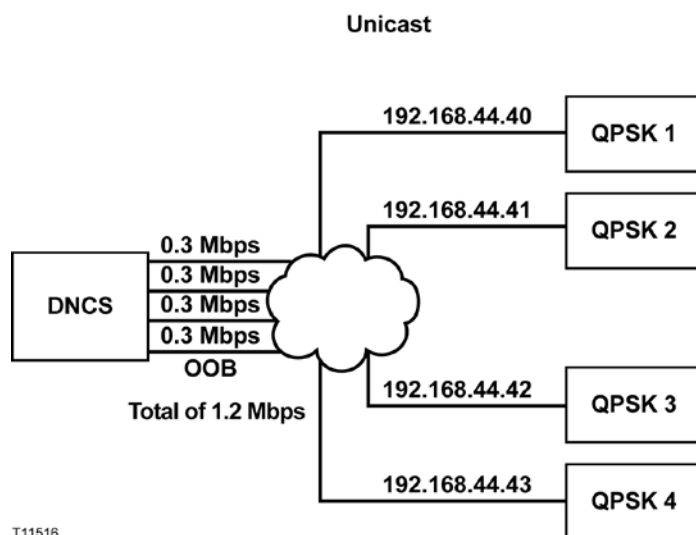
SR 4.0 also introduces single-flow multicast support to help you conserve bandwidth on your data network. This section describes new network configurations and several user interface (UI) changes associated with these new features.

**Digital Audio Visual Council; Data Over Cable Service Interface Specification*

Use One IP Address and Less Bandwidth with Single-flow Multicast

Previous system releases relied solely on unicast Internet Protocol (IP) routing to deliver Broadcast File System (BFS) and broadcast data, system information (SI), conditional access information, and PassThru messages to different set-top populations. With unicast IP routing, the DNCS can only send data to one destination at a time. Because unicast traffic is destined for a unique IP address, network administrators must configure a different OOB bridge on the DNCS for each physical OOB bridge on the network. This configuration consumes additional network bandwidth and is inefficient.

For a given hub with unicast IP routing, the destination IP address for each OOB bridge is unique; however, the information carried across each bridge is almost exactly the same. The following diagram provides a basic example of unicast IP routing in a single hub. In this example, each OOB bridge requires 0.3 Mbps of bandwidth. The network uses four different IP addresses and a total of 1.2 Mbps of bandwidth to deliver four copies of the same data to multiple set-top populations.

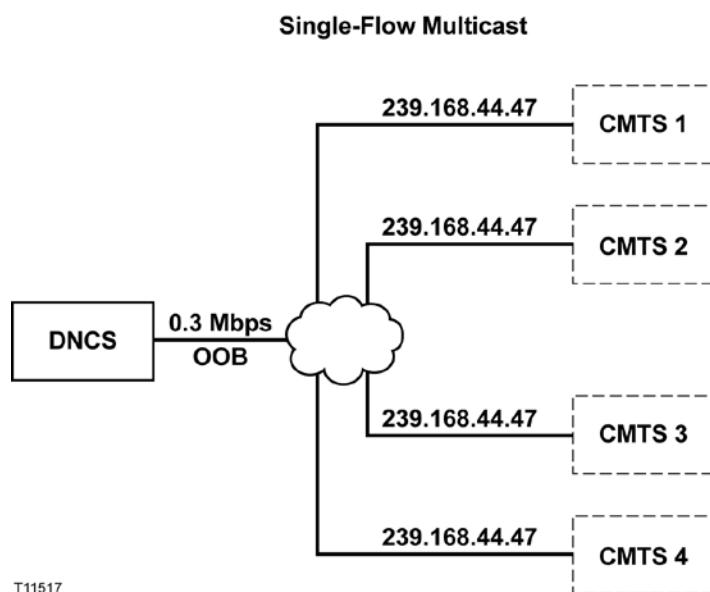


DSG: New DOCSIS Option Can Consolidate Administration of the Data Network, Continued

In SR 4.0, systems can continue to use unicast IP routing as necessary to support non-DOCSIS-capable set-tops. For DOCSIS-capable set-tops, SR 4.0 introduces support for “single-flow” multicast IP routing (multicasting). With single-flow multicast, the network uses one group destination IP address (GDA) to deliver all OOB data to multiple set-top populations. Administrators can create one or more multicast streams as needed, depending on the channel map and SI configuration of the DBDS. To support single-flow multicast, administrators create one or more logical DOCSIS OOB bridges on the DNCS and then configure the network and cable modem termination systems (CMTSs) to join the appropriate multicast stream as necessary.

Note: You can use single-flow multicast with CMTS devices only. Quadrature Phase-Shift Keying (QPSK) modulators do not support multicasting.

Multicasting conserves bandwidth on your data network. As shown in the following diagram, the 1.2 Mbps of bandwidth required to deliver information in the previous unicast example is reduced to only 0.3 Mbps of bandwidth with single-flow multicasting. The network also uses a single GDA to send the same data to multiple groups of set-tops sharing the same channel maps and SI.



DSG: New DOCSIS Option Can Consolidate Administration of the Data Network, Continued

Editing the Time-to-Live Parameter for Multicasting

An IP multicast packet must “hop” or traverse routers to reach its final destination of a CMTS device. SR 4.0 adds a default Time-To-Live (TTL) parameter of 10 for IP multicast packets that are generated by the DNCS. This TTL parameter decrements by 1 each time the IP multicast packet traverses a router. Whenever the TTL parameter reaches 0, the packet is discarded. Without TTL, an IP multicast packet could exist in an endless loop – never reaching its destination and never being discarded by the system.

If the system administrator for your DBDS network concludes it takes more than 10 hops for an IP multicast packet to reach a CMTS device, the administrator can increase the TTL parameter by changing *all* of the following environment variables in the .profile file:

- COMM_MULTICAST_TTL
- HCTM_MULTICAST_TTL
- BFS_MULTICAST_TTL

Each of these variables must be set to the same value in the .profile file. For assistance on determining the number of hops required for a packet of data to reach a CMTS and setting environment variables to alter the TTL parameter if necessary, contact Cisco Services.

Which Set-Top Models Can I Use?

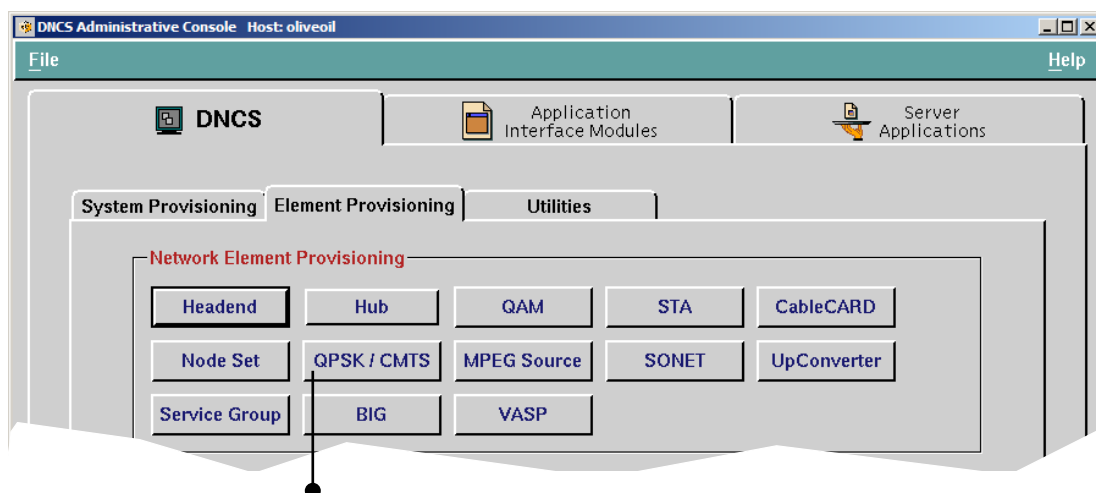
You can use the Explorer 8300™ and Explorer 8300HD™ Set-Top in a DOCSIS network to deliver digital broadcast video and support real-time, two-way interactive applications. In addition, the 8300 models include a digital video recorder (DVR) with picture-in-picture (PIP) control.

The 8300 models can use either a DOCSIS or DAVIC channel depending upon the communication mode of the set-top. In DOCSIS mode, the set-top receives both OOB data and unicast data on a DOCSIS channel. In DAVIC mode, it receives both OOB data and unicast data on the DAVIC channel.

DSG: New DOCSIS Option Can Consolidate Administration of the Data Network, Continued

The New QPSK/CMTS Interface

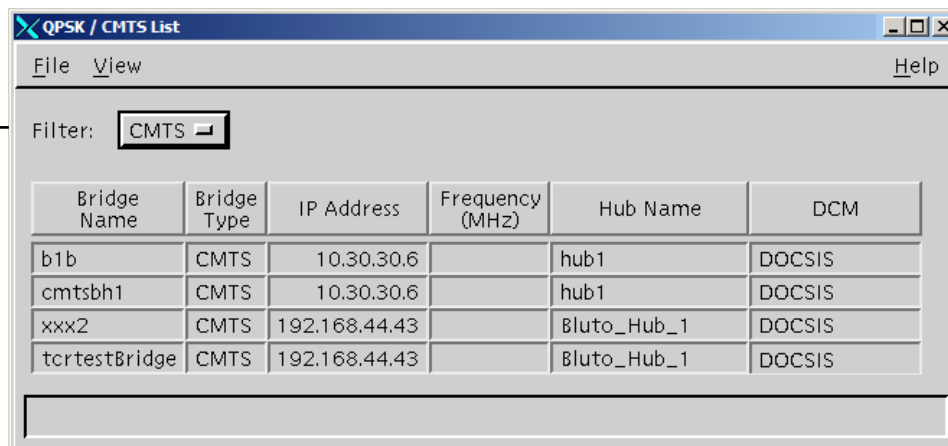
The QPSK/CMTS button on the Element Provisioning tab opens the QPSK/CMTS List window. From this window, you can complete a variety of DSG-related tasks. You can find the details for all of these tasks in the *DNCS Online Help*.



Click the QPSK/CMTS button to open the QPSK/CMTS List window.

When you click QPSK/CMTS from the Element Provisioning tab, the following screen appears. You can immediately view bridges that are already configured, or you can click the File menu to complete many other tasks, such as creating a new CMTS bridge.

You can filter the list to show CMTS bridges only, QPSK bridges only, or both.



DSG: New DOCSIS Option Can Consolidate Administration of the Data Network, Continued

CMTS Bridges for Explorer 8300 Set-Tops

To support DOCSIS-capable set-tops operating in DOCSIS mode, you must configure CMTS bridges on the DNCS. A bridge is either a single QPSK modulator or a collection of CMTS devices.

Any CMTS that joins a multicast group defined for a CMTS bridge becomes part of the hub associated with that bridge. In addition, all CMTSs joined to the multicast group receive the same OOB data. For these reasons, it is important for operators to ensure all CMTSs joined to the multicast group of a CMTS bridge do actually belong on the hub for the bridge.

You can select this box to turn on multicast IP address validation. This validation ensures the IP Address is a multicast address.

If a vendor other than Cisco provides your conditional access system, select this box to disable Cisco's PowerKEY EMMs. When disabled, all set-tops that have signed on and reported the ID for the CMTS bridge will not receive PowerKEY EMMs. In addition, new EMMs will not be generated for any set-tops associated with the CMTS bridge.

Set Up CMTS Bridge:

Hub Name: hub1

Bridge Name: OOB_Bridge1

IP Multicast Group: ☐

IP Address: 239.168. 44. 47

DCM: DOCSIS

SRM IP: 10.253. 0. 1

☐ Disable EMM Generation

Save Cancel Help

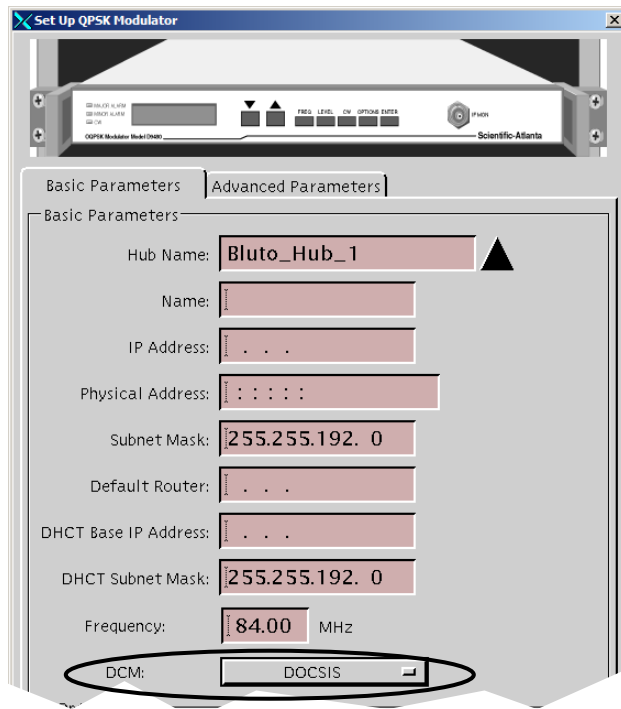
In SR 4.0, the new Set Up CMTS Bridge window allows you to configure CMTS bridges. To configure the CMTS bridge for multicasting, you must enter a multicast IP address in the range from 225.0.0.0 to 239.255.255.255. Detailed instructions for creating CMTS bridges and completing the parameters in this new window are included in the *DNCS Online Help*.

DSG: New DOCSIS Option Can Consolidate Administration of the Data Network, Continued

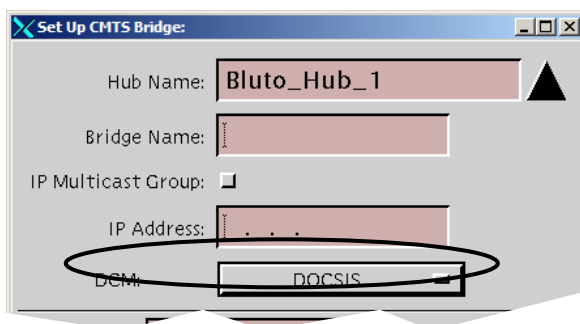
DOCSIS Added as a DCM Option

The DHCT Communication Mode (DCM) tells each set-top which mode to operate in to receive OOB data and to receive and send unicast data. In addition to the existing DAVIC and Mixed DAVIC/DOCSIS DCM options, SR 4.0 adds a new DOCSIS DCM option.

For a QPSK modulator, the new DOCSIS DCM option appears in the DCM list on the Set Up QPSK Modulator window.



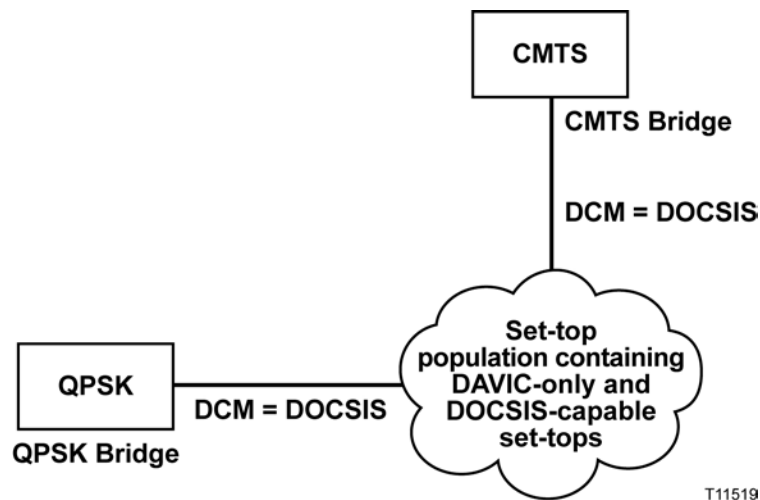
For a CMTS, the DOCSIS option appears in the DCM list on the Set Up CMTS Bridge window.



DSG: New DOCSIS Option Can Consolidate Administration of the Data Network, Continued

If your network uses both QPSK modulators and CMTSs to feed a given set-top population, the DCM for these associated QPSK and CMTS bridges must be set to the same value. If you want the DOCSIS-capable set-tops in the set-top population to run in DOCSIS mode, all DCMs for bridges serving the set-top population must be set to DOCSIS. Any DAVIC-only set-tops in the population will ignore the DOCSIS DCM; however, DOCSIS-capable set-tops require the DOCSIS DCM in order to run in DOCSIS mode.

The following diagram provides a simplified example of this concept.



Where Can I Learn More?

For more information on DOCSIS and the supported DOCSIS-capable set-tops, refer to the following publications:

- *Basic DOCSIS Set-Top Gateway (No Straddle)*
- *Connecting the Explorer® 8300 Digital Video Recorder*
- *Getting Started With the Explorer® 8300 and 8300HD DVR*

CableCARD: New Features Bring the CableCARD Module to the Next Level

Overview

SR 4.0 includes CableCARD™ module support for the following PKM600 PowerKEY® Conditional Access Module features:

- Automated Content Protection Binding for Two-Way Hosts
- New SAM Service for Setting Up Dual Sources and Hiding Services from CableCARD Hosts
- Split Channels

Automated Content Protection Binding for Two-Way Hosts

Note: This feature requires a two-way host to function.

SR 4.0 supports content-protection binding for two-way OpenCable™ Host devices (Hosts). With two-way Hosts, content protection binding occurs automatically, assuming the CableCARD module is already loaded on the DNCS.

After acknowledging the Host as a two-way Host, the CableCARD module sends the Host ID upstream to the DNCS, where the Host ID field is automatically populated on the DNCS. Content protection binding is complete when the DNCS returns an authentication message to the CableCARD module.

For content protection binding to work, the DNCS must be configured properly to ensure two-way communication and the host must be able to make a two-way connection. For detailed instructions, refer to the *DNCS Online Help* or to *Setting Up the PowerKey CableCARD Module on the DNCS for SR 4.0*.

Setting Up Dual Sources and Hiding Services from CableCARD Hosts

SR 4.0 supports configuration of two sources for a single SAM service. This feature gives you the ability to identify one source for the set-top and another source for a CableCARD host. In addition, you can now hide services from a CableCARD host. This allows you to offer selected services only to the set-top population.

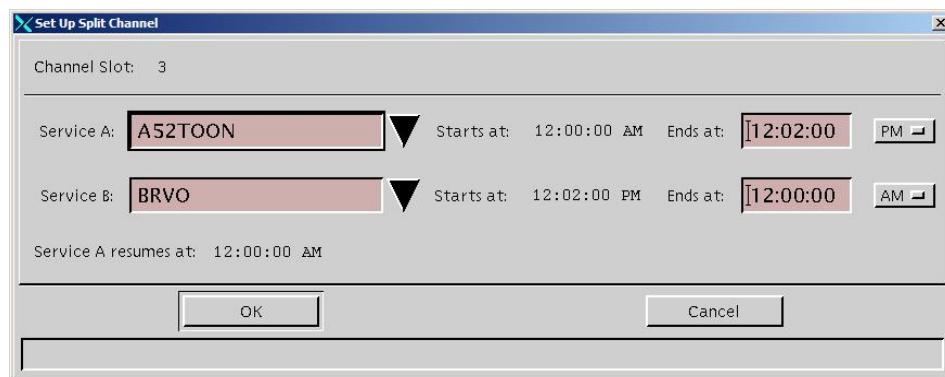
The DNCS must be configured properly to set up dual sources for a single SAM service and hide services from CableCARD hosts. For detailed instructions, refer to *Setting Up Dual Sources and Hiding Services from CableCARD Hosts*.

CableCARD: New Features Bring the CableCARD Module to the Next Level, Continued

Configure Split Channels for CableCARD Modules and Set-Tops at the Same Time

CableCARD modules now support split channels. With the split channels feature, you can enable switching between two different content streams. This allows you to carry one service part of the day, and then carry a different service the remainder of the day.

Configure split channels the same way you always have. The familiar Set Up Split Channel window that appears when you double-click an empty slot in the channel map now applies to set-tops and CableCARD modules.



Note: The SaManager process was modified to support all of the necessary changes to enable split channels for the CableCARD module. Behind the scenes, the SaManager process updates the CableCARD channel map file each time a split channel switches sources (programs).

After upgrading to SR 4.0, any currently configured split channels will start switching based on the existing schedule. As a result, CableCARD modules will mirror set-top behavior.

Logging: New Logging Utility Makes Troubleshooting Even Easier

Overview

A new button has been added to the Utilities tab that allows you to configure and display information that the DNCS records about some critical processes and their libraries.

The new Logging utility makes it easier than ever to capture key information for troubleshooting. Historically, many of the messages in the dncsLog file were simply statuses and did not indicate any error conditions. Operators had to filter through a lot of status information to find specific error conditions. The new Logging utility allows you to fine-tune log levels for processes and their libraries. The fine-tuning ensures that the dncsLog file contains more of the information you need to troubleshoot issues. The dncsLog file contains information for all processes. Each process also has its own log file, providing access to focused troubleshooting information.

During normal operation, you may choose to log information at the Error Condition level only. If a problem occurs, you can turn on several additional log levels, such as the Alert and Debug levels, to capture more information in the dncsLog file and the individual process log files.

A key benefit of the logging utility is that logging level changes are now allowed without the need to restart processes, potentially correcting a problem before data can be found to explain the problem.

Note: The dncsLog file is a very large file; a full day could easily reach 10 MB or more. Use care when Logging to avoid the risk of filling the disk. Logging can impact system performance.

For more information on all of the available log levels and for step-by-step procedures for adjusting log levels, see the *DNCS Online Help*.

Does the Logging Utility Eliminate the Need for EMCDEBUG Flags?

Not yet. While one long-term goal of the Logging utility is to obsolete the need for Enhanced Machine Control Debug (EMCDEBUG) flags, most of the processes still require setting of the EMCDEBUG flags in the .profile file.

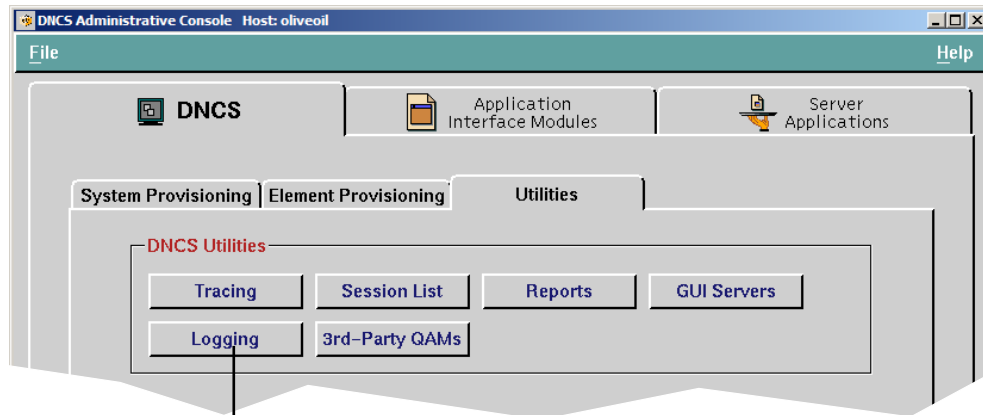
At the present time, the eventManager, logManager, ocdlMgr, and oxaitMgr processes do not require the EMCDEBUG flags to be set. You must continue to maintain your current EMCDEBUG flags in the .profile file on the DNCS to control the output of various processes that still use the old logging scheme.

Note: As a general rule, the only processes that should *always* be set to debug are bossServer, camPsm, dsm, qamManager, and siManager. Cisco Services may instruct you to temporarily set additional processes to debug for troubleshooting purposes. In these cases, Cisco Services will tell you whether to use the Logging utility or EMCDEBUG flags.

Logging: New Logging Utility Makes Troubleshooting Even Easier, Continued

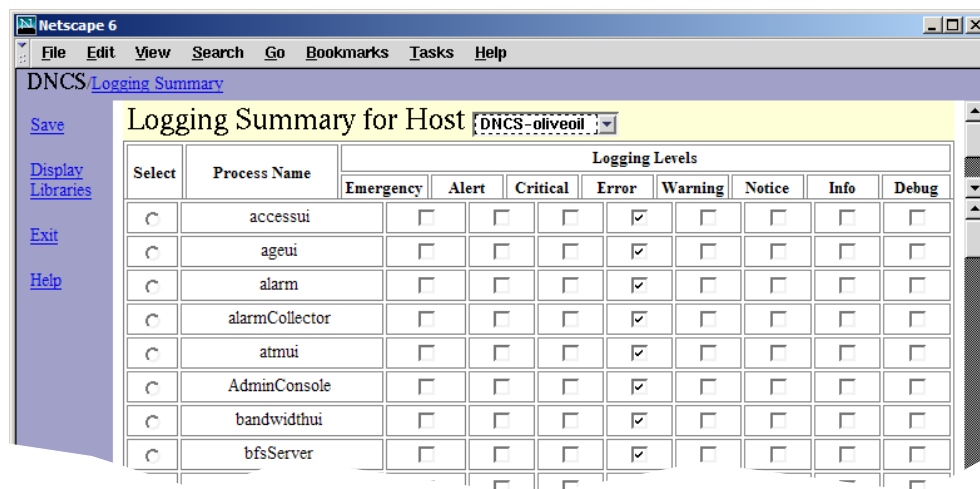
Welcome to the New Logging Interface

Access the new Logging Web User Interface (WUI) from the Utilities tab.



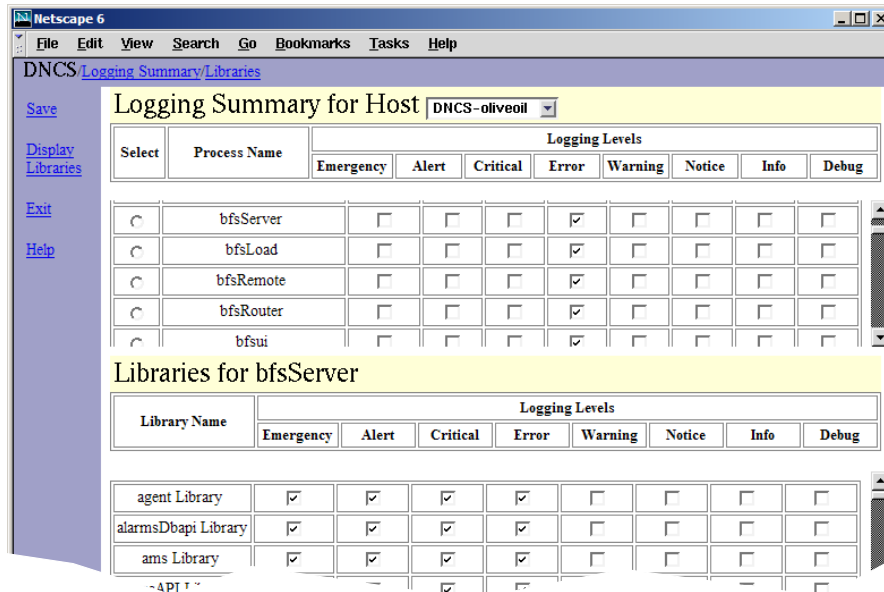
Click the Logging button to open the Logging Summary window, where you can select the type of information the DNCS records about critical processes (and their libraries).

The Logging Summary page allows you to set logging levels for each process on a specific host. If you are using Cisco's Regional Control System (RCS) solution, you can set the log levels for each remote site.



Logging: New Logging Utility Makes Troubleshooting Even Easier, Continued

To view or edit the logging levels for the libraries of a process, select the button next to the process and click **Display Libraries**. The libraries for the selected process are listed beneath the Logging Summary list, as shown in the following example.



Where Do Log Files Reside?

After you configure your logging levels, make sure you know how to access the DNCS log file and log files for individual processes. You can open the DNCS log in `/var/log/dncsLog` and view the data that the DNCS has recorded.

You can find the most recent log files for an individual process in `/dvs/dncs/tmp/[name of process.*]`. The asterisk (*) represents a numeric value, as you can have a number of different log files for each process.

Notes:

- All processing logging levels can be viewed in `/dvs/dncs/tmp`.
- Only the Emergency, Alert, Critical, and Error logging levels can be viewed in `/var/log/dncsLog`.

For more information on how to use log files to maintain a healthy system, see the *Maintenance Recommendations for the DBDS System Guide*.

Am I Required to Stop and Restart Processes When Enabling or Disabling Logging from the Logging WUI?

No. You can enable and disable logging for a process on the fly without having to stop and restart the process. However, when setting the EMCDEBUG flags, the corresponding process will have to be stopped and restarted (bounced).

Instastaging: Stage On Demand in the Subscriber's Home

Overview

Instastaging streamlines the set-top staging process for two-way, PowerKEY Conditional Access Systems. Rather than racking up large quantities of set-tops to stage from your warehouse, you can allow professional installers or your subscribers to stage set-tops on demand.

Professional Instastaging and Subscriber Instastaging: What's the Difference?

The actual steps to Instastage set-tops from the home are the same for both subscribers and professional installers. However, from a system perspective, professional Instastaging and subscriber Instastaging differ in two important ways: administrative status and package assignment.

Professional Instastaging

Professional Instastaging requires set-tops to be in a Deployed administrative status. In addition, the set-tops on the truck do not have packages pre-assigned to them. Instead, you identify the packages that comprise your standard Instastaging services using the **Default Staging Package** option from the Set Up Package window.



WARNING:

Using this option requires that you place non-pay customers in service *without* the brick mode package or with some other *low level* of service. All set-tops set to out-of-service will get the default package is connected to a two-way drop!

Select this option for each package containing services you want to define as standard Instastaging services.

Set Up Package

Package Name: Basic Service

EID:

☒ Default Staging Package

Duration: ☒ Unlimited ☐ Limited

Start Date: MM/DD/YYYY

Start Time: HH:MM:SS AM

Package List

File View Help

Show: Default Staging Packages Only

Package Name

Ultimate Movies *

* Default Staging Packages

You can use this filter to quickly review your list of default staging packages.

Instastaging: Stage On Demand in the Subscriber's Home, Continued

Subscriber Instastaging

Subscriber Instastaging requires set-tops to be in an administrative status of In Service Two Way, and packages must be assigned to the set-top. For subscriber Instastaging, the set-top is placed on the subscriber's account when picked up by the subscriber. This placement triggers the billing system to set the administrative status to In Service Two-Way and send a ModifySet-topConfiguration transaction to authorize the set-top for the specific services requested by the customer.

How Does Instastaging Work?

In the home, the installer or subscriber completes the following three-step process to stage the set-top.

1. Connect and plug in the set-top.
2. Wait for the set-top to boot and display four dashes (----) or the current time.
3. Press the **Power** key to force the set-top to sign on to the network for the first time.

If the set-top successfully signs on and goes into two-way mode, the DNCS will send the required EMMs and authorize the correct services. For professional Instastaging, the set-top receives the default staging packages configured on the DNCS. For subscriber Instastaging, the set-top receives the packages for the services the subscriber ordered from the retail center.

How Do I Turn It On?

To enable Instastaging, you must complete the following tasks. You can find detailed instructions on these tasks in the *DNCS Online Help* or the *Instastaging Guide*.

1. Add the following line to the end of the .profile file using vi or another text editor.

```
export HCTM_PROVISIONING_APP=1
```

Note: Placing this line at the end of the file ensures the correct value is set even if this same entry already appears earlier in the .profile file. As an alternative, you can search for this entry, and, if the entry already exists, you can update the value as shown.

2. Stop Spectrum, DNCS processes, and Application Server processes, and then restart Spectrum, DNCS processes, and Application Server processes.

Important: Complete this task when system usage is low, such as during a maintenance window.

3. (Optional) If you are using default staging packages to provision set-tops for professional Instastaging, set up the default staging packages on your DNCS.

Instastaging: Stage On Demand in the Subscriber's Home, Continued

How Do I Configure a Churned Set-top to Be Instastaging Capable?

Simply take the set-top out of service. When the admin status is changed to out-of-service, the DNCS will clear the IP address, delete the secure micro record, and then change the admin status to "deployed."

How Long Will It Take the Set-top to Receive EMMs?

Set-tops should receive EMMs within approximately 5 minutes. This time may vary based on system traffic.

When Instastaging Is Used, What Happens with Respect to IPPV (Credit Limit and Purchase Limit) and VOD Related Settings, Such As the DIS Enable Flag)?

It is critical to set these settings at the same time that the set-top is placed in either two-way status or deployed status. It is especially important to set the Digital Interactive Service (DIS) Enable flag at this time so that the DNCS will create the Session Based Encryption (SBE)-related EMMs.

What Is the Network Traffic Impact?

Instastaging can actually improve network traffic overall, especially when you use Instastaging for two-way staging in the warehouse. In this case, the EMMs only need to be sent to the one QPSK modulator feeding the staging rack, rather than every QPSK modulator if you were previously staging in a one-way environment.

Where Can I Learn More?

For more information on Instastaging, see the *DNCS Online Help* or the *Instastaging Guide*.

UI Servers: New GUIs Make It Easier to Monitor UI Servers

Overview

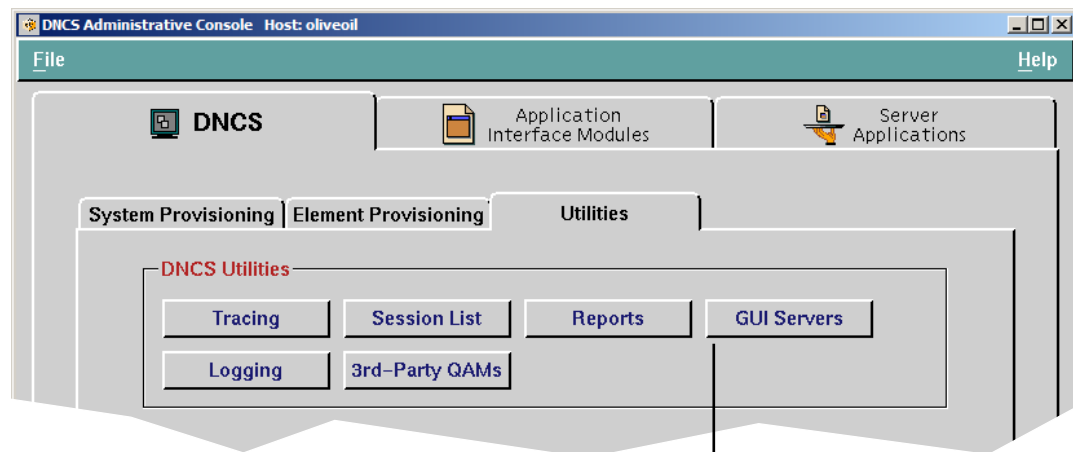
Simple Object Access Protocol (SOAP) is an XML-based messaging protocol for exchanging information over the Internet. The DNCS now uses SOAP servers to integrate new Web-based interfaces with the legacy DNCS database and servers. As an example, the dbUIServer SOAP Server plays an important role in populating the Web-based CableCARD UIs with information from the DNCS database.

Note: On the DNCS Administrative Console, SOAP Servers are also referred to as both GUI servers and UI servers.

Welcome to the New UI Server Interface

On occasion, you may need to check the status of a UI server. For example, if the CableCARD Web interface opens, but no data is populated, you can check to see if the UI server for the CableCARD module (dbUIServer) is running. For SR 4.0, all UI servers are managed by a single Server Manager. If the Server Manager is running, all of the UI servers under this Server Manager should also be running. If desired, you can also view the status for each individual UI server under the server Manager.

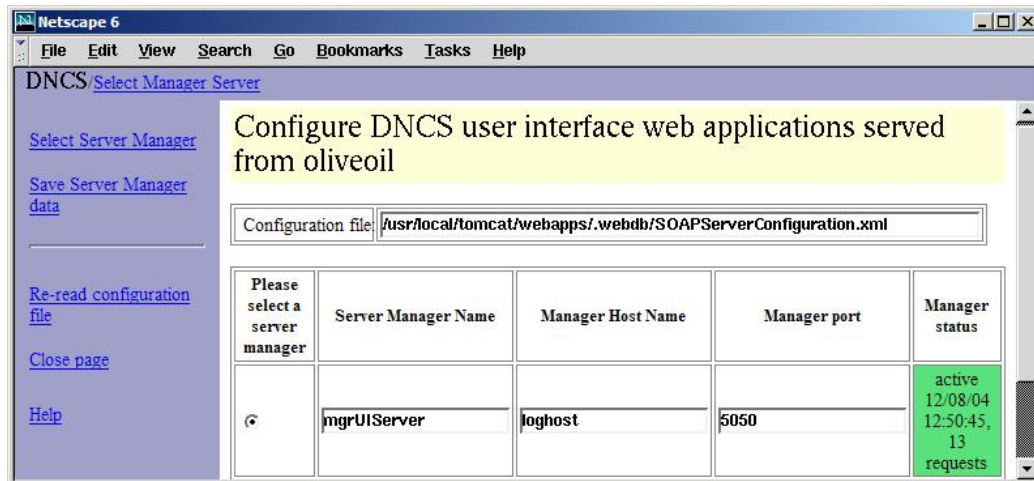
Click the new GUI Servers button to open the Select Manager Server window, where you can immediately view the status for the Server Manager.



Click the GUI Servers button to view the status of the overall Manager for all UI servers.

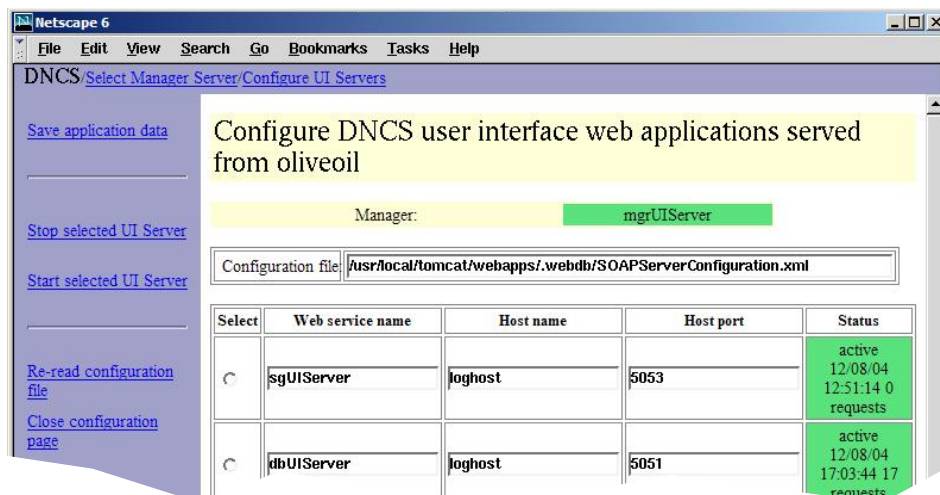
UI Servers: New GUIs Make It Easier to Monitor UI Servers, Continued

For SR 4.0, only one Server Manager appears. Other managers may be added in future system releases as needed. The Server Manager status is color-coded to make it easy for you to determine if the Server Manager is running. Green indicates the Server Manager is active and running. Red and the message “inactive” indicate the Server Manager process is inactive. If you see red and the message “unknown,” the Server Manager returned no status when queried, indicating a communication or configuration issue.



In addition to “active,” “inactive,” or “unknown” statuses, the Manager Status also shows the date and time that the server started and the number of service requests the server has processed since it was started.

You can click **Select Server Manager** from the left column of the page to view the status for each UI server under this Server Manager.



UI Servers: New GUIs Make It Easier to Monitor UI Servers, Continued

Which UI Servers Can I Stop and Start from the New Interface?

SR 4.0 uses the following UI servers for Web interfaces. Each of the following servers can be stopped and restarted from the Configure UI Servers page:

- **sgUIServer** provides service group processing support.
- **dbUIServer** provides database access.
- **logUIServer** provides logging utility support.
- **rpcUIServer** provides DNCS server interaction.

If a UI server requires a patch, you can stop the UI server, install the patch, and then restart the UI server. This feature removes the need to stop and restart the entire DNCS for a single UI server patch.

For detailed instructions on stopping and starting UI servers, see the *DNCS Online Help*.

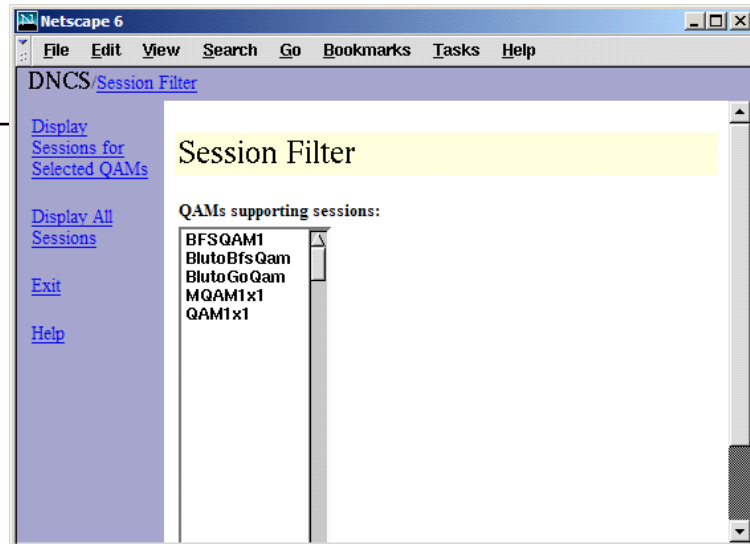
Sessions: UI Enhancements Increase Usability of the Session List

Overview

Based on usability reviews, significant enhancements were implemented for the Session List WUIs. This section provides an overview of these enhancements.

Quick Path: DNCS Administrative Console> Utilities tab> Session List

To focus session information, select QAMs from the list and click Display Sessions for Selected QAMs.



Focus the Session List with New Filtering Options

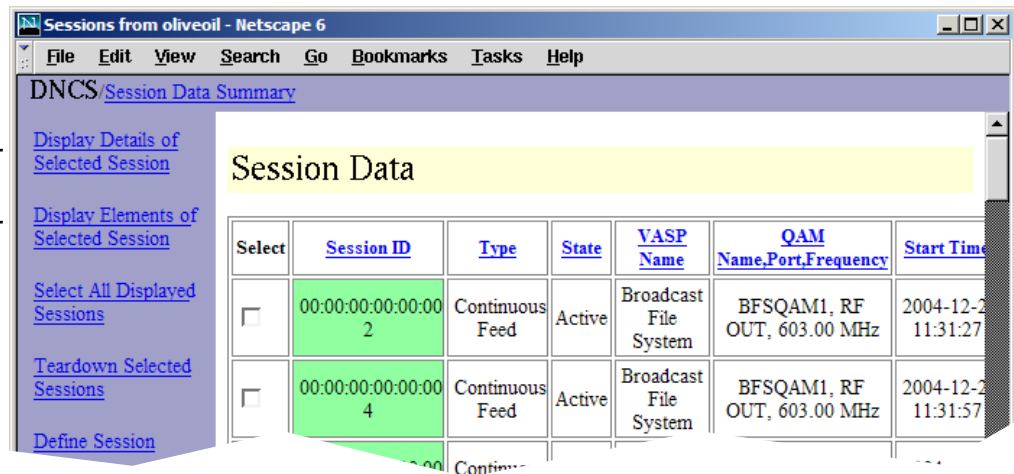
If you are only interested in sessions for particular QAM modulators (QAMs), new filtering options allow you to display sessions for those QAMs only. Select a single QAM, or use the **Ctrl** or **Shift** keys to select multiple QAMs. You can still show session information for all QAMs if desired.

Sessions: UI Enhancements Increase Usability of the Session List, Continued

Access Detailed Information for Selected Sessions

Two new menu options make it easy to display details or elements for a selected session.

You can display details or elements for a selected session.



Sessions: UI Enhancements Increase Usability of the Session List, Continued

Session Details

When you click **Display Details of Selected Session** from the Session Data Summary window, the Session Resources page opens. You can view details such as the MPEG Program Number, PMT PID, PCR PID, and ECM PID for each view of the session. From this page, you also have the option of viewing the details for a specific resource.

Use this option to view details for a specific resource.

View	MPEG Program Number	PMT PID	PCR PID	ECM PID
Server	135	32769	8191	8191

Select	Resource Number	Resource Type	View	State
<input type="radio"/>	16381	MPEG Program	Server	Active
<input type="radio"/>	16283	MPEG Program	Client	Active
	16382	Trans		

The following example shows the resulting Resource Details page that opens when you select a resource and click **Display Selected Resource Details** from the Session Resources page.

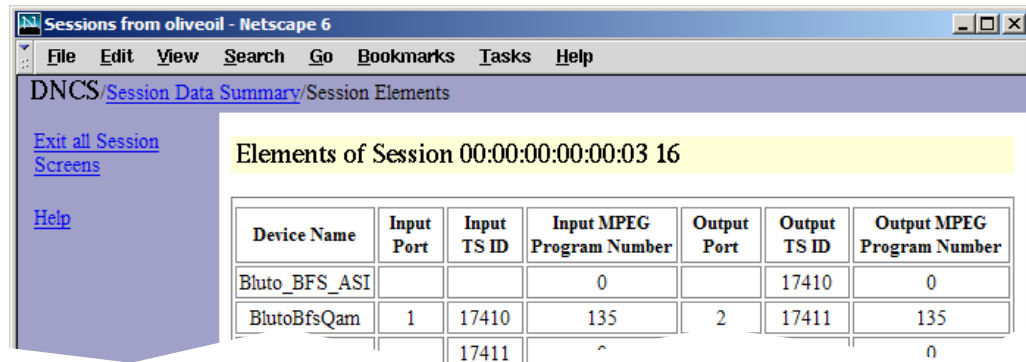
Resource Attribute	Resource Value
Session ID	00:00:00:00:00:03 16
Session Oid	9708
Resource Number	16381
Allocation Time	12/08/04 10:50:07
Rel Time	

Sessions: UI Enhancements Increase Usability of the Session List, Continued

Element Details

When you click **Display Elements of Selected Session**, from the Session Data Summary window, the Session Elements page opens.

From this page, you can view key information for each device associated with the session, including the Input Port, Input TSID, Input MPEG Program Number, Output Port, Output TSID, and Output MPEG Program Number.



Device Name	Input Port	Input TS ID	Input MPEG Program Number	Output Port	Output TS ID	Output MPEG Program Number
Bluto_BFS_ASI			0		17410	0
BlutoBfsQam	1	17410	135	2	17411	135
		17411	0			0

More DNCS Enhancements: Improvements Make Familiar Tasks Easier

Overview

Several enhancements to existing features throughout the DNCS application make common tasks even easier. This section provides an overview of these enhancements.

Work with Service Groups from a Web-Based Interface

The existing Service Group user interface was ported to the new Web-based user interface. You can still complete all of the same tasks you always have for service groups. For more information on service groups, see the *DNCS Online Help*.

Quick Path: DNCS Administrative Console> DNCS tab> Element Provisioning tab> Service Group

Add New BFS Sources and Sessions Without the Need for Special Handling of OSM Sessions

SR 4.0 treats the OSM session just like other BFS sessions rather than requiring its own unique configuration. This change eliminates the special handling of OSM when adding new BFS sources and sessions. As a result, the Configure Carousel window is no longer needed and has been removed.

Modify Data Carousels in Fewer Steps, Less Time

The OSM carousel is now fully integrated into the BFS carousels. As a result, when adding a new data carousel to the Program Allocation Table (PAT), you no longer need to delete the OSM carousel and add it back to the PAT.

Eliminate Mirror QAMs for PSIP Configuration

The new Non-SA Digital Source Definition UI eliminates the need for mirror QAMs in PSIP configuration. Refer to the *Program and System Information Protocol Configuration for System Releases 2.5, 3.5, and 4.0* technical bulletin for details.

Note: Contact Cisco Services to have the DNCS “Third-Party Source” feature support enabled on your system.

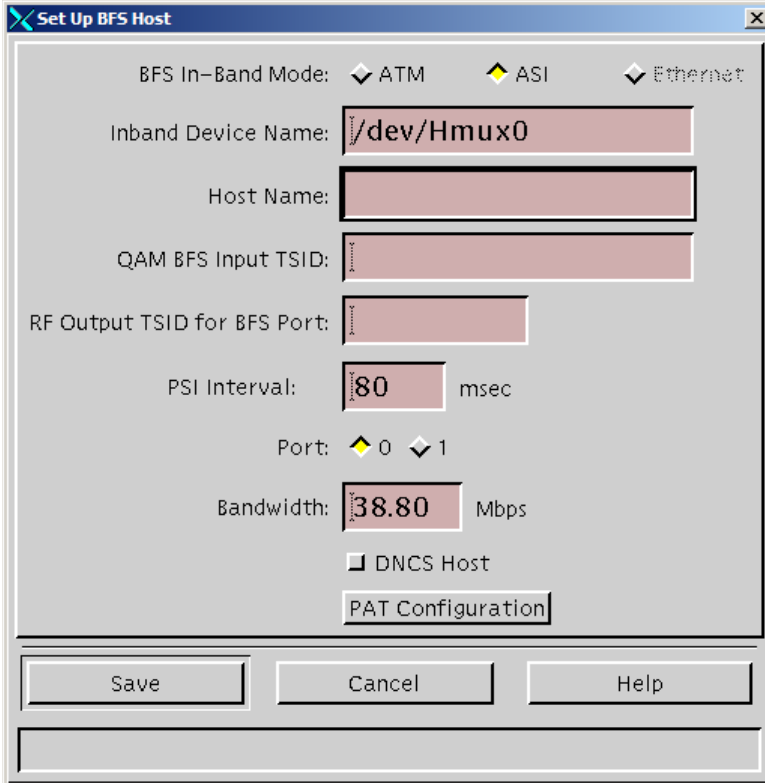
More DNCS Enhancements: Improvements Make Familiar Tasks Easier, Continued

Set Up the Inband Data Path from a More Logical Location

With SR 4.0, set up of the inband data path is now done from the Set Up BFS Host window.

In previous releases, the inband data path was configured by clicking the **Inband Data Config** button on the Application Interface Module tab. However, set up for the inband data path is machine-specific; and, in a distributed system, each machine may have different inband mode data. For example, each machine may have a different device name and port. For this reason, setting up the inband data path is now done from a machine-specific screen (the Set Up BFS Host window). As a result, the Inband Data Config button on the Application Interface Module tab has been removed.

Quick Path: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > Hosts Tab > File > New



The image shows a screenshot of the "Set Up BFS Host" configuration window. The window has a title bar with a blue icon and the text "Set Up BFS Host". The main area contains several configuration fields and options:

- BFS In-Band Mode:** Three radio buttons are present: "ATM" (selected), "ASI" (unselected), and "Ethernet" (unselected).
- Inband Device Name:** A text field containing the value "/dev/Hmux0".
- Host Name:** An empty text field.
- QAM BFS Input TSID:** An empty text field.
- RF Output TSID for BFS Port:** An empty text field.
- PSI Interval:** A text field containing the value "80", followed by the unit "msec".
- Port:** Two radio buttons are present: "0" (selected) and "1" (unselected).
- Bandwidth:** A text field containing the value "38.80", followed by the unit "Mbps".
- DNCS Host:** A checkbox that is currently unchecked.
- PAT Configuration:** A button located below the "DNCS Host" checkbox.

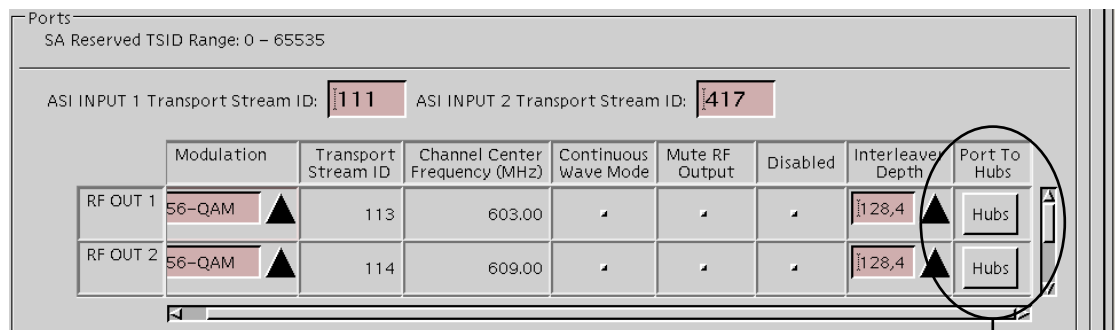
At the bottom of the window, there are three buttons: "Save", "Cancel", and "Help".

More DNCS Enhancements: Improvements Make Familiar Tasks Easier, Continued

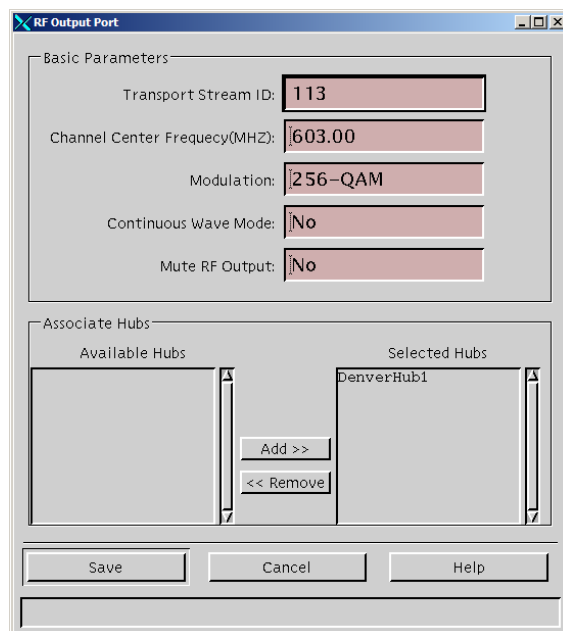
Use MQAMs and GQAMs To Feed Multiple Hubs

A new user interface allows you to associate individual RF outputs in an MQAM modulator (MQAM) with specific hubs or RF output carrier groups with hubs for GQAM modulators (GQAMs). This feature is useful in special instances where you have a need to feed multiple hubs, such as when you configure public education and government (PEG) services. Refer to the *Configuring Simulcast Services at a Sub-Hub Level Technical Bulletin* for details.

To access this new interface, click the **Hubs** button under the Port To Hubs column in the Basic Parameters tab for the Set Up MQAM window.



Click Hubs to open the RF Output Port window, where you can associate output ports with specific hubs.



When you click **Hubs**, the RF Output Port window opens.

To send data from this MQAM to only specific hubs in the headend, select the hub name in the Available Hubs field and then click Add. The hub name moves into the Selected Hubs field. Repeat this step for each hub you want to receive data from this MQAM.

If you want to send data from this MQAM to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. Any QAM with no hubs selected is considered to be feeding all hubs. This allows you to add hubs without having to modify the configuration for QAMs.

More DNCS Enhancements: Improvements Make Familiar Tasks Easier, Continued

Get Targeted Online Help Based on Your Current Task

Clicking the **Help** link on any of the WUI windows in the DNCS Administrative Console now displays help topics for the tasks you can perform from that window. For example, clicking the Help link on the Service Group Setup window displays help for adding, modifying, or deleting a service group. It also explains the differences between standalone, parent, and child service group.

You can still navigate to other Help topics using the Contents, Index, or Search features. Targeted help is available only for WUI windows.

OCAP: Support for OCAP-Based Applications Increases Options for You and Your Subscribers

Overview

In SR 4.0, the DNCS supports the OpenCable Applications Platform (OCAP™) middleware standard. As a cable service provider, your selection of portable and interoperable software is more extensive. Software suppliers are competing to develop the interactive television services and applications you and your subscribers demand. SR 4.0 adheres to OCAP standards to promote this new plug and play business model.

Where Can I Learn More?

Support for OCAP-based applications includes options for you and your subscribers when used with the OCAP Object Carousel. For more information on OCAP and the OCAP Object Carousel, refer to the following publications:

- *Configuring the DBDS System for Using the Common Download Process With OpenCable™ Hosts Application Guide*
- *OCAP Architecture Guide*
- *OCAP Installation and Upgrade Instructions*
- *TSBroadcaster User's Guide Cisco's OCAP™ Object Carousel Solution*

Additional DNCS Behavior Change in SR 4.0

Overview

A change in the DNCS IPPV polling process behavior has occurred in SR 4.0. This section provides an overview of this change.

Change in IPPV Polling Process

Prior to SR 2.5/3.5/4.0, when the DNCS received IPPV set-top billing information as a result of the IPPV Polling process, the DNCS verified that the event matched an entry in its database before sending the purchase information to the billing system. If the event ID (EID) did not match the database, the polling process did not report the purchase to the billing system and left the event on the set-top.

Beginning with SR 2.5/3.5/4.0, the DNCS now passes all Impulse Pay-Per-View (IPPV) events to the billing system and removes the events from the set-top. With this change, it is possible that a few old IPPV events that could not be validated in the DNCS database will now be passed along to the billing system. These events will upload like other events except that the package name for the old IPPV events will be reported as "Purchased Movie."

For more information about this change, refer to the *Recovered IPPV Purchases After SR 2.5 Upgrade Operations Alert Bulletin*.

Chapter 2

What Are the New Optional Features in SR 4.0?

Overview

Introduction

SR 4.0 offers several new optional features, including Direct ASI, Regional Control System (RCS), and Overlay. This chapter provides a brief description of each of these optional features.

If you are interested in any of these features, please contact your Cisco marketing representative for more information.

In This Chapter

This chapter contains the following topics.

Topic	See Page
Direct ASI: Direct ASI Replaces the BIG	2-2
Regional Control System: A New Solution for Geographic Challenges	2-3
Overlay: Deploy Cisco Set-Tops in Other Networks	2-4

Direct ASI: Direct ASI Replaces the BIG

What's Direct ASI?

You can now send BFS data directly from the DNCS to a BFS QAM modulator. Direct ASI simplifies your network by eliminating the need for a BFS BIG or for Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) between the DNCS and a BFS BIG.

Direct ASI requires a DVB-ASI card and may require additional network components. Cisco Service engineers can configure your DNCS to support Direct ASI when they upgrade your system to SR 4.0.

Due to Cisco's previously announced plans to phase out the BIG and the operations advantages of the Direct ASI configuration, sites should begin to budget and plan for this upgrade.

If you are interested in ordering this feature, please contact your Cisco marketing representative. For technical questions about migrating to Direct ASI, contact Cisco Services.

Regional Control System: A New Solution for Geographic Challenges

What's RCS?

With the RCS solution, an operator at a central DNCS can provision and manage a Remote Network Control Server (RNCS) for one or more remote sites. After each RNCS is configured, a central DNCS and Application Server can communicate with these unmanned sites across a T1-rate data link.

Each RNCS offloads tasks which were historically performed by the DNCS. For example, the DNCS is normally responsible for propagating BFS data to a given set-top population. In an RCS system, the RNCS performs this task. Additionally, with the RNCS in place, network elements can boot from and download directly from the remote platform without involving the central DNCS. The Emergency Alert System (EAS) is also local to the RNCS.

Please contact your Cisco marketing representative for more information about this feature and information about the necessary site planning requirements.

Overlay: Deploy Cisco Set-Tops in Other Networks

What's Overlay?

Overlay is an optional feature that supports deployment of Cisco set-tops in a non-Cisco network environment. With Overlay enabled on the DNCS, Cisco set-tops and non-Cisco set-tops can be mixed throughout a non-Cisco network, independent of headend, hub, or node location.

You can currently deploy the following Cisco Explorer model set-tops in an Overlay environment:

- 1850
- 3250
- 3250HD
- 8000
- 8000HD
- 8300
- 8300HD

Please contact your Cisco marketing representative for more information about this feature.

Chapter 3

What Are the Site Requirements?

Overview

Introduction

This chapter provides information to help you prepare for the SR 4.0 upgrade. Please read this entire chapter before you install SR 4.0. This chapter includes important information to help you schedule the appropriate amount of time for the upgrade.

Application Testing

Application testing for SR 4.0 was completed using a sample of applications developed for SR 2.2. SR 4.0 did not affect the functionality of the applications tested.

For More Information

If you have any questions or would like to order our products, please contact Cisco Services.

In This Chapter

This chapter contains the following topics.

Topic	See Page
Hardware and Software Requirements	3-2
Scheduling Requirements	3-5

Hardware and Software Requirements

Introduction

This section provides the hardware and software requirements you must meet before upgrading your system to SR 4.0. You can check your system against these requirements by running the Doctor report.

Running the Doctor Report

Use the following procedure to run the Doctor report on the DNCS.

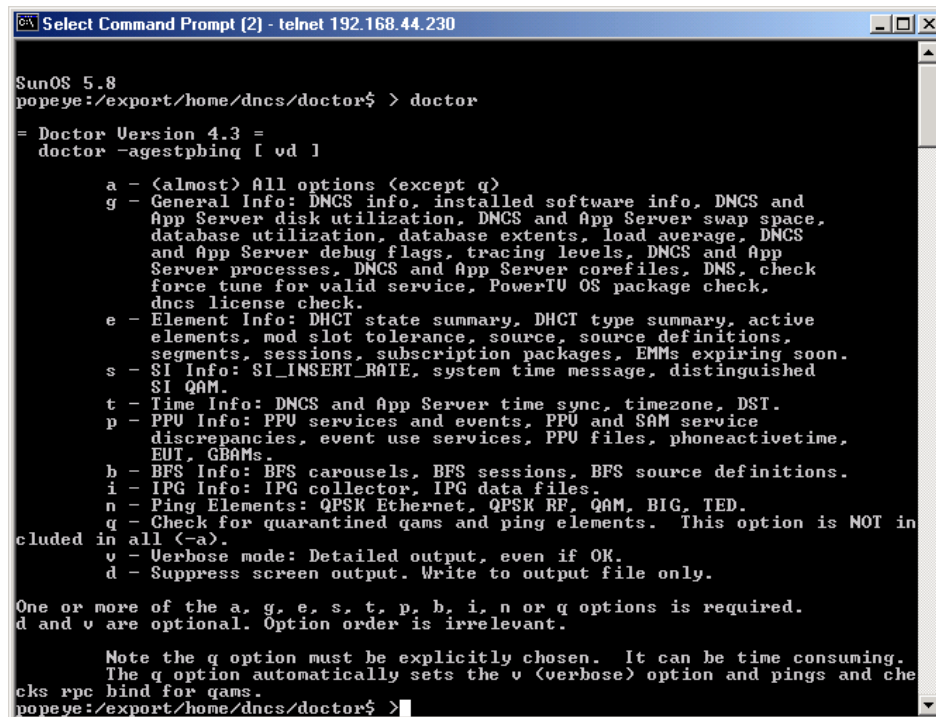
1. If necessary, open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and then press **Enter**.

Result: The /export/home/dncs/doctor directory becomes the working directory.

3. Type **doctor** and then press **Enter**.

Result: The system generates a list of parameters that you can use to run the Doctor report.

Note: Each parameter causes the Doctor report to generate output with specific configuration information.

A screenshot of a telnet session window titled "Select Command Prompt (2) - telnet 192.168.44.230". The window shows a SunOS 5.8 prompt where the user has navigated to the directory /export/home/dncs/doctor and executed the command "doctor". The output displays the "Doctor Version 4.3" and a list of options: "a - (almost) All options (except q)", "g - General Info: DNCS info, installed software info, DNCS and App Server disk utilization, DNCS and App Server swap space, database utilization, database extents, load average, DNCS and App Server debug flags, tracing levels, DNCS and App Server processes, DNCS and App Server corefiles, DNS, check force tune for valid service, PowerTU OS package check, dnscs license check.", "e - Element Info: DHCT state summary, DHCT type summary, active elements, mod slot tolerance, source, source definitions, segments, sessions, subscription packages, EMMs expiring soon.", "s - SI Info: SI_INSERT_RATE, system time message, distinguished SI QAM.", "t - Time Info: DNCS and App Server time sync, timezone, DST.", "p - PPU Info: PPU services and events, PPU and SAM service discrepancies, event use services, PPU files, phoneactivetime, EUT, GBAMs.", "b - BFS Info: BFS carousels, BFS sessions, BFS source definitions.", "i - IPG Info: IPG collector, IPG data files.", "n - Ping Elements: QPSK Ethernet, QPSK RF, QAM, BIG, TED.", "q - Check for quarantined qams and ping elements. This option is NOT included in all (-a).", "v - Verbose mode: Detailed output, even if OK.", "d - Suppress screen output. Write to output file only." The text continues with "One or more of the a, g, e, s, t, p, b, i, n or q options is required. d and v are optional. Option order is irrelevant." and a note: "Note the q option must be explicitly chosen. It can be time consuming. The q option automatically sets the v (verbose) option and pings and checks rpc bind for qams." The prompt is now "popeye:/export/home/dncs/doctor\$".

```
Select Command Prompt (2) - telnet 192.168.44.230

SunOS 5.8
popeye:/export/home/dncs/doctor$ > doctor

= Doctor Version 4.3 =
  doctor -agestphinq [ vd ]

  a - (almost) All options (except q)
  g - General Info: DNCS info, installed software info, DNCS and
    App Server disk utilization, DNCS and App Server swap space,
    database utilization, database extents, load average, DNCS
    and App Server debug flags, tracing levels, DNCS and App
    Server processes, DNCS and App Server corefiles, DNS, check
    force tune for valid service, PowerTU OS package check,
    dnscs license check.
  e - Element Info: DHCT state summary, DHCT type summary, active
    elements, mod slot tolerance, source, source definitions,
    segments, sessions, subscription packages, EMMs expiring soon.
  s - SI Info: SI_INSERT_RATE, system time message, distinguished
    SI QAM.
  t - Time Info: DNCS and App Server time sync, timezone, DST.
  p - PPU Info: PPU services and events, PPU and SAM service
    discrepancies, event use services, PPU files, phoneactivetime,
    EUT, GBAMs.
  b - BFS Info: BFS carousels, BFS sessions, BFS source definitions.
  i - IPG Info: IPG collector, IPG data files.
  n - Ping Elements: QPSK Ethernet, QPSK RF, QAM, BIG, TED.
  q - Check for quarantined qams and ping elements. This option is NOT in
cluded in all (-a).
  v - Verbose mode: Detailed output, even if OK.
  d - Suppress screen output. Write to output file only.

One or more of the a, g, e, s, t, p, b, i, n or q options is required.
d and v are optional. Option order is irrelevant.

      Note the q option must be explicitly chosen. It can be time consuming.
      The q option automatically sets the v (verbose) option and pings and che
cks rpc bind for qams.
popeye:/export/home/dncs/doctor$ >
```

4. Type **doctor -g** and then press **Enter** to view the version of DNCS software installed and the DNCS and Application Server platform, CPU, and disk information.

Hardware and Software Requirements, Continued

What to Verify Using the Doctor Report

Using the results of the Doctor report, verify that your system meets the following requirements. For detailed information on reading the data in the Doctor report, see the *DBDS Utilities 5.1 Installation Instructions and DNCS Utilities User's Guide*.

Important: DBDS Utilities 5.1 is required for SR 4.0.

DNCS System Release

Your system must be running SR 2.2 at a minimum. In the Doctor report, look for the **SAIdnccs** entry under the **All SAI Installed Package Information** section. Ensure the version is **3.0.1.16** or later. If you have installed Service Packs for SR 2.2, your version may include additional letters and numbers. For example, 3.0.1.16p7 is SR 2.2 Service Pack 2.

DNCS Hardware Requirements

Ensure your site meets the following DNCS hardware requirements before upgrading to SR 4.0.

Platform	Hard Drives	Memory (Minimum)	CPU (Minimum)
Sun Fire V880	6 X 73 GB	4 GB	2 X 900 MHz
Sun Fire V880	12 X 73 GB	8 GB	4 X 900 MHz
Sun Enterprise 450	<ul style="list-style-type: none">• 7 X 9 GB• 7 X 18 GB• 10 X 9 GB• 10 X 18 GB	1 GB	4 X 300 MHz
Sun Enterprise 250	<ul style="list-style-type: none">• 2 X 9 GB• 2 X 18 GB	1 GB	2 X 300 MHz

Application Server Hardware Requirements

Ensure your site meets the following Application Server hardware requirements before upgrading to SR 4.0.

Note: If you are using another vendor's application server, contact the vendor to ensure the hardware and software compatibility with Cisco's SR 4.0.

Platform	Hard Drives	Memory (Minimum)	CPU (Minimum)
Sun Blade 150	1 X 40 GB	512 MB	1 X 550 MHz
Sun Ultra 5	1 X 20 GB	256 MB	1 X 333 MHz

Hardware and Software Requirements, Continued

Application Platform Release Dependencies

The following table shows the application platform release dependencies for SR 4.0.

Important: You must have these versions of application platform software *or later* installed on your system prior to upgrading to SR 4.0. If you do not install the correct application platform software *before* you upgrade to SR 4.0, subscribers may see video freezing and black screens when using video-on-demand (VOD) or anything-On-Demand (xOD) applications.

Set-top Platform	Operating System (Minimum)	SARA (Minimum)
8300 DVR 1.3.1a17 (or later)	6.14.10.1	1.87.14.1
8000/8010 DVR 1.3.1a17 (or later)	6.12.7.1	1.87.13.1
3250HD MR4 P1 (or later)	3.12.8.1	1.57.8.1
2xxx, 31xx, 3200, 3100HD	3.10.9	1.54.23.1
Pace	Pace to Provide OS Build	N/A
Pioneer	Pioneer to Provide OS Build	N/A

Scheduling Requirements

How Long Does It Take to Complete the Upgrade?

With the live upgrade, your site only needs to be down for 2 to 3 hours during the entire upgrade process. Most of the upgrade procedures have no system impact. The pre-install and pre-upgrade steps can be performed at any time of day. However, the actual upgrade process normally takes place during a maintenance window beginning at midnight. The following table provides a breakdown of each upgrade process.

Process	Length of Time	Activity
Pre-install	1-3 hours	Activities are performed by Cisco Services, including checking the overall health of the system. These activities do not impact the system.
Pre-upgrade	3-4 hours	Backing up the system: <ul style="list-style-type: none">• Back up the system components• Back up the DNCS and Application Server files• Complete system checks These activities do not impact the system.
Upgrade	6-8 hours total; 2-3 of these hours require system outage Note: Actual time may vary based on the number of devices being upgraded.	Upgrade the DBDS network: <ul style="list-style-type: none">• Back up the DNCS database• Install the DNCS and Application Server software• Determine which optional features (licensed or unlicensed) need to be enabled as a result of this upgrade• Install and download the component software (QAM, MQAM, GQAM, and QPSK modulator)• Reboot the hardware• Complete functional checks QPSK modulator upgrades and some QAM and MQAM upgrades can be completed with little or no subscriber impact. However, 2 to 3 hours of the upgrade require system outage.
Post-Upgrade	3-4 hours	Back up the system: <ul style="list-style-type: none">• Back up the file system• Back up the DNCS database These activities do not impact the system.

Chapter 4

What CRs Are Included in SR 4.0?

Overview

Introduction

This chapter describes change requests (CRs) that were found in previous system releases and corrected in SR 4.0 to improve operational performance of the DNCS.

In This Chapter

This chapter contains the following topics.

Topic	See Page
Issues Corrected in SR 4.0: The Short Story	4-2
Want to Know More?	4-3

Issues Corrected in SR 4.0: The Short Story

Overview

If you want to see if a specific CR was fixed in this release, refer to the following quick reference list. If you would like to review CRs in more detail, the next section provides descriptions of each issue corrected in SR 4.0.

Quick Reference to Issues Corrected in SR 4.0

The following list provides a one-line description of each fix that was implemented in this release.

CR Number	Short Description of Fix
CR 31239	Session List WUI Now Displays Filtered Count Value
CR 39488	Option -a Removed from clearDbSessions Utility
CR 49483	Improved Performance for the camEx Process
CR 49570	Memory Issues with camEx Process Corrected
CR 49972	PPV Free Preview Window No Longer Displays Black Screen
CR 50834	siManager Process Restarts Automatically
CR 52619	Set-tops Correctly Booting in DOCSIS Mode
CR 52829	Hundreds of "sh*" Files in the /tmp Directory Now Automatically Deleted
CR 52833	Encrypted Service Content Does Not Go in the Clear When sgManager Refresh Cache Sent

Want to Know More?

Overview

This section provides more detail about each fix in SR 4.0. The descriptions in this section are not intended to be comprehensive. If you have additional questions about a particular change request, contact Cisco Services.

Session List WUI Now Displays Filtered Count Value

The Session List WUI now shows the Filtered Count value for sessions. **CR 31239** corrects this issue in the DNCS.

Option -a Removed from clearDbSessions Utility

The clearDBSessions utility removes orphaned and completed sessions from the DNCS database. The -a option removes all sessions in the system including video and audio sessions. If the -a option was used accidentally, all sessions would have to be set up again, resulting in significant system down time. **CR 39488** removes this option from the clearDBSessions utility.

Improved Performance for the camEx Process

The camEx process performance throughput was improved with SR 4.0. **CR 49483** corrects this issue with the camEx process.

Memory Issues with camEx Process Corrected

Various memory leaks within the camEx process resulted in slower processing time. **CR 49570** corrects these memory issues with the camEx process.

PPV Free Preview Window No Longer Displays Black Screen

Previously, subscribers were seeing a black screen instead of video in the PPV free preview window. **CR 49972** corrects this issue in the DNCS.

siManager Process Restarts Automatically

If the siManager process unexpectedly shuts down, the process is designed to restart automatically. Previously, if the siManager process shut down more than three times in a row, the process would not restart automatically. If you did not manually restart the siManager process, set-tops that rebooted would not have system information. **CR 50834** corrects this issue in the DNCS.

Want to Know More?, Continued

Set-tops Correctly Booting in DOCSIS Mode

A condition was reported where unknown DCM information was being sent to set-tops. As a result, these set-tops would not correctly boot up in DOCSIS mode.

To address this issue, reported in **CR 52619**, Cisco added the Digital Storage Media – Command and Control (DSM-CC) message header to the UNConfig message.

Hundreds of “sh*” Files in the /tmp Directory Now Automatically Deleted

Previously, an issue within the dnscSetup script would cause hundreds of temporary sh* files (sh followed by 5 digits) to be created in the /tmp directory. These files would not automatically be removed, and the /tmp directory would contain hundreds of sh* files. To remove the files, you had to manually delete the temporary sh* files from the /tmp directory. **CR 52829** corrects this issue in the DNCS.

Encrypted Service Content Does Not Go in the Clear When sgManager Refresh Cache Sent

Previously, the sgManager would intermittently send a refresh cache to the drm that caused a mismatch between the drm and dsm. This mismatch would result in segment information not being sent to the bsm; therefore, the content could go out in the clear. **CR 52833** corrects this issue in the DNCS.

Chapter 5

What Are the Known Issues for Standard SR 4.0?

Overview

Introduction

This chapter provides a summary of known issues for the standard version of this software release.

Note: For a summary of known issues related to optional software features, see Chapter 6, **Known Issues for Optional Features**.

For More Information

The lists in this chapter are not intended to be comprehensive. If you have questions about a particular change request, contact Cisco Services.

In This Chapter

This chapter contains the following topic.

Topic	See Page
Known Issues in the Standard Version of SR 4.0	5-2

Known Issues in the Standard Version of SR 4.0

Introduction

Resolutions to the following system release issues are currently in development at Cisco.

CR 42202: DSI Messages Being Sent Outside Carousel Bit Rate Partitions

Download Server Initiate (DSI) messages are sent outside the carousel bit rate partitions. This results in a slightly higher bandwidth rate on the carousel packet identifier (PID). Because the bandwidth used falls within the allowed SI bandwidth, the overall stream bandwidth is not affected.

Workaround: No workaround is required if you are using a standalone carousel. If the carousel bandwidth must fall within a prescribed limit, then reduce the nominal carousel bandwidth by 16000 bits per second (bps).

CR 50885: Issue with CableCARD Servers Operating in Daylight Savings Time Mode

This CR describes a corner case. If a system's CableCARD server authorization timeout period is set as 1 hour, and that system is operating in Daylight Savings Time (DST) mode, the "Copy Protection Authorization" message is not sent to the CableCARD module's host device. As a result, the host device is not authorized to receive copy protected content.

Workaround: If this issue is detected on your system, perform one of the following steps to correct the issue:

- Define the Authorization and Deauthorization timeout periods as 2 hours or greater
- Bounce the DNCS SOAP Servers

CR 51869: EMMs Do Not Increment After Selecting DHCT Instant Hit Option

When you add a package and select the DHCT Instant Hit option, the EMM count will not increase.

CR 51897: DHCT Provisioning Window Does Not Display "DOCSIS DSMCC Initialized Failed" Message

If a set-top fails to sign on to the DNCS in DOCSIS mode, the DHCT Provisioning window for that set-top incorrectly displays the message "DOCSIS DSMCC Initialized." You cannot see that the word "Failed" is included at the end of the message, and you do not have the ability to click within the message field and view the entire status message.

CR 52037: CCardServer Process Does Not Delete Manually-Created mmi.txt and gfc.txt Files

In previous software versions, the mmi.txt and gfc.txt files were manually created through the BFS Client UI. These text files are now automatically created as a part of the CCardServer process.

If old mmi.txt and gfc.txt files exist on your system, these old files will not be deleted and replaced with the new text files. As a result, CableCARD modules will not receive updated file information for the RF Output or Authorization Phone Number values.

Known Issues in the Standard Version of SR 4.0, Continued

CR 54437: EAS Message Window Shows “Send Message Failed” Error

When an EAS message is sent to a set-top tuned to a digital channel, the set-top will pass the message to the TV for display, but the EAS Message window on the DNCS displays a “Send Message Failed” error message.

CR 54547: dncsControl Does Not Stop SOAP Server’s Child Processes

If you use the dncsControl command to stop the DNCS processes, the SOAP Server’s managing server process will stop, but any “child” SOAP Server processes will continue to run. When you use dncsControl to restart the DNCS processes, the SOAP Server’s managing server process will not restart, and the GUI Servers WUI page will not open.

CR 54916: DHCT Groups UI Allows New Groups with Duplicate or Invalid Group IDs to be Saved

When you enter and save duplicate or invalid Group ID values, the Set Up DHCT Group window displays a “Save Failed” message without any explanation as to why the save failed. Also, the duplicate or invalid Group ID values are inserted into the pdoshct table, even though the UI indicated that the save failed.

CR 54917: Set Up DHCT Group UI Changes Group ID Value During Save Without Notifying User

When you create a new DHCT Group within the Set Up DHCT Group window, do not enter group ID values greater than 32768. Downloads to group ID values greater than 32768 will not occur.

CR 55981: qamManager UI Exits Unexpectedly

This CR describes a corner case. The qamManager UI can exit unexpectedly if you attempt to delete an object that is in the process of being deleted.

CR 56569: QAM Source UI Does Not Recognize QAMs Connected to BFS BIG

When upgrading from SR 2.2 to SR 4.0, the sessions for any third-party applications that use ATM PVC routed through the BFS BIG and the QAM cannot be restarted. In the event of this issue, the session UI displays a “No QAMs available. Check bandwidth and connectivity of session elements” message.

Workaround: A correction to this CR is available through an emergency software patch. Contact Cisco Services for more information.

Chapter 6

What Are the Known Issues for Optional Features in SR 4.0?

Overview

Introduction

This chapter provides a summary of known issues related to optional features. These CRs only apply if you have the RCS optional feature.

For More Information

The lists in this chapter are not intended to be comprehensive. If you have questions about a particular change request, contact Cisco Services.

In This Chapter

This chapter contains the following topics.

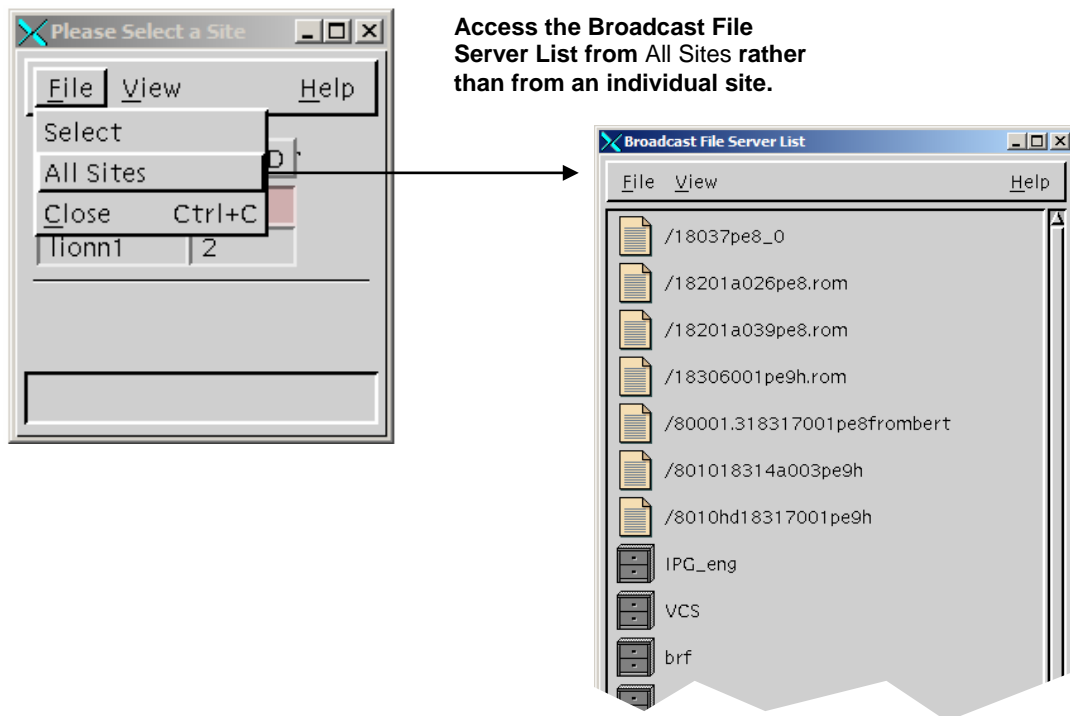
Topic	See Page
Known Issues for RCS in SR 4.0	6-2

Known Issues for RCS in SR 4.0

CR 48374: BFS Elements Created from All Sites Must Be Edited from All Sites

If you create links, files, directories, servers, and sources using the All Sites feature from the BFS Client, you must make any changes to these elements through the Broadcast File Server List for All Sites. Changes you make to these BFS elements from All Sites are propagated to all of the individual sites by the bfsServer process.

If the BFS elements were originally propagated using the All Sites feature, deleting or editing these elements from individual sites can result in error conditions, such as missing or broken links, that prevent set-tops from receiving BFS services.



Important: If you did *not* use the All Sites feature to create BFS elements, edit those elements from the individual sites as necessary.

CR 50551: Emergency Alert Messages Are Not Filtered on the Inband Path

The FIPS code filtering is currently only done OOB per QPSK/CMTS. However, hosts without CableCARD modules receive all Emergency Alert Messages through the inband path. In the RNCS architecture, this means if Site2 in Florida receives a tornado warning, Hosts without CableCARD modules at Site3 in Colorado will also receive the warning.

Known Issues for RCS in SR 4.0, Continued

CR 50771-01: Incorrect Site IDs Affect Alarms for RNCS Systems

Site IDs for RNCS devices are reported correctly in the DNCS database. However, site IDs in the RNCS database are incorrect. For example, if the site ID for a QAM connected to a RNCS is 2, the site ID is 2 in the DNCS database. However, the site ID in the RNCS database is 1.

Given these incorrect site IDs, the RNCS cannot detect when a device, such as a QAM, should be part of its system. As a result, alarms are not issued in Alarm Manager if the device experiences issues, such as failure to connect.

CR 53407: dnscs_host Alias Added To /etc/host Files For RNCS and Object Carousel

The ntp.conf file uses the dnscs_host alias for its server. The dnscs_host alias was added to the /etc/host files for the RNCS and the Object Carousel to allow the ntp.conf file to work correctly.

Chapter 7

Customer Information

If You Have Questions

For More Information

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

Appendix A

What's Installed with SR 4.0?

Overview

Introduction

This appendix provides a table of the versions of software that will be installed after you upgrade to SR 4.0.

Important: This appendix provides versions for software installed with the base SR 4.0 system. If you have optional features, such as Direct ASI, Overlay, or RCS, check your documentation for these features for version information.

In This Appendix

This appendix contains the following topics.

Topic	See Page
A Snapshot of Your System Post-Upgrade	A-2

A Snapshot of Your System Post-Upgrade

Post-Upgrade Version Information

The following table lists the software versions that are installed or included with base SR 4.0. If you have optional features, such as Direct ASI, Overlay, or RCS, you may have additional components installed. For version information on optional features, check the documentation for the optional feature.

DBDS Component	Version #
DNCS	
Application	4.0.0.27
GUI	4.0.0.27
WUI	4.0.0.27
DNCS Application Patch CD	4.0.0.27p3
DNCS Support Software	
DNCS/App Server Tools	3.5.0.7
DNCS Spectrum Kit	2.0.0.8
Report Writer	3.5.0.2
Online Help	3.5.0.3
DBDS Maintenance CD	
Backup/Restore CD	6.0.6
Unipack Install Scripts	1.3.0.12
DBDS Utilities CD	
DNCS Utilities	5.1.0.6
Cool Tool (CT) Utilities	5.1.0.3
DHCT Status	5.1.0.3
Doctor	5.1.0.4
Spectrum Installation	
Spectrum Enterprise Manager App Version	5.0 R1
Spectrum Supplement App.	CS3/MMS3 P122

A Snapshot of Your System Post-Upgrade, Continued

DBDS Component	Version #
DNCS Platform	
Platform	3.5.0.3
Solaris	8 02/02
Solaris 8 Recommended/Security Patches	3.5.0.3
Prom Patches	2.3
Fore ATM Drivers	3.0.1.2
Informix	9.20 uc3
Video Propulsion DVB Direct ASI	1.0.0.5
Application Server	
Application Server	3.1.5.3
Application Server Support Software	
DNCS/ App Server Tools	3.5.0.7
QAM CD	
Application	2.4.0a
MQAM	
Application	2.5.0a
GQAM CD	
GQAM	1.2.0
GoQAM	
GoQAM RF	1.1.0
GoQAM IF	1.1.0
QPSK Modulator/Demodulator	
QPSK Modulator	C70
QPSK Demodulator	A62

A Snapshot of Your System Post-Upgrade, Continued

DBDS Component	Version #
ATM/BFS BIG	
MSYNC Control Card D9711 App	2.25
MSYNC Control Card D9711 Boot	0.75
ATM OC3 Card D9722 Application	3.01.0
SWIF Receiver Card D9730 Application	2.02
SWIF Transmitter D9714 Application	2.03
Grooming BIG	
MSYNC Control Card D9711-2 App	3.01
MSYNC Control Card D9711-2 Boot	0.75
GPI Card D9746 App	0.8.2
GPI Card D9746 Boot	0.6.7
AutoMux Script	2.3
Sonet	
SONET/ASI (STA)	1.3.4



Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2006, 2012 Cisco and/or its affiliates. All rights reserved.

April 2012 Printed in USA

Part Number 4001703Rev B