System Release 5.0 Release Note

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. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

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

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. (1009R)

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

Contents

About This Guide

Introduction

System Release 5.0 (SR 5.0) is a release of Cisco's Digital Broadband Delivery System (DBDS) software. This release note contains the following information:

- New feature descriptions
- Media and software versions for this release
- Site requirements
- Descriptions of closed and open CRs (Change Requests)
- General information on contacting Cisco® Systems

Purpose

The purpose of this release note is to inform system administrators contemplating an upgrade of the new features, known issues, related documents, and upgrade notes for SR 5.0.

Audience

This document was written for system operators. Field service engineers and Cisco Services engineers may also find the information in this document helpful.

Document Version

This is the first formal release of this document.

1

Highlights

Introduction

New features and product improvements for SR 5.0 are described in this chapter.

In This Chapter

Internet Protocol Version 6

SR 5.0 now supports Internet Protocol version 6 (IPv6) as well as IPv4. IPv6 has a vastly larger address space than IPv4 (128 bits vs. 32 bits), which provides greater flexibility in allocating addresses. Network security is also integrated into the design of the IPv6 architecture.

The following systems and subsystems within the DBDS support IPv6.

System or Subsystem	Supported IP Versions
DOCSIS® set-tops	■ IPv6 ■ IPv4 ■ Dual-stack IP
Unicast traffic	■ IPv6 ■ IPv4
DNCS	■ IPv6 (static addresses) ■ IPv4 (static addresses) ■ Dual-stack IP
Headend components that interact with the DHCT (USRM, SDV server, CMTS, VOD server)	■ IPv6 (static addresses) ■ IPv4 (static addresses) ■ Dual-stack IP **Note**: These components present both IPv6 and IPv4 addresses to the DNCS for information and storage.

For more information, see **IPv6** in *System Release 5.0 Online Help* (part number 4038475).

Enhanced User Level Security

User level security has been enhanced for SR 5.0 by implementing the Solaris 10 operating system "Secure by Default" feature, which disables unnecessary and insecure network services. Also, the generic DNCS user has been converted to a role. This allows system administrators to assign full or partial control of selected parts of the system to individual users. Session security and password management have also been enhanced.

For more information, see the *DNCS System Release 5.0 Security Configuration Guide* (part number 4034689).

Support for LDAP and RADIUS

Since user accounts are now role-based, it is possible for system administrators to define a large number of users across an enterprise network. To address the accompanying issues, SR 5.0 supports the following protocols:

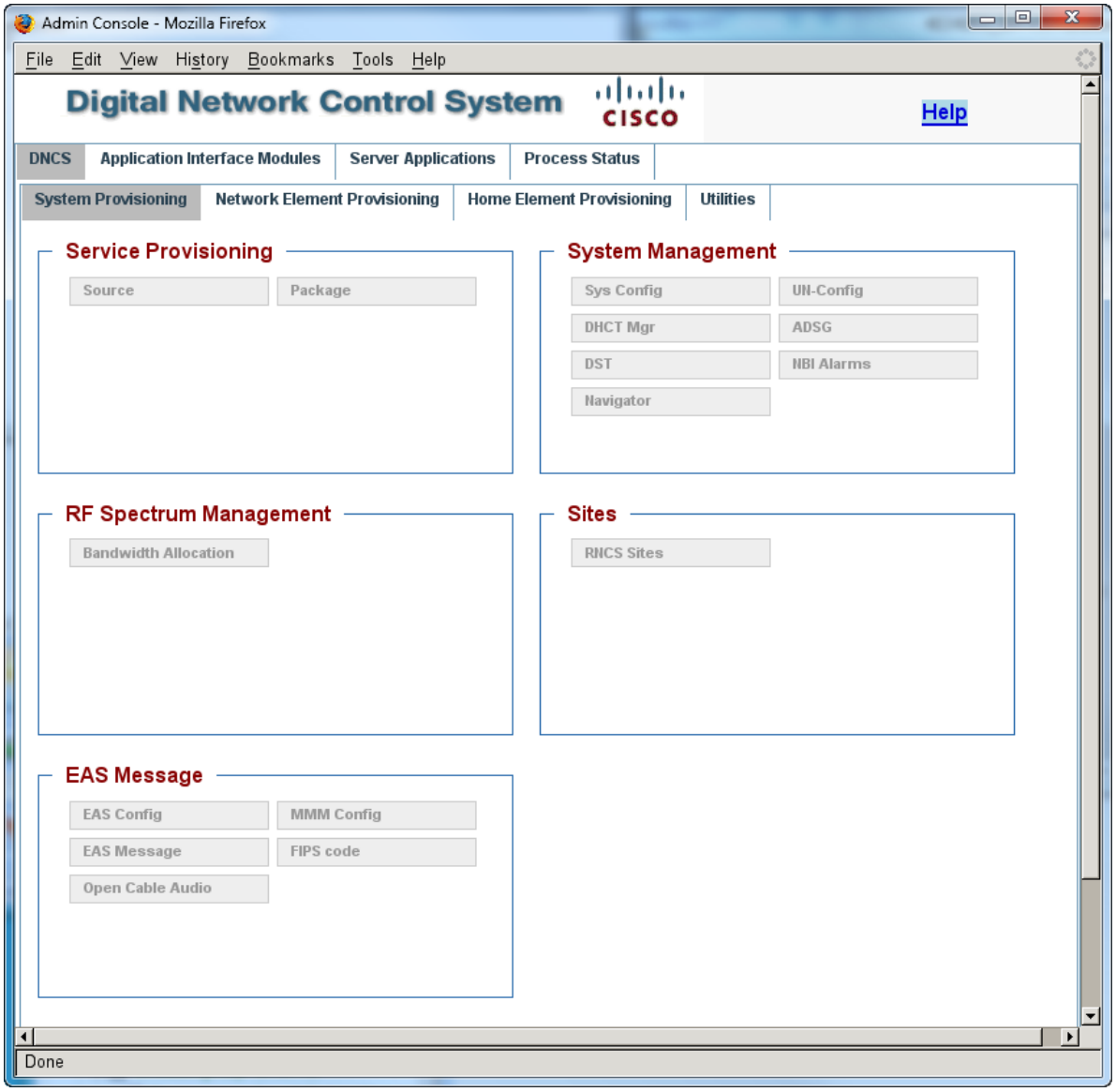
- Remote Authentication Dial In User Service (RADIUS) protocol, which is a client/server protocol that provides centralized Authentication, Authorization, and Accounting (AAA) service
- Lightweight Directory Access Protocol (LDAP), which is an application protocol that queries and modifies directory entries in a directory server

For more information, see *Enable RADIUS and LDAP Support in a DBDS for SR 5.0 Configuration Guide* (part number 4017610).

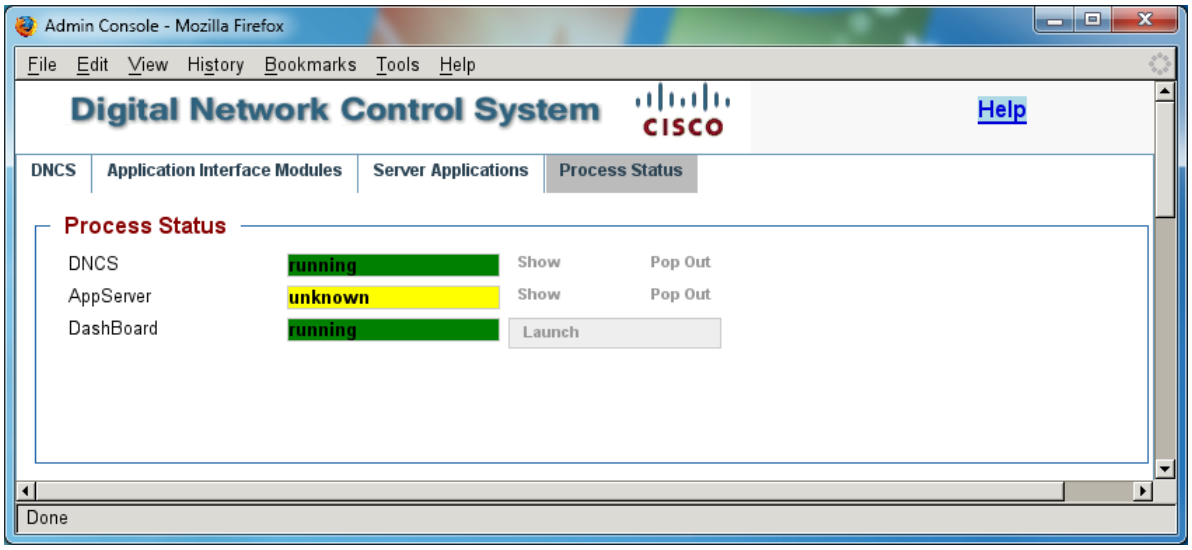
Web Browser-Based User Interface

A web browser-based user interface (WUI) has replaced the DNCS GUI for SR 5.0. All windows have been converted to web pages and the Online Help and user documentation have been updated accordingly. Where possible, the previous design and hierarchy have been retained in order to make the transition for operators as smooth as possible.

To access the Administrative Console, open an xterm window, type **admincon**, and press **Enter**. The Administrative Console looks like this:



Note: A Console Status window does not open by default when you open the Administrative Console. Instead, the WUI equivalent is accessed by pressing the **Process Status** tab at the top of the Administrative Console. The Process Status window looks like this:



For more information, see **What's New In This Release?** in *System Release 5.0 Online Help* (part number 4038475).

RF Gateway 1 VOD Support

The DNCS now supports all inputs on RF Gateways that service VOD sessions. Additionally, the DNCS prevents input overflows and can load-balance inputs.

The Cisco RF Gateway 1 is a fully-featured universal edge QAM (U-EQAM) solution for the convergence of high-speed and high-bandwidth data and video distribution at the edge of the cable access network. The device offers high density (48 QAMs per rack unit), improved reliability, superior RF performance, and 1 GHz RF output.

The DNCS treats the RF Gateway 1 as a generic QAM. For more information, see *Generic QAMs* and *Generic QAM Model List Window* in the DNCS Online Help. For installation and operation instructions, see the *Cisco RF Gateway 1 System Guide*, part number 4024958 and the *Cisco RF Gateway 1 Configuration Guide*, part number 4025112.

Optionally Integrated Application Server

SR 5.0 allows for the Application Server to be optionally installed on the DNCS platform, eliminating the need for a separate Application Server platform. Configuration and operational procedures are identical, no matter which platform hosts the application.

For more information, see the *Application Server 5.0 Configuration Guide* (part number 4038960).

Sun Explorer Tool

SR 5.0 includes the Sun Explorer tool, a data collection utility that provides diagnostic information for troubleshooting Sun systems. To learn more about Sun Explorer, go to http://docs.sun.com/app/docs/doc/819-6614/6n8k8pjc4?a=view and download the Sun Explorer FAQ document.

Net SNMP

SR 5.0 supports Net-SNMP, a suite of applications and libraries used to implement SNMP v1, SNMP v2c and SNMP v3. Net-SNMP lets you manage any or all of the DBDS network elements with an SNMP-based NMS (Network Management System).

The Net-SNMP suite includes the following:

- Command-line tools to retrieve information from SNMP-capable devices
- An extensible agent (snmpd) for responding to SNMP queries
- A library API for developing new SNMP applications

The North Bound Interface (NBI) and other SNMP applications on the DNCS use the library and the extensible agent in their implementation. For more information, see the *DBDS SNMP Administration Guide* (part number 4038396).

Replicated Database

The Replicated Database (RepDB) package has two components:

- The IBM Informix Dynamic Server Data Replication for the database
- The rsync utility — a fast and versatile remote file-copying tool for file systems

Data replication allows a copy of the database from a primary server to be maintained on a secondary server. When activated, the primary database server continuously replicates data between itself and the secondary server by sending copies of the logical-log transactions to the secondary database server.

The rsync utility allows a copy of file systems from a primary server to be maintained on a secondary server. When activated, the rsync utility periodically synchronizes files and directories from the primary server to the secondary server.

Additionally, RepDB addresses Mean Time to Recovery (MTTR) and is the replacement for Disaster Recovery, which is being EOL'd.

For more information, see *Installing and Operating the Replicated Database Package on the DNCS Installation Guide* (part number 4034803).

PSIP/EAS Aggregation

SR 5.0 now supports PSIP (Program System Information Protocol) and EAS (Emergency Alert System) aggregation for customer DTAs and QAM tuner-equipped TVs. PSIP data is a requirement of the digital broadcast stream that includes channel information for the EPG (Electronic Program Guide) option.

For more information, see **PSIP/EAS Tab - Content GQAM Modulator** in *System Release 5.0 Online Help* (part number 4038475).

Gigabit Ethernet BFS

SR 5.0 now supports direct delivery of inband broadcast file system (BFS) data to the BFS QAM via Gigabit Ethernet. Currently, inband BFS data is delivered to the QAM via a BIG or an ASI card on the DNCS host. Both methods require expensive additional hardware and software. The Gigabit Ethernet BFS feature eliminates the need for an ASI or ATM interface, though ASI is still supported in SR 5.0.

Each BFS session is a single-program transport stream (SPTS) with its own program number and a distinct destination IP address. The uniqueness of the program number and IP address is maintained per site. Program association table (PAT) and program map table (PMT) data is sent for each session individually to the session's destination IP address.

For information on how to configure GbE BFS, see **Adding a BFS GQAM Modulator Using the GigE Port** in *System Release 5.0 Online Help* (part number 4038475).

2

Site Requirements

Introduction

This chapter provides information to help you prepare for the upgrade to System Release 5.0. Read this entire chapter before you upgrade.

If you have questions or would like to order our products, please contact Cisco Services at 1 866 787-3866.

In This Chapter

Upgrade Logistics

Introduction

This section contains information that can help system operators plan the upgrade to SR 5.0.

Supported Upgrade Path

Note these important upgrade requirements:

- Systems that upgrade to SR 5.0 must currently be operating with system software from SR 4.3, as well as DHCT client operating system (OS) 3.1 or later.
- The upgrade software is on a CD. For upgrade instructions, refer to *DVD Upgrade Installation Guide for System Release 5.0 with Integrated Application Server* (part number 4035749). Rollback procedures and software are also provided in the event that the upgrade is unsuccessful.
- You must already have the DBDS Utilities software installed on the DNCS and should have already run the pre-upgrade checks to ensure system compatibility with SR 5.0 CD upgrade requirements. Refer to *DBDS Utilities Version 6.4 Installation Instructions and User Guide* (part number 4040232) for instructions on installing and executing the DBDS Utilities.

Time to Complete

The entire upgrade to SR 5.0 must be completed within a single maintenance window that usually starts around midnight. A few pre-upgrade procedures, consisting mainly of system checks, backups, and various operations upon the metadevices of the DNCS, can be completed *before* the maintenance window begins.

Cisco engineers have determined that a typical site can be upgraded within one maintenance window. See ***Scheduling Requirements*** (on page 19) for additional details.

System Performance Impact

Interactive services will not be available during the maintenance window.

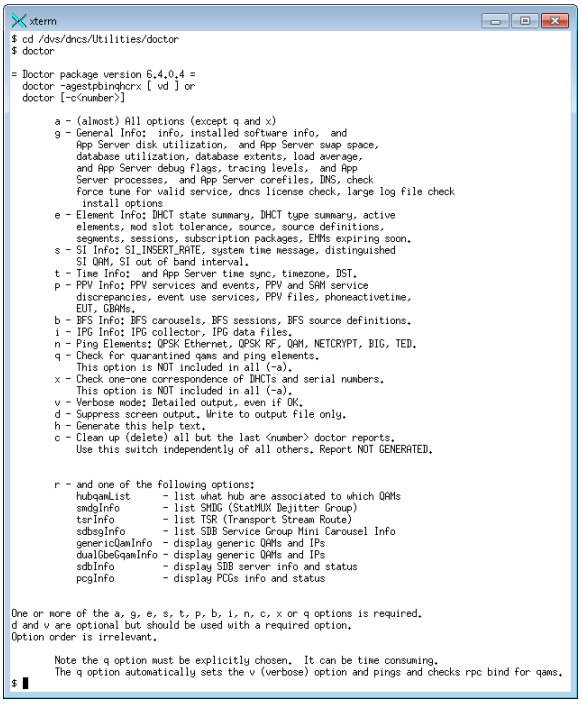
DNCS and Application Server Hardware Platforms

Introduction

This section describes the hardware configurations that are supported by SR 5.0.

Running the Doctor Report

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/Utilities/doctor** and then press **Enter**. The /dvs/dncs/Utilities/doctor directory becomes the working directory.
3. Type **doctor** and then press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report. Each parameter causes the Doctor Report to generate output with specific configuration information.



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

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 Version 6.4 Installation Instructions and User Guide* (part number 4040232).

Important: DBDS Utilities 6.4 is required for SR 5.0.

DNCS System Release Required

Your system must be running SR 4.3. In the Doctor Report, look for the **SAIdncs** entry under the **All SAI Installed Package Information** section. Ensure the **SAIdncs** version is 4.3 or later. If you have installed Service Packs for your system release, your version may include additional characters.

DNCS Hardware Configurations

Ensure your site meets the following DNCS hardware requirements before upgrading to SR 5.0. The following table lists the minimum requirements for the DNCS hardware platforms that are supported by SR 5.0.

DNCS Server Platform	Hard Drive Configuration	Memory	Processor
Sun Fire V445	■ 4 X 73 GB	■ 4 GB min	■ 2 X 1.5 GHz min.
Sun Fire V890	■ 6 X 146 GB ■ 12 X 146 GB	■ 8 GB min. ■ 16 GB min.	■ 4 X 1.5 GHz min. ■ 2 X 1.5 GHz min.
Sun Fire V880	■ 12 X 73 GB ■ 6 X 73 GB	■ 8 GB min. ■ 4 GB min.	■ 4 X 900 MHz min. ■ 2 X 900 MHz min.

Application Server Hardware Configurations

The following table lists the Application Server hardware platforms that are supported by SR 5.0.

Application Server Platform	Hard Drive Configuration	Memory	Processor
Sun V240	2 X 36 GB min.	512 MB min.	1 X 1.34 GHz min.
Sun V245	2 X 73 GB min.	2 GB min.	2 X 1.5 GHz min.
Sun Blade 150	1 X 20 GB min.	512 MB min.	1 X 550 MHz min.
Sun Ultra 5	1 X 18 GB min.	256 MB min.	1 X 333 MHz min.

Application Platform Release Dependencies

The following table shows the application platform release dependencies for this software.

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

Set-Top Platform	Operating System (OS)	SARA	PowerKEY® Conditional Access Version
Explorer RNG200 DVR 1.5.5.1003 or later	OS 8.0.40.1	1.90.12.1	N/A
Explorer 4250HDC Exp 2.0.0 (0701) or later	OS 6.20.28.1	1.61.5a100	4.0.1.1
Explorer 8300HDC DVR 1.5.3 (0801) or later	OS 6.20.28.1	1.90.5a101	3.9.7.13
Explorer 8300 DVR v. 1.4.3a10 or later v. 1.5.2	 OS 6.14.74.1 OS 6.14.79.1	 1.88.22.1 1.89.16.2	 3.9 3.9
Explorer 8000/8010 DVR v. 1.4.3a10 or later v. 1.5.2	 OS 6.12.74.1 OS 6.12.79.1	 1.88.22.1 1.89.16.2	 3.7.5 3.7.5
Explorer 3250HD HD 1.6.0 or later	OS 3.24.5.2	1.59.18.1	3.9
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.13.6.1	1.60.6.2	1.0.6.20 (Explorer 2000s) 1.0.7 (all others)

Scheduling Requirements

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.

Process	Length of Time	Activity
Pre-upgrade	3-4 hours	Backing up the system: ■ 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: ■ 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, 2-3 hours of the upgrade require system outage.
Post-Upgrade	3-4 hours	Back up the system: ■ Back up the file system ■ Back up the DNCS database These activities do not impact the system.

Software Configuration

Introduction

This section lists the software versions in each media kit supplied with SR 5.0.

Antecedents

This release succeeds and carries forward all of the enhancements, features, and improvements of previous system releases and related service packs.

Software Versions

The following table lists the configuration of headend components *after* the upgrade to SR 5.0.

DBDS Component	New Version Number
DVD/UniPack	
UniPack Core	4.1.36
SR DVD	5.0.0.27
Backup/Restore	6.0.39
DNCS	
Application (SAIdncs)	5.0.0.22
GUI (SAIgui)	5.0.0.22
WUI (SAIwui)	5.0.0.22
Application Patch	5.0.0.22P2
DNCS Support Software	
DBDS Utilities (SAIdbdsutils)	6.4.0.8
DNCS Report Writer (SAIrptwrt)	2.0.0.11
DNCS Online Help (SAIhelp)	5.0.0.5
Maintenance CD	
Unipack Install Scripts	N/A
Backup / Restore Scripts	N/A
Spectrum	
Spectrum (SAIspec)	N/A
Spectrum Kit (SAIspkit)	N/A
Spectrum Support (SAIspsup)	N/A
Platform	
Platform (SAIcomplat/SAIdnapp)	3.0.27
Solaris	10 10/09 (U8)
Solaris 10 Recommended / Security Patches	10.20100322.2-20110309
Informix IDS	N/A
Tools (SAItools)	4.2.1.35
ASI Drivers (SAIasi)	1.0.0.7
ATM Drivers	N/A

DBDS Component	New Version Number
QPSK Mod/Demod	
QPSK Mod/Demod (SAIqpsk)	G13
QAM	
QAM App (SAIqam)	2.5.8
MultiQAM	
MQAM App (SAImqam)	2.7.2
GQAM	
GQAM (SAIgqam)	4.4.7
GoQAM RF / GoQAM IF	
GoQAM RF / GoQAM IF (SAIgoqam)	1.1.4
SCS MQAM	
SCMQAM (SAIscmqam)	5.0.5
Netcrypt	
Netcrypt Bulk Encryptor (SAIncrypt)	1.3.4
Command2000	
Command2000 (SAIcmd2k)	3.0.0.8
Replicated Database	
RepDB	1.1.0.2
TED Updater	
TED Updater (SAITedUpd)	3.1.0.8
Application Server	
AS Application (SAIapp)	5.0.0.11
AS Platform	3.0.27
AS Tools	4.2.1.34
AS Application Patch	5.0.0.11p1
RNCS	
Platform (SAIcomplat)	3.0.10

DBDS Component	New Version Number
LIONN (SAIlionn)	5.0.0.22
Tools (SAItools)	4.2.1.35
ASI Drivers (SAIasi)	1.0.0.7

3

Implemented and Open CRs

Introduction

This section contains information on implemented and open CRs for SR 5.0.

If you have questions or would like to order our products, please contact Cisco Services at 1 866 787-3866

In This Chapter

Implemented System CRs

The following report contains a list of System CRs that have been implemented in this release. All of them are fixes for software defects except where noted. The CRs are indexed by ID number in ascending order.

CR ID	Title
CSCtq48022	dbUIServer cored while resetting QPSK Demodulator
CSCtq86400	TSID's Not Excluded When Added To TsidsToExclude.txt
CSCtq87218	Clear Sessions Sent To pkeManager
CSCtq92618	DNCS 5.0 Bandwidth Allocation not showing correct values
CSCtr18030	Restoring DB table backups using 'mvsrcid.sh' deletes all SAM entries
CSCtr18107	QamManager core on ECM delivery timeout
CSCtr27774	AppServer has a bfsRemote configured with a state of stopped
CSCtr33600	DRM does not recover VOD sessions on RFGW single element sessions
CSCtr35684	Doctor erroneously flag bootloader entry as BFSDir entry
CSCtr48390	(dbdsutil/6.4.0.8) Fix path issue. (mvsrcid.sh)
CSCtr53953	PkeManager has wrong bandwidth at startup for noncommunicating netcrypts
CSCtr62650	WUI using query that is pulling input and output port for sessions on a TSID
CSCtr64901	hctmprovision claims no IPs are available
CSCtr70127	Doctor reports default SI_INSERT_RATE is 1000 when not defined
CSCtr70247	QPSK and CMTS SRM port turns to 0 after 5.0 upgrade
CSCts65089	DSM NetAddrPgetBinaryString multiple cores
CSCts99186	pkeManager does not deliver MSK to NOBE
CSCtt19565	Cannot modify existing segments
CSCtt29559	DSM NetAddrPgetBinaryString multiple cores
CSCtt29689	pkeManager does not deliver MSK to NOBE
CSCtt32672	siManager produces DCM table with 0 data length
CSCtu05631	DSM core recovering CF sessions associated to a non-existent VASP
CSCtu16541	camPsm incorrectly rejects definePkg provisioning for nested pkgs
CSCtu18328	PPV files not being updated in DNCS 5.0.0.22 due to PPVLock issue
CSCtu18350	Unable to create ppv events
CSCtu18356	appserver logs not being saved after +ZIP

CSCtu21908	_pkgui allows recursive provisioning of package members
CSCzk37807	effective_year field missing value in dst_rules table
CSCzk37989	VOD encryption fails when GQAM connected to MPEG source
CSCzk38893	SAM and IPG are in Waiting state in DHCTs after Save the Global dhct config
CSCzk38969	dbUIServer got coring whenever open OS WUI.
CSCzk39006	GbE input port IP data not deleting from database when delete a GQAM
CSCzk39122	Report Writer ->; TSID List report will not work
CSCzk39147	Package name with special characters are displayed wrongly in Batch Authoriz WUI
CSCzk39148	Hubs should not be deleted when QPSK is associated to it
CSCzk43161	qamManager needs to quarantine QAMs when it times out on messages
CSCzk43171	Incorrect Boss Transaction from web UI.
CSCzk43181	EAS - 1 part channel number is not populated correctly by MMMServer in SCTE-18
CSCzk43182	Disabled QAM ports should not be added to the C2 Table in the CDT section
CSCzk43187	DTACS: Make the CDS indexes to match with EIA channel line up.
CSCzk43195	siManager removes c3 packet when there is test hub with no session streamd to it
CSCzk43204	drm has issues with sessions on table-based qams
CSCzk43390	The WUI incorrectly rejects the TSR setup with GigE as input
CSCzk43398	QpskManager not sending SI data, database connection error
CSCzk43932	perfUIServer is getting cored when drmperfmon.csv file has service group data
CSCzk44099	drm not setting multicast indicator correctly for SMDGs
CSCzk44705	pkeManager incorrectly rejects ECM for session it owns
CSCzk47035	DRM will not recover SMDG
CSCzk55154	improve qamManager performance for CVT insertion
CSCzk55877	EARS does not correctly convert GMT time received from EAC.
CSCzk58686	qamManager can fail to process errors from rapid responses
CSCzk58687	qamManager needs to throttle session and packet audits for SA QAMs
CSCzk58689	qamManager does not quarantine QAM correctly on RPC failure
CSCzk58693	Insta-staging zeroized bit maps are not sent when STB goes OOS

Open System CRs

The following report contains a list of open System CRs that were identified during testing of the SR 5.0. Resolutions to these issues are currently under investigation or in development.

CR ID	Title/Impact
CSCtq57606	Segment WUI allows sequential white spaces within segment name
CSCtr29030	cmd2000 fails to connect to MCard via MAC Address from the command line
CSCtx57867	qamManager cores when SRM on RFGW-1 is set to 'Legacy Mode' **Workaround:** Unselect the SRM "Legacy Mode" option, under System Configuration in the RFGW-1 WebUI.
CSCzk45517	DNCS TSR list WUI does not show 'Source IP Address 1'
CSCzk45892	DNCS GQAM WUI should provide Dual GIGE settings reported by GQAM.
CSCzk46599	MPEG Source name with comma/semicolon causes errors in Source Definition WUI
CSCzk60433	Hidden Channel number upper limit needs to be bound in Update Source WUI
CSCzk60934	Segment with wild cards does not display properly in Package Provisioning WUI
CSCzk64477	Hidden channels assign in sourceui should not be accessible in channel map **Workaround:** To prevent the conflict between real A/V channel numbers and hidden channel numbers, assign hidden channel numbers outside of the range that carries A/V contents. For most DNCS systems, you will assign hidden channel numbers in the range above 1900.
CSCzk64479	DSM doesn't handle reuse of xactionIds in DSMCC msgs properly

4

Customer Information

If You Have Questions

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.

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

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

March 2012 Printed in United States of America Part Number 4035750 Rev A