System Release 2.7

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 Acknowledgements

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.

CableCARD and OpenCable are trademarks 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 2.7 (SR 2.7) is a minor release built on System Release 2.5 (SR 2.5). These release notes contain the following information:

- Descriptions of the new standard and optional features introduced with this system release
- Descriptions of the optional features carried forward into SR 2.7 from previous system releases
- Information you need to prepare your site for an upgrade to SR 2.7
- Change requests (CRs) that were found in previous system releases and corrected in SR 2.7
- A summary of open issues for the standard and optional features of SR 2.7
- General information for contacting Cisco
- A list of software versions installed with the base SR 2.7 system

Scope

These release notes provide an executive overview of SR 2.7. 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 call Cisco Services.

Audience

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

Software Product Offering

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

- Application Platform Releases (Client Releases) offer a bundled software package that includes both the SARA and PowerTV OS. Application Platform Releases are compatible with multiple system releases.
  - Application Maintenance Releases address a group of specific change requests that are required before the next application 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.

Application Software provides cable service providers with unique services and increased functionality that enhance the subscriber experience.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document. Check the copyright date on your resources to assure that you have the most current version. The publish dates for the following documents are valid as of this printing. However, some of these documents may have since been revised:

- *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455, published October 2006)
- *Daylight Saving Time Configuration Guide* (part number 749233, published December 2006)
- *DBDS Backup and Restore Procedures For System Releases 2.2 through 4.2* (part number 4013779, published December 2006)
- *DBDS Utilities Version 6.1 Configuration Guide* (part number 4000828, expected publish date: early 2007)
- *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User's Guide* (part number 740020, expected publish date: early 2007)
- *DNCS On-line Help (UNIX) 4.2.0.3* (part number 4012122, published December 2006)*
- *DNCS Report Writer Version 4.2 User's Guide* (part number 4013430, published December 2006)
- *Enabling Content Protection for Broadcast Programming* (part number 4005893, published September 2005)
- *Enhanced Channel Maps User's Guide* (part number 4011413, published December 2006)
- *GoQAM Software Version 1.1.2 Release Notes and Installation Instructions* (part number 4002628, published December 2006)
- *GQAM Software Version 4.0.6 Release Notes and Installation Instructions* (part number 4011046, published December 2006)
- *Maintenance Recommendations for the DBDS System Guide* (part number 4002341, published March 2003) [expected revision date: mid-year 2007]
- *MQAM 2.6.10 Release Notes and Installation Instructions* (part number 745250, published December 2006)
- *Netcrypt™ Bulk Encryptor Hardware Installation and Operation Guide* (part number 4001444, published December 2006)
- *Netcrypt™ Bulk Encryptor Software Version 1.1.3 Release Notes and Installation Instructions* (part number 4009746, published December 2006)

- *Program and System Information Protocol Configuration for System Releases 2.5, 3.5, and 4.0* (part number 4011319, published September 2005)
- *Provisioning the DNCS to Support SDV Services User Guide* (part number 4012948, published January 2007)
- *QAM Modulator Software Version 2.5.1 Release Notes and Installation Instructions* (part number 740242, published December 2006)
- *QPSK (Release E14) Release Notes and Installation Instructions* (part number 4013491, published December 2006)
- *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377, published June 2005)
- *SARA Application Server 3.4.1 Release Notes and Installation Instructions* (part number 4012158, published December 2006)
- *SARA Application Server 3.4.1 User's Guide* (part number 4012159, published December 2006)
- *SDV Operator's Guide For System Releases 2.7/3.7 or SR 4.2* (part number 4000308, published December 2006)
- *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584, published May 2006)
- *Setting Up PowerKEY® CableCARD™ and M-Card™ Modules on the DNCS for System Releases 2.7/3.7 and 4.2* (part number 4014667, published December 2006)
- *Switched Digital Video Architecture Guide* (part number 4012490, published December 2006)

The SR 2.7 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:

- *DNCS On-line Help (PC) 4.2.0.3* (part number 4012121, published December 2006)

Document Version

This is the second release of this guide.

1

Why Choose System Release 2.7?

Introduction

SR 2.7 includes many features and enhancements implemented at the request of our customers. Review this chapter to learn more about these exciting changes.

Important! This chapter describes the features and enhancements for the standard version of this software release. This chapter also describes certain features and enhancements that are carried forward from previous system releases along with several optional features that are also carried forward. In addition, this chapter introduces Switched Digital Video (SDV), a new optional feature available with SR 2.7.

Note: If you want information on the new optional feature available for this software release, see ***SDV: The New Optional Feature in SR 2.7*** (on page 31).

In This Chapter

SR 2.7 at a Glance

Overview

This section provides an "at-a-glance" look at the new features and enhancements for SR 2.7. Each new feature and enhancement is described in detail later in this chapter. In addition, this chapter also describes certain features and enhancements that are carried forward from previous system releases.

What Are the New Features in SR 2.7?

Switched Digital Video (Optional)

See ***SDV: The New Optional Feature in SR 2.7*** (on page 31) for details on the optional Switched Digital Video (SDV) feature.

DNCS GUI Enhancements

The DNCS Element Provisioning tab has now been split into the following tabs:

- Network Element Provisioning
- Home Element Provisioning

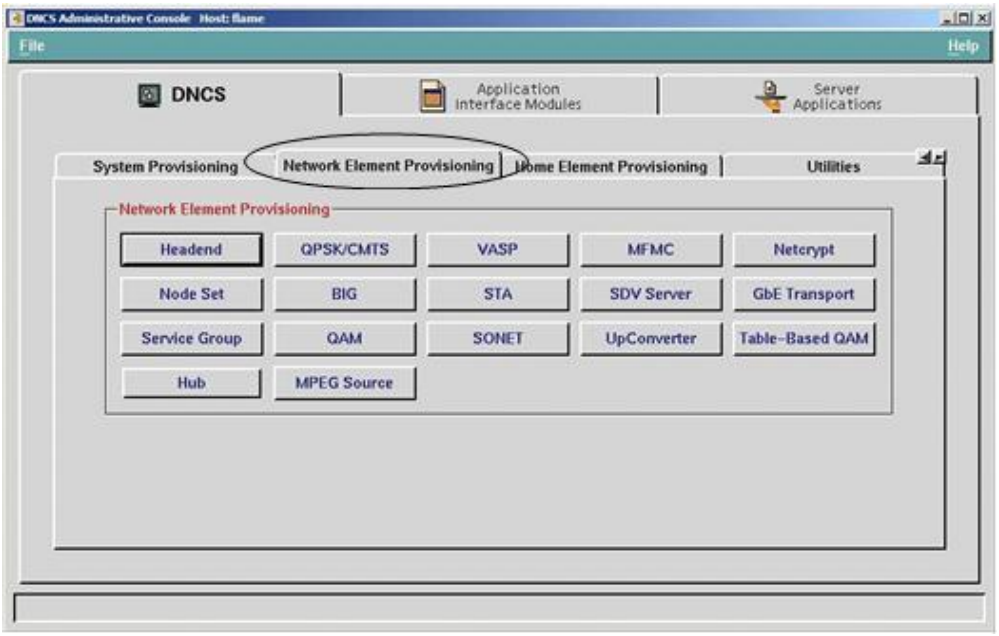
The **Network Element Provisioning** tab provides access to the provisioning and configuring GUIs for all network hardware and software elements (devices).

The **Home Element Provisioning** tab provides access to the provisioning and configuring GUIs for all hardware and software elements that provide services to subscribers' homes. Buttons on the Home Element Provisioning tab are grouped into the areas of **DHCT Provisioning** and **CableCARD Provisioning**.

The following illustrations provide examples of the new DNCS Administrative Console Element Provisioning tabs.

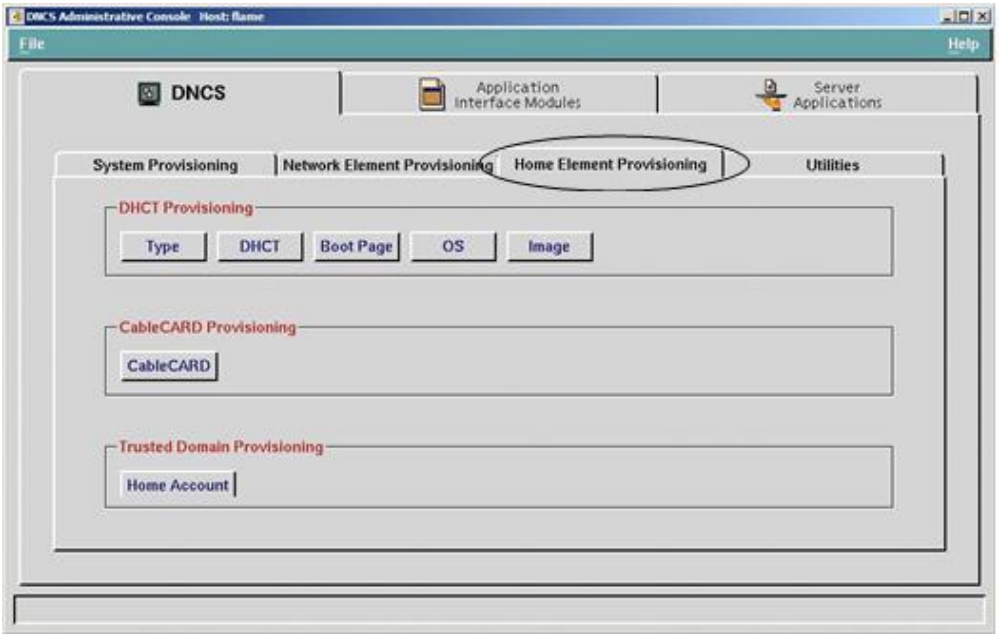
Network Element Provisioning Example

Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab



Home Element Provisioning Example

Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab



Staging Bridges Support

The current staging method involves sending all EMMs to every bridge on the DNCS network when operators stage DHCTs with the reverse plant disabled (one-way staging). The primary purpose of Staging Bridges support is to provide the capability for operators to identify a specific bridge (hub) on which staging is to be performed. Then, staging communications are delivered to the specific bridge used for staging. Staging Bridges Support eliminates the need to broadcast staging communications (EMM distribution) throughout the entire network, and it reduces the processing load on the DNCS when staging is performed.

Note: For detailed information about Staging Bridges Support, see ***Staging Bridges: Reduce Network Message Traffic and Improve DHCT Staging Efficiency*** (on page 13).

Support for the Netcrypt Bulk Encryptor

The Netcrypt Bulk Encryptor optional feature is a powerful encryption engine designed for use in Gigabit Ethernet (GbE) transport networks. The Netcrypt Bulk Encryptor encrypts digital broadcast and narrowcast transport streams across multiple headends and can use up to three distinct conditional access systems (CASs).

Note: *Broadcast* refers to one signal going to many sites; *narrowcast* refers to one signal going to a select group of sites.

The Netcrypt Bulk Encryptor has a maximum throughput of 4 Gbps. It is capable of encrypting as many as 4000 input programs into individual transport streams suitable for digital broadcast or multicast sessions. The Netcrypt Bulk Encryptor also provides the technology to multicast both the input and the output streams.

The Netcrypt Bulk Encryptor enables you to maximize your bandwidth usage and provides countless programming options that will enhance your service to your customers as well as increase your revenue potential.

Note: If you would like to purchase or activate this separate software product for your system, contact your Cisco marketing representative.

For More Information

Refer to the following publications for additional information about the Netcrypt Bulk Encryptor:

- *Netcrypt™ Bulk Encryptor Hardware Installation and Operation Guide*
- *Netcrypt™ Bulk Encryptor Software Version 1.1.3 Release Notes and Installation Instructions*

Performance Monitoring GUI on the DNCS

SR 2.7 introduces a Performance Monitoring (perfmon) GUI for the display of performance data collected from DNCS processes. A **Performance Monitoring** button has been added to the Utilities tab. This button provides easy access for system operators to a new tool that uses a graphical format to display data collected from DNCS processes. This performance monitoring feature also includes data about DHCT and VOD performance.

Note: For detailed information about the new Performance Monitoring GUI, see ***Performance Monitoring GUI: Easier Access to Performance Monitoring Data*** (on page 15).

Solaris 10 Support

Solaris 10, the new operating system from Sun Microsystems, provides a number of innovative and improved facilities over earlier versions. Solaris 10 includes new facilities such as Dynamic Tracing (DTrace), Solaris Containers, Predictive Self-Healing, and improved networking (new TCP/IP stack).

Note: For detailed information about Solaris 10 support, see ***Solaris 10 Support: Increase Your Processing Capability*** (on page 14).

Support for Enhanced Channel Maps on the DNCS

Cisco customers have requested greater flexibility in assigning channel maps. In earlier system releases, service providers could only assign channel maps to a set-top based on the hub where the set-top was deployed. At that time, all of the set-tops deployed in any hub shared the same channel map.

A **Group Definitions** button has been added to the Applications Interface Modules tab, and a lineup group ID (**LUG ID**) field has been added to the Set Up Display Channel Map window. These tools give you great flexibility in assigning channel maps by allowing you to create channel maps that are not associated with hubs.

For example, you can now add a channel that is visible to all high-definition (HD) set-tops, but does not appear on standard-definition (SD) set-tops.

Enhanced Channel Maps requires the following DHCT software:

- DVR 1.3.1a17, or later
- HD 1.5, or later
- SARA 1.58, or later

Enhanced Channel Map Features

The following list includes a few examples of channel map flexibility requested by customers:

- Create a channel to be used only by a small group of DHCTs in a hub for an application trial
- Create channels that can be tuned by subscribers of premium services, but are not visible to subscribers of basic services
- Add a channel that is visible to all high-definition DHCTs but does not appear on standard-definition DHCTs
- Define a "family friendly" channel lineup that omits adult channels, and assign that channel to subscribers who request it

For More Information

For more information on Enhanced Channel Maps, refer to the *Enhanced Channel Maps User's Guide*.

Support for Configurable Daylight Saving Time

To comply with the Energy Policy Act of 2005, SR 2.7 provides a new user interface that allows system operators to input, view, change, or delete Daylight Saving Time (DST) rules. The DNCS database schema and libraries will also be modified to allow the system to store and update DST rules. This modification allows for the dynamic configuration of set-tops at the hub level to conform to local DST rules.

A new **DST** button has been added to the System Provisioning tab. Clicking the **DST** button displays the Set Daylight Savings Time Rules window. From this window, you can configure your system so that set-tops automatically adjust for daylight saving time as it is observed in the different regions your DBDS serves. Daylight Saving Time rules are applied on a hub basis: after you create rules for different daylight saving time zones, you can assign a rule to one or more hubs. Set-tops then use the rule of the hub to which they belong.

Note: For detailed information about support for configurable Daylight Saving Time in SR 2.7, see ***Configurable Daylight Saving Time: Manage Time Changes*** (on page 20).

Support for Dual Gigabit Ethernet QAM Modulator

SR 2.7 provides support for the new Dual Gigabit Ethernet [GbE] QAM Modulator (GQAM). SR 2.7 also includes support for Dual GbE port dejitter with automatic redundant switching between ports.

Note: The GQAM may use the second GbE port, instead of the first port, for source data.

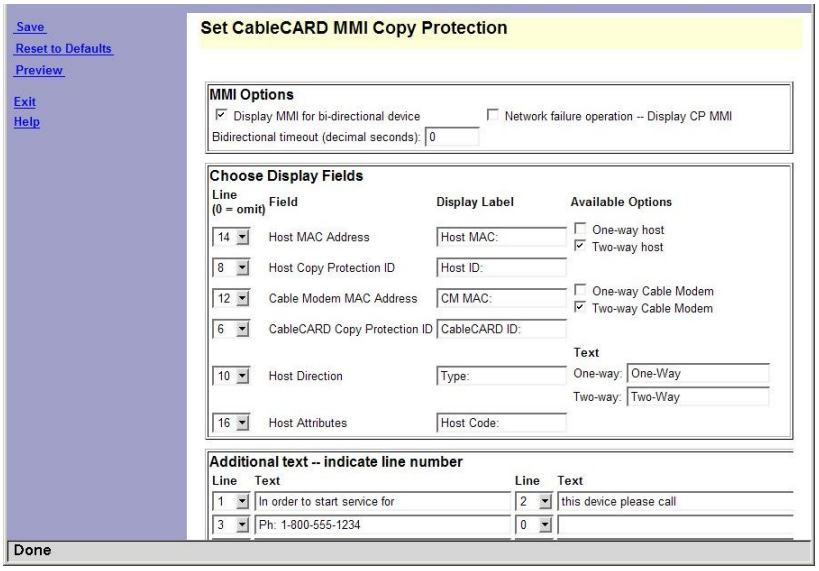
CableCARD MMI Copy Protection Screen

At the request of customers, Cisco has changed the Man Machine Interface (MMI) copy protection screen to provide additional information to be used for setting the service level of an OpenCable host in the billing system. The display of the copy protection MMI screen is independent of whether the host is one-way (unidirectional) or two-way (bidirectional). SR 2.7 provides support for this new feature.

The MMI Copy Protection screen is configurable from the following new GUI on the DNCS:

Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Configure CableCARD Server > MMI Screen Format

The following illustration shows an example of the Set CableCARD MMI Copy Protection screen.



Support for New Organizationally Unique Identifiers (OUIs)

SR 2.7 contains support for new Organizationally Unique Identifiers (OUIs). Currently the system supports the OUI values of **00:02:DE, 00:0A:73, 00:0F:21**, and **00:11:E6**. If you receive PowerKEY CableCARD modules that use a new OUI, you must contact Cisco Services to have a technical support engineer update your DNCS database.

Support for Persistent QPSK Database Reduces DHCT Sign-On Time

The QPSK software maintains a database that contains various parameters for each of the up to 16K DHCTs that can be signed on to a single QPSK modulator (QPSK) at any one time. These parameters include such things as IP Address, MAC Address, Signon State, Power Level, and various counters that are used to track each DHCT. When a QPSK reboot occurs, the current software clears this database and requires the DHCTs to sign on again. Although the reboot itself takes approximately 30 seconds, the process of signing on up to 16K DHCTs to a single QPSK can take an appreciable period of time.

SR 2.7 provides support for a new persistent DHCT database module in the D9482 QPSK Modulator software subsystem. This enhancement saves relevant DHCT data in RAM and restores it after a QPSK reboots, thereby decreasing the amount of time necessary to recover from a QPSK reboot.

Therefore, instead of requiring the DHCTs to sign on again, certain relevant data for each DHCT such as IP Address, MAC Address, Channel number, etc., are stored in space that is persistent across "short" reboots. Thus, during short reboots, the QPSK uses this data to refurbish the DHCT database. This data in the DHCT database provides an efficient method to shorten the previously lengthy sign-on process.

The following DNCS GUI changes support this new feature:

- A **Database Persistence** selection on the Set Up QPSK Modulator screen
- A **Reset and Clear DB** selection on the QPSK/CMTS File menu

What Standard Features Are Carried Forward in SR 2.7?

Support for Two-Way CableCARD Binding/Autobinding

SR 2.7 provides support for two-way Multi-Stream CableCARD module autobinding. Binding between the host and the CableCARD module is needed to provision a cable host. Binding involves matching both host and CableCARD module MAC addresses at the DNCS to associate the CableCARD module with the host. With two-way hosts, binding can be accomplished manually, or it can be done automatically (autobinding). Autobinding allows the automatic exchange of host- and CableCARD-specific information (for example, MAC addresses) with the DNCS for binding. With autobinding, two-way hosts automatically authorize CableCARD modules, and subscribers do not need to telephone for authorization.

Dynamic Logging

SR 4.0 first introduced a new Logging utility to make it easier than ever to capture key troubleshooting information.

The new Logging utility allows an operator to manipulate those logs that Cisco historically considered "Developer-Only" debug logging. Specifically, these are the EMCDEBUG logs that reside in the /dvs/dncs/tmp directory that, in the past, required process restarts for activation. These process restarts were quite inconvenient and could, at times, result in disruption of some services. These disruptions occurred usually at the least opportune time, for example, when an issue required troubleshooting.

In order to streamline this problem-solving process and to remove any adverse impact on functionality, Cisco developed the new logging utility. This new utility allows you to fine-tune log levels for DNCS processes and their associated libraries in much the same manner as the legacy DNCS Tracing utility (which is unaffected by this new tool).

As a reminder, the legacy DNCS Tracing Utility allows dynamic activation, provides fine-grained control over DNCS processes and their respective libraries, and saves its output into the /var/log/dncsLog file. This logfile continues to contain information that DNCS software developers considered appropriate to assist customers in their day-to-day operation of the DNCS Application. Additionally, this content included information about all DNCS processes.

In contrast, the SR 4.0 Logging Utility was focused on the more detailed debug logging. The following list includes some of the highlights of this feature:

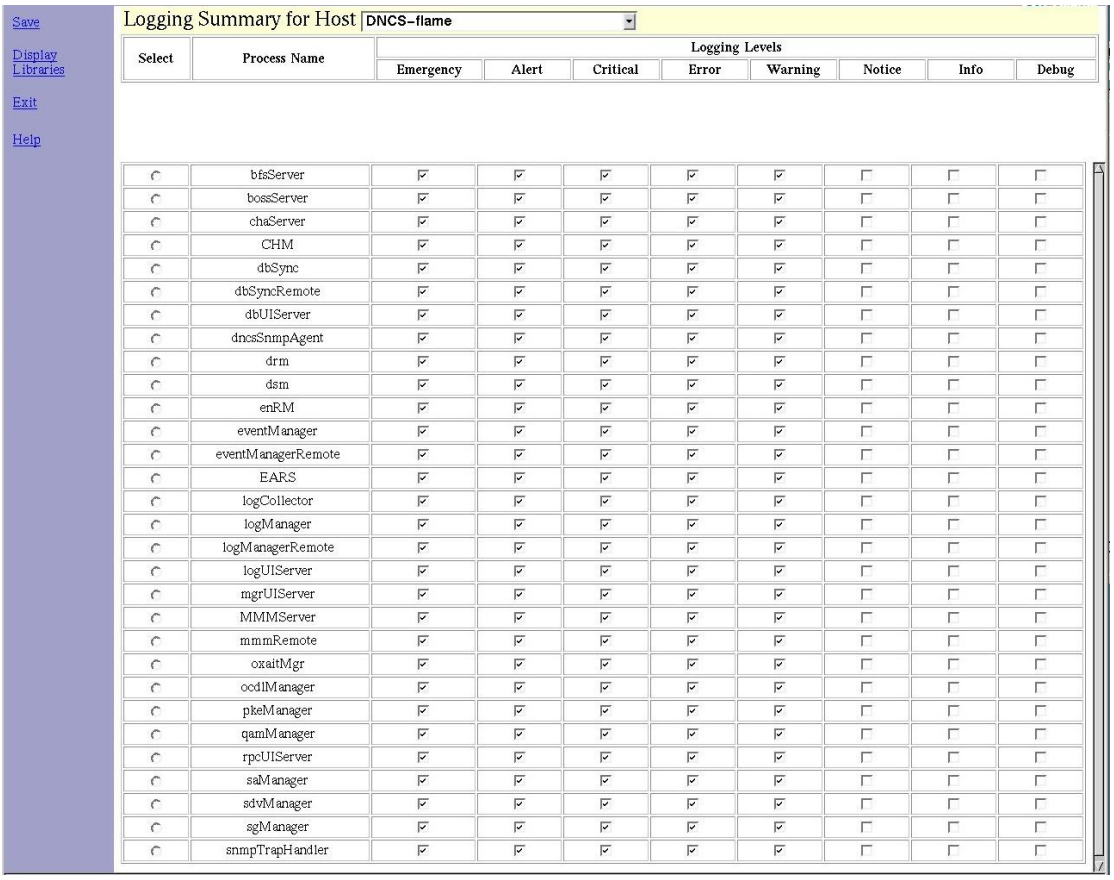
- Dynamic Activation
- Integrated DNCS User Interface using a Web browser user interface
- Seven levels of logging detail, all while retaining the operation of the detail output, which are deposited into a per-process set of Generation Log Files that use the naming convention /dvs/dncs/tmp/[name of process.*]

Important! If you are using Cisco's RCS solution, you can use this utility to capture DEBUG logging information about the processes and libraries for each site in your system.

Another key benefit of the logging utility is that logging level changes are now allowed without the need to restart processes.

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

The following illustration shows an example of the Dynamic Logging summary screen.



GQAM IP Multicast Input

SR 2.7, in conjunction with GQAM modulators loaded with GQAM software version 3.x (or later), provides support for GQAM IP multicast input. This feature allows system operators to use GQAM modulators to join an IP multicast service or source to obtain and broadcast content to digital set-tops in different formats (simulcast). Basically, this feature allows different GQAMs to use the same IP content source.

What Optional Features Are Carried Forward in SR 2.7?

EAS Filtering

As a leading provider of cable services to your community, you want to ensure that your subscribers accurately receive emergency messages intended for their community. Emergency Alert System (EAS) filtering is an optional feature that, through its integration with the DNCS, uses the Federal Information Processing Standards (FIPS) to filter and send EAS messages only to targeted states, counties, or subdivisions. This feature enables you to serve your customers and your community in a timely and efficient manner.

Note: If you would like to purchase or activate this separate software product for your system, contact your Cisco marketing representative.

Session-Based Encryption Security

Video-on-demand (VOD) is an interactive application that provides video services to subscribers upon request. SR 2.7 carries forward support for the Session-Based Encryption (SBE) security option. SBE provides an added degree of security for VOD content and prevents QAM tuner-equipped televisions from viewing unpurchased VOD content. SBE also presents an opportunity for you to increase your revenue potential by increasing the numbers of opportunities for VOD purchases.

Note: If you would like to purchase or activate this separate software product for your system, contact your Cisco marketing representative.

Regional Control System: A New Solution for Geographic Challenges

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

Each RNCS offloads tasks that 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. RCS provides an opportunity for you to save and consolidate your resources by not requiring technical personnel to be present at remote sites.

Note: If you would like to purchase or activate this separate software product for your system, contact your Cisco marketing representative.

Overlay: Deploy Cisco Set-Tops in Other Networks

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

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

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

Overlay technology allows you to maximize your network and your resources by enabling you to use a variety of equipment to provide programming and services to your customers without having to pay for expensive rebuilds of your network.

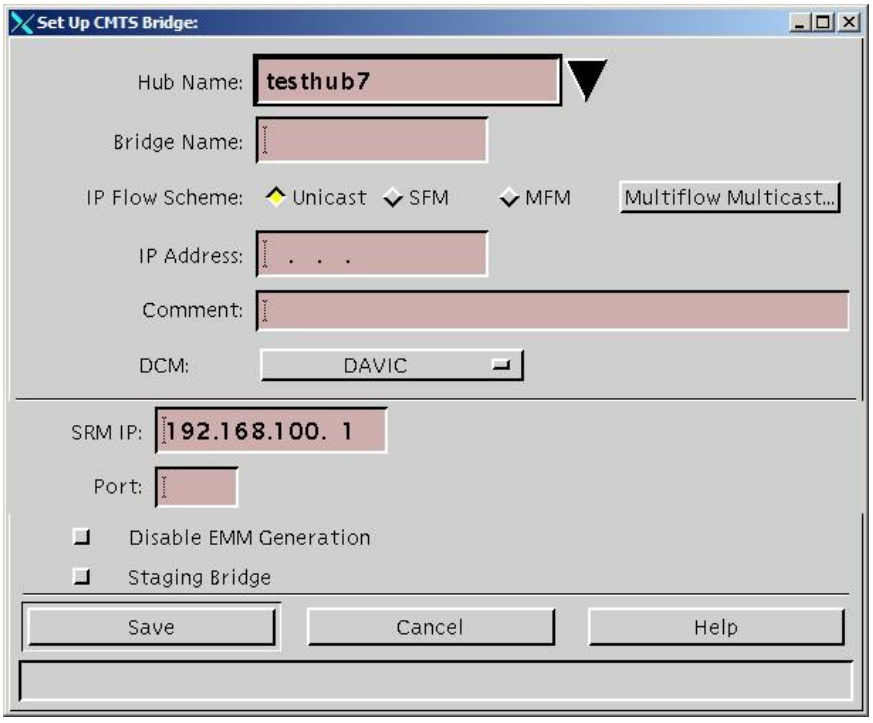
Note: If you would like to purchase or activate this separate software product for your system, contact your Cisco marketing representative.

Staging Bridges: Reduce Network Message Traffic and Improve DHCT Staging Efficiency

The current method for staging new DHCTs involves sending all EMMS for each given DHCT to every out-of-band (OOB) bridge, and, ultimately, to every DHCT resident in a given DBDS. This method is known as "broadcast" or "one-way" staging and requires system operators to disable the "reverse" communication path. Another aspect of this staging technique lies in the fact that even though a given set of EMM authorizations apply only to a specific single DHCT, the data is propagated throughout the cable system. This is a very inefficient model that wastes both DNCS and network resources.

The primary purpose of the Staging Bridges feature is to address this network inefficiency and to provide an alternative staging paradigm that results in an improved use of DNCS and network resources while also streamlining the staging process. With the Staging Bridges feature, system operators identify a subset of the OOB bridge population within a DBDS to use for the staging function. Once this subset is identified, system operators can use the DNCS GUI subsystem to isolate and route staging communications traffic (for example, EMMs) only to this specified subset of OOB bridges. When configured and administered properly, the Staging Bridges feature can greatly reduce unnecessary network message traffic while reducing DNCS platform processing usage.

Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > New > CMTS > Set Up CMTS Bridge



Solaris 10 Support: Increase Your Processing Capability

SR 2.7 includes support for Solaris 10, the new operating system from Sun Microsystems. Solaris 10 provides a number of innovative and improved facilities over earlier versions. Among these innovative and improved facilities are Dynamic Tracing (DTrace), Solaris Containers, Predictive Self-Healing, improved networking (new TCP/IP stack), and many others.

Dynamic Tracing (DTrace) facility can be used by administrators and developers to explore the internal operation of the system, track down performance problems, or locate the cause of aberrant behavior. It is safe to use on production machines and does not require restarting either the system or applications.

Solaris Containers is a server virtualization and software partitioning methodology that can isolate applications and services using flexible, software-defined boundaries. Solaris Containers enables you to create many private execution environments within a single instance of the Solaris operating system.

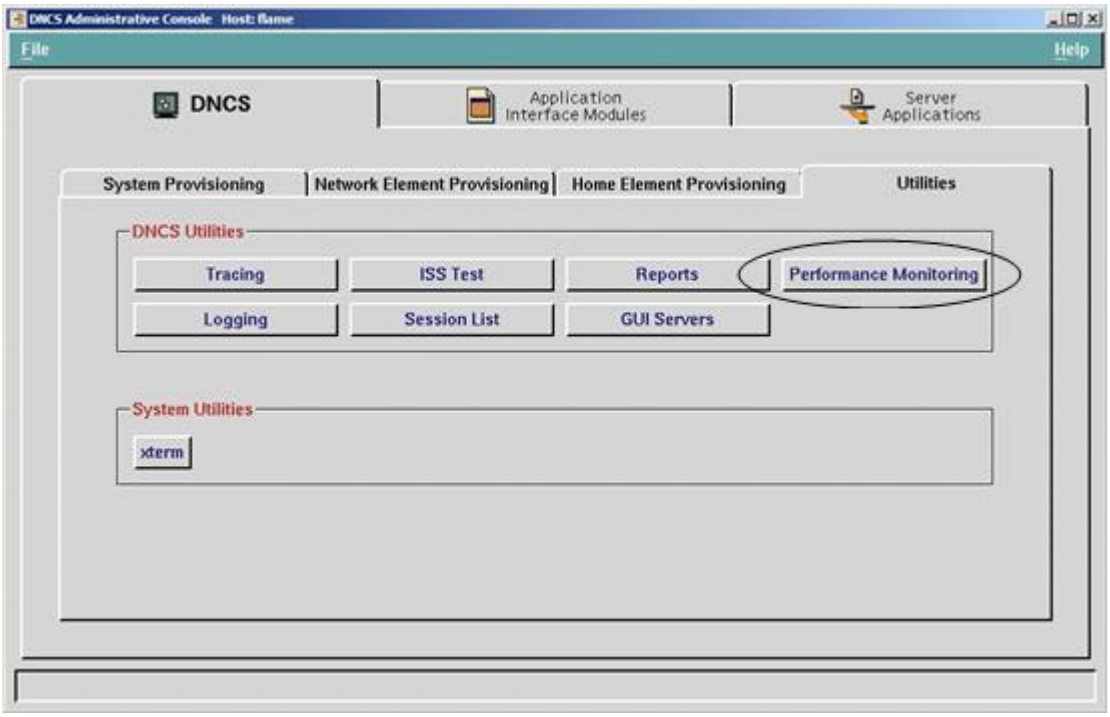
Predictive Self-Healing is an innovative feature that monitors, diagnoses, isolates, and recovers from hardware faults and software errors. It works along with Service Management Facility (SMF), a feature that replaces the traditional UNIX run-level (rc) scripts and enhances the monitoring, starting, stopping, and restarting of both operating system and application daemons.

Solaris 10 Operating System also contains a new and scalable TCP/IP stack that increases network throughput and capacity. The TCP/IP stack has been tuned for 10 Gigabit Ethernet, wireless networking, and hardware offloading technologies.

Performance Monitoring GUI: Easier Access to Performance Monitoring Data

This feature provides a new Performance Monitoring (perfmon) GUI for the display of performance data collected from DNCS processes. This feature provides a front-end GUI to display the data collected from these processes.

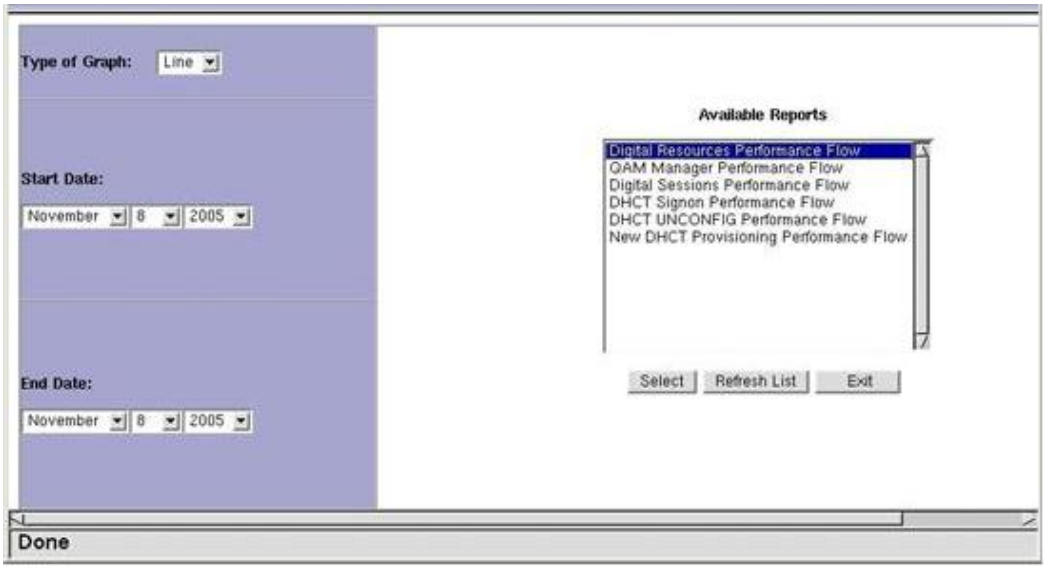
Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Performance Monitoring



Digital Network Performance Monitoring GUI Example

Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Performance Monitoring > Digital Network Performance Monitoring GUI

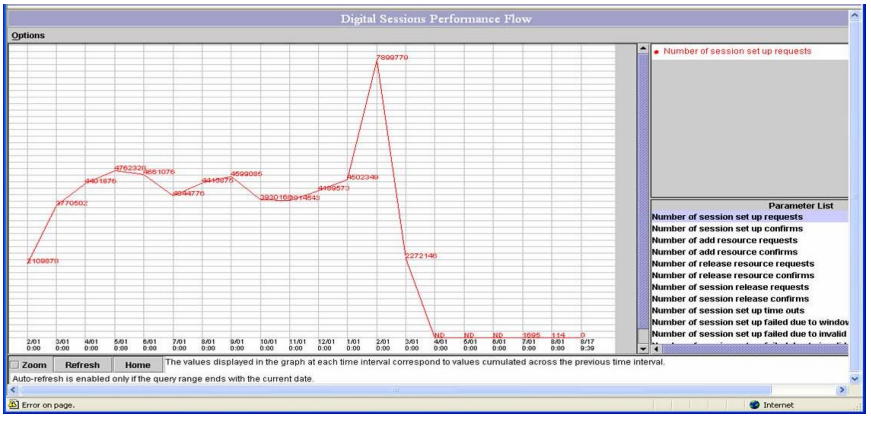
The Digital Network Performance Monitoring features allows you to collect and display system performance data. The following illustration is an example of the new Digital Network Performance Monitoring GUI on the DNCS.



Viewing a Report

Follow these steps to view a report.

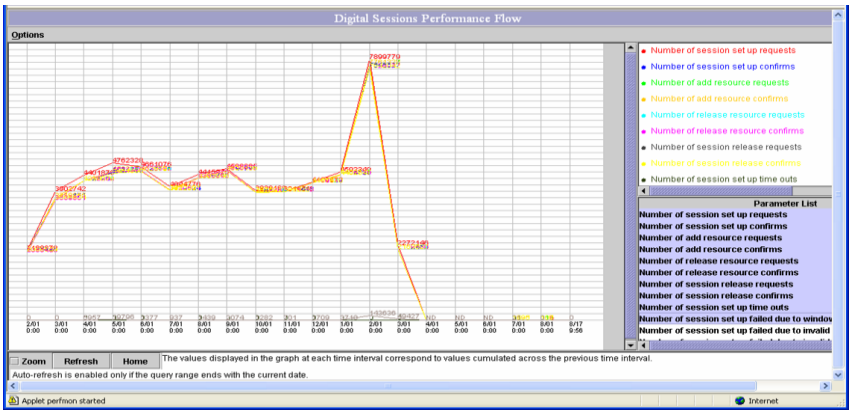
1. Click the **Type of Graph** arrow and select **Line** from the list.
2. Click the **Start Date** and **End Date** arrows and select the start date and end date for the report data from the respective lists.
3. Select one of the **Available Reports** from the list.
4. Click **Select.** A graph similar to the following appears.



Performance Monitoring Features

The following list shows some of the Performance Monitoring features you can use after you create and display a report:

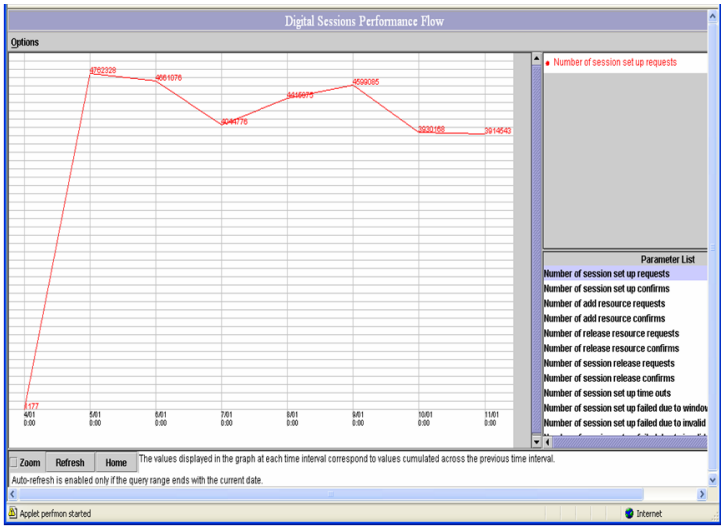
- You can select the various parameters displayed in the parameter list.



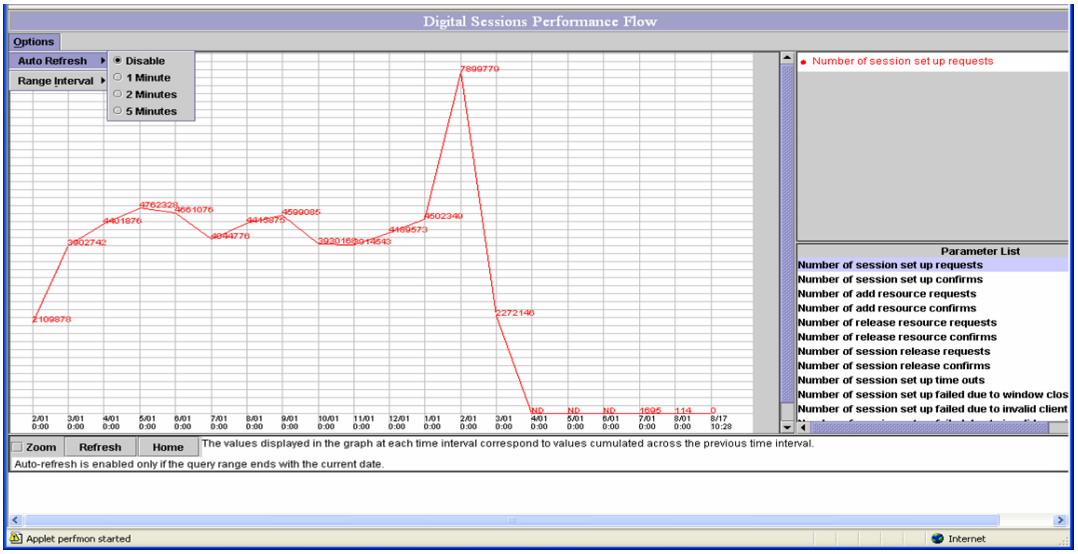
Notes:

- Each selected parameter is displayed in a line graphic.
- Each selected parameter is displayed in the color shown in the parameter list control.
- More than one parameter can be selected in the parameter list.
- All selected parameters are drawn on the graph in different colors.

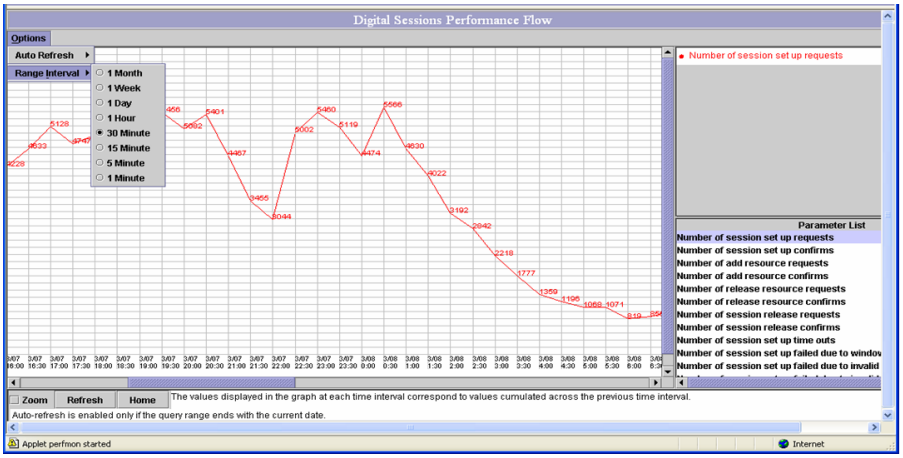
- You can **Zoom** to certain areas of the report.



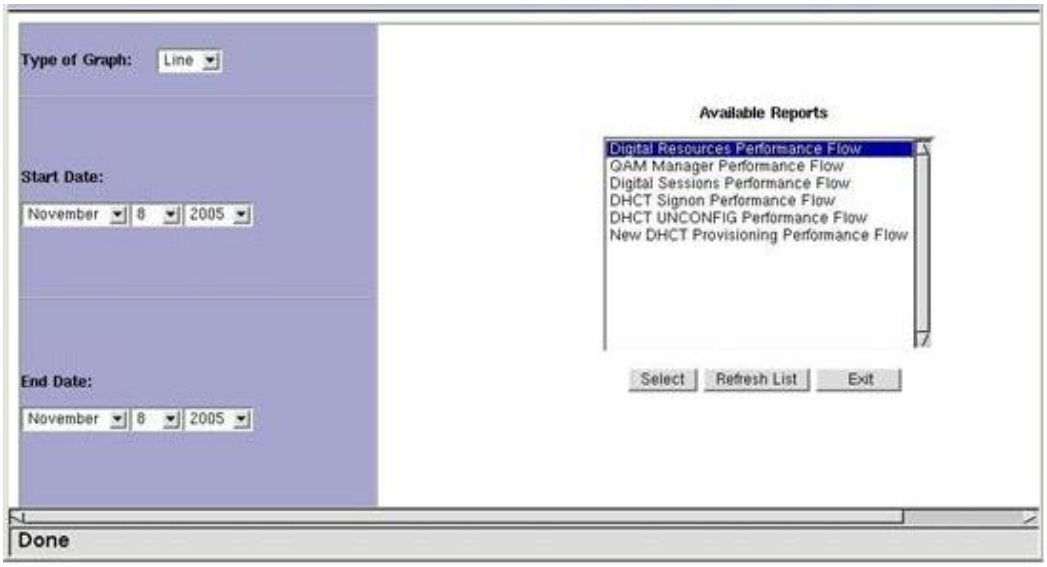
- You can **Refresh** the report.



- You can select various **Range Intervals** for which to display data.



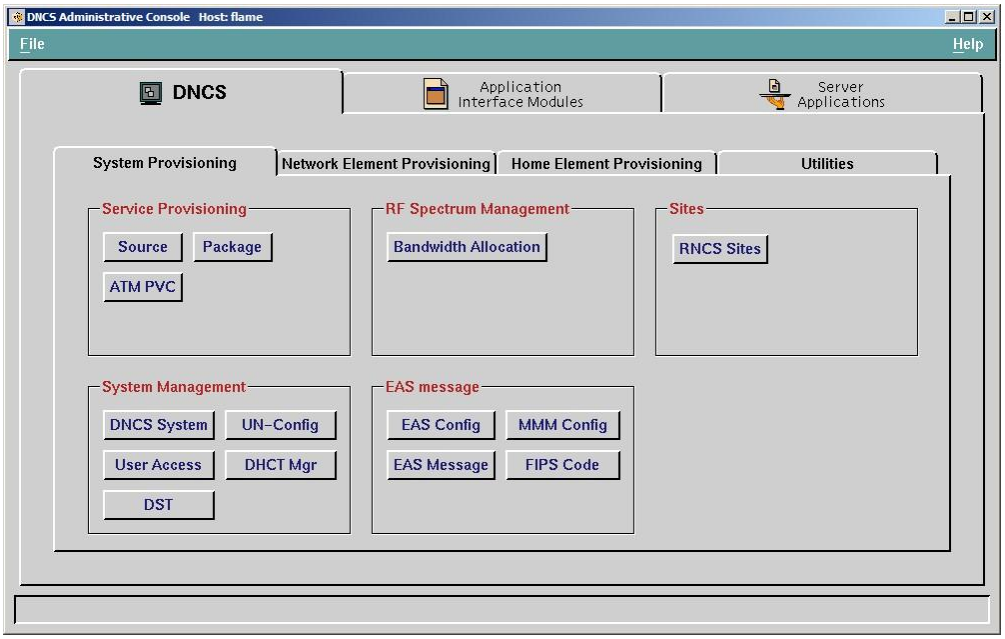
- You can click **Home** to return to the initial screen.



Configurable Daylight Saving Time: Manage Time Changes

Overview

A new **DST** button has been added to the System Management area of the System Provisioning tab on the DNCS Administrative Console. Clicking the **DST** button displays the Set Daylight Savings Time Rules window. From this window, you can configure your system so that DHCTs automatically adjust for daylight saving time as it is observed in the different regions your DBDS serves. If you have a distributed system, where the DNCS is in one time zone and remote sites are in other time zones, daylight saving time is applied on a hub basis, according to the DST Zone ID setting assigned to the hub.



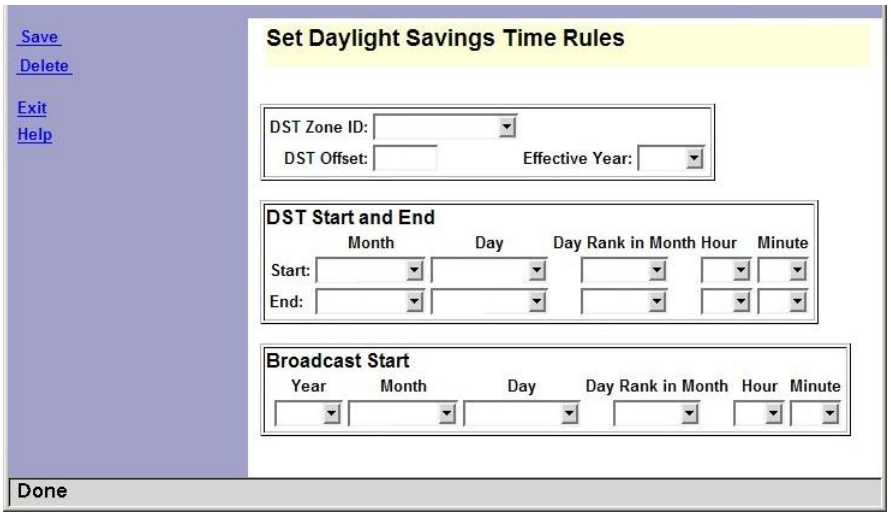
Configurable Daylight Saving Time

Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST > DNCS DST Rule Definitions GUI

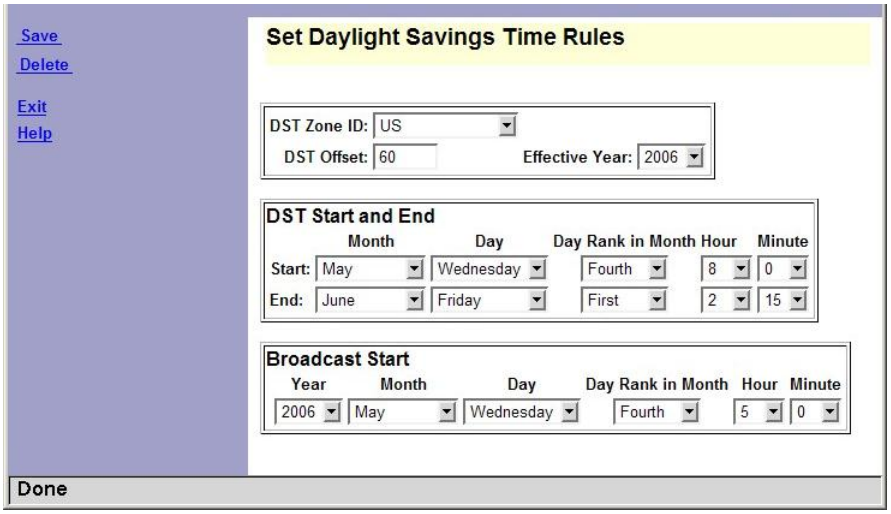
From the Set Daylight Savings Time Rules window, you can create, modify, and delete daylight saving time (DST) rules that can be used by DHCTs in different time zones. Setting up the right DST rules enables the DHCTs in your system to automatically adjust to changes in DST observance.

DST rules are typically created for your system during a system upgrade or installation. However, as your system changes, you can use this window to change or delete existing rules and create new ones.

The following illustration shows an example of the new DST user interface with no DST Rule data defined.



The following illustration shows the DST Rule Definition user interface with sample DST rule data.



What's Fixed?

This section provides a description of the CRs implemented in SR 2.7.

CR 28097

The sgManager process no longer goes in and out of recovery when saving or resetting a service group.

CR 51927

Report Writer now displays correct information for sessions configured on the GQAM Ethernet inputs.

CR 52045

Improved camPsm ECM delivery performance when delivering ECMs to the Netcrypt device.

CR 52176

Reordered the table-based QAM data table to match the potential input file. This change makes using the File Load capability for table-based QAMs more intuitive.

CR 53350

Modifications made to a SAM Service that affect a CableCARD channel map are now automatically updated in the CableCARD channel map file.

CR 53486

A memory leak in the ResAppServer process has been fixed and no longer requires a restart to reclaim the lost memory.

CR 53846

Invalid QAM key certificates no longer cause the camEx process to core dump when setting up sessions.

CR 54125

A security vulnerability issue in the Xsun and Xprt commands has been fixed.

CR 55039

While the IPG is publishing new data, the rate of out-of-band broadcast packets fluctuates above the normal BFS carousel rate. After the new data is published, the BFS carousel rate returns to normal.

CR 55435

The Spectrum .vnmrc file list is now included as a keyfile. This eliminates the need to acquire and re-load the Spectrum activation key.

CR 55911

The PassThru server no longer leaves a core dump file when shutting down.

CR 55981

A timing issue has been corrected that occasionally caused the qamManager process to core when it attempted to delete an object that was in the process of being deleted.

CR 56506

The OSM now correctly audits bootloader images so that set-top staging can occur correctly.

CR 57240

UniPack migration scripts now exit when the database restore fails. This prevents DNCS and AppServer conversion failures during the upgrade process.

CR 57419

Improved CVT download groups to handle 10 CVT Download Groups of 10,000 DHCTs in the pdoshct table.

CR 57436

The dncsDbData process no longer reports an error if the database views are out of order.

CR58640

The Solaris operating system has been updated to support DST requirements for calendar year 2007.

CR 59077

Processes on the LIONN no longer must be stopped and restarted (bounced) to re-establish connection to the database during database log maintenance when the sqlexec process is stopped by the resetLionnDbLog script.

Note: This CR applies to Distributed RNCS systems only.

CR 59518

The emmDistributor process is now able to transmit updated Entitlement Management Messages (EMMs) to DHCTs in the field when audit queries take longer than 10 minutes to complete.

CR60383

The Unipack Live Upgrade process no longer repartitions database disks on the Sun E450 DNCS.

CR 60385

A condition that caused ufs_log errors to occur after a system reboot has been corrected.

CR 60796

A condition that caused an occasional crash of the qamManager process when processing QAM configuration data entered through the DNCS user interface has been corrected.

CR 62085

A new /var/spool/cron/crontabs.previous is now created as a part of the keyfiles backup during the Live Upgrade process. The /var/spool/cron/crontabs.previous file is now listed as a key file. After the upgrade completes, the correct crontabs.previous directory is restored.

Known Issues

This section describes the known issues found during the testing of SR 2.7. A resolution to these issues is currently in development at Cisco.

CR 53029

The QAM List GUI allows users to sort the list by IP address only one time.

CR 54387

Users must refresh the BFS Administration GUI in order to delete BFS servers from the list.

Workaround: After you delete a BFS server, choose **View > Refresh Item** to refresh the GUI.

CR 55194

The Performance Monitoring WUI does not allow users to cancel a selected zoom range within the displayed graph.

CR 55432

The Session Data Summary GUI displays a blank screen when navigating with shortcuts.

CR 55826

The Channels, Sources, and Sessions report does not display the Hub Name information correctly for the corresponding lineup group (LUG) IDs.

CR 56524

Navigation between the Session Resources screen and the Resource Details screen in the DNCS Session Filter WUI takes users to the Session Data Summary page instead.

CR 56637

The Session List WUI displays incorrect information.

CR 56662

Users are unable to change values in the Session Type and Session Status fields in the Define Session Filter WUI.

CR 56683

The pdsource table does not update correctly when a session is started from the Source Definition List UI using a modified Session ID. The new active session does not display.

CR 56785

A component UI session teardown selection is not available on the Netcrypt WUI.

CR 56861

When a user selects the **Software For Selected** WUI, the DNCS SDV Server WUI should indicate that the system is active during the times that the software loading times are slow.

CR 56876

A run-time exception error and a core dump occur when a user stops the spectroServer process. The system dumps the core file into the /export/home/dncs directory.

Workaround: Restart _consoleui.

CR 57335

Process status in the DNCS Control GUI is not updated correctly for the dbsync, eventManager, logManager, and dncs-snmpd-* processes. Users may draw incorrect conclusions from what they see in the GUI.

CR 57542

The Netcrypt Multicast Session List WUI may display incorrect User Datagram Protocol (UDP) port values for a corresponding session.

CR 59375

Users are unable to create Playouts using out-of-band signaling in the tsBroadcaster window.

CR 60034

The Netcrypt Report displays an incorrect Encryption Type when the 3rd Party CA Parameters page is updated. The Netcrypt Report displays “DVB Simulcrypt” instead of “PowerKEY.”

CR 60046

During staging, if Operating System Manager (OSM) download cannot find an image file in the /dvs/dvsFiles/OSM directory, OSM does not copy new image files to bootloader.

Workaround: Delete the failed image from the Image GUI.

CR 60572

When a system operator replaces a defective GQAM modulator unit, the sessions will become active; however, they will not be encrypted.

Workaround: Save the configuration for the GQAM modulator on the DNCS GQAM GUI, and then reboot the GQAM.

CR 61108

When a third-party network management system (NMS) is used to receive alarms from the DNCS, the session IDs and session numbers will not match the actual values in the NMS.

CR 61767

Users cannot add two programs for a single channel when using a PowerKEY CableCARD module. The split channel function is not working correctly.

CR 62388

The DNCS sends an incorrect provisioning message to the GQAM when a user sets the switching mode to "Auto" while configuring a dual GigE GQAM from the DNCS. The GQAM interprets the switching mode as "Manual" instead of "Auto." This can be confusing to the user.

CR 62649

Users cannot disable GQAM ports from the DNCS UI. This creates difficulty when setting up VOD sessions.

CR 62980

The DNCS must bypass the Netcrypt for clear VOD sessions.

CR 63068

System operators cannot create MPEG Multicast sessions on GQAM modulators.

CR 63518

The siManager process does not update correctly when upgrading a system from SR 2.2 to SR 4.2. After the upgrade, there may be conflicting or duplicate frequencies and hub parameters associated with the same source. After the duplicates are resolved, the siManager process does not update.

Workaround: Stop and restart the siManager process.

CR 63558

When a user enters invalid data into the Client ID and DSG Tunnel Address Fields on the Client Filter WUI, the WUI provides a message specifying the correct format for the data. However, you can still save the WUI with invalid Client ID and DSG Tunnel Addresses.

CR 63755

When a QAM modulator reboots, there is limited bandwidth on QAM channels.

CR 63914

Enhanced Channel Map Group Definition Rules do not retain their position in the list. This may cause set-tops using the Enhanced Channel Map feature to unexpectedly change from using one channel map to another after the number of rules exceeds 32.

CR 63936

When a user creates and saves new Enhanced Channel Map Group Definition rules, or when a user modifies existing rules and then selects the Group Definitions navigation link prior to selecting the Write File link, all of the new, saved, and modified rules are lost and must be re-created.

CR 64110

Users are unable to build continuous feed (CF) Broadcast Unicast sessions on the Netcrypt.

CR 64144

When the Channel Logo Number option is used for the Music Screen Saver feature, the number entered in the Channel Logo Number field does not appear in the field after the number has been saved.

CR 64658

Netcrypt sessions may not be visible at the set-top after they are modified to an encrypted state.

Workaround: Stop and restart (bounce) the siManager process after changing security modes for non-Cisco sources (third party QAMs).

CR 65268

The DRM process exhibits minor memory leaks while running VOD with an Extra Dense QAM Array (XDQA) QAM as the edge device.

CR 65327

During staging, code version table (CVT) download association fails intermittently and generates a core dump.

CR 65380

When a user deletes an Hct_type that is currently in use on the system, the Idm process returns an unspecified error.

CR 65573

The DNCS does not provide enhanced channel map information for Multi-Stream CableCARD modules (M-Cards).

CR 65909

Users may not be able to change or remove hub associations from the channel map.

CR 65972

When a user creates a segment with the same name as an existing segment, the system modifies the existing segment without notifying the user.

CR 65976

Users cannot edit the IP/Bridge name for a Cable Modem Termination System (CMTS) that is already provisioned on the system.

Workaround: Delete the CMTS and provision it again with the new name.

CR 66213

The Multi-Media Message (MMM) UI occasionally fails unexpectedly. When this failure occurs, users are unable to send EAS messages from the DNCS.

CR 66354

If the .profile file on the DNCS contains the variable LOG_TO_EMS and the value is set to "1," several system GUIs core dump.

Workaround: Set the LOG_TO_EMS variable to "0" (zero), source the .profile file, and then re-open the DNCS Administrative Console.

CR 66393

If the system operator changes the DNCS system IP address, the remote procedure call (RPC) UI is not available when the operator creates a new Value Added Service Provider (VASP) Type.

CR 66862

The qpskManager process occasionally causes corrupt SI packets. Corrupt SI packets may cause the set-top to lose its authorization and go into brick mode.

CR 67052

PowerKEY CableCARD modules may not receive split channels correctly during DST changes.

CR 67063

The dataPump (carousel) is sending bad packets to the ASI card, which causes the card to reset. When this reset occurs, there is no BFS data transmitted from the DNCS.

Workaround: Reboot the DNCS host to correct this condition.

CR 67225

The bfsServer does not reject create link requests on a source when the source is full. This failure to reject create link requests causes the carousel to become non-functional.

CR 67312

System operators are unable to set up VOD using MPEG Source to GQAM GigE port connectivity.

CR 67356

The SW TOC Selection window on the DNCS does not allow users to select a TOC file for the set-top.

Workaround: Manually type the TOC file name into the Selection field on the SW TOC Selection window.

2

SDV: The New Optional Feature in SR 2.7

Introduction

SR 2.7 offers Switched Digital Video (SDV) as a new optional feature. This chapter provides a brief description of the features and benefits of SDV.

If you are interested in SDV, please contact your Cisco marketing representative for more information.

In This Chapter

Switched Digital Video: Optimizes Bandwidth Utilization

Overview

The growth in service bandwidth available to the cable service provider has far outpaced the increases in available access network bandwidth. This growth is due, in part, to upgrades and rebuilds. This same expansion of available services has also created a situation in which, at any given time and in any given service group, most services are not being viewed. Thus, bandwidth for an edge device (for example, a QAM modulator) and access network bandwidth is wasted because many of the services that are continuously broadcast to subscribers are not being watched. SDV is a technique that recaptures such potentially wasted access network bandwidth by delivering selected services only where and when users are actively requesting service. This technique is performed through program switching.

SDV is an optional feature in SR 2.7 that optimizes bandwidth utilization at edge devices delivering content to cable network subscribers. Implementation of SDV in the Cisco DBDS network utilizes technology that ensures efficient sharing of QAM bandwidth between VOD and SDV services.

As a new DBDS technology, SDV imposes requirements on the following existing DBDS elements: DNCS, GQAM, and DHCT. These elements all interact with a new element of the DBDS—the SDV Server.

Important! SDV is an optional feature that must be purchased and installed separately.

Note: SDV also requires the functionality of the Netcrypt Bulk Encryptor.

An End-to-End Solution is Now Available

With the release of SR 2.7, Cisco is able to provide an end-to-end solution for cable service providers that want to deploy SDV in their system. The hardware, software, and technical expertise required to implement SDV is now available from Cisco.

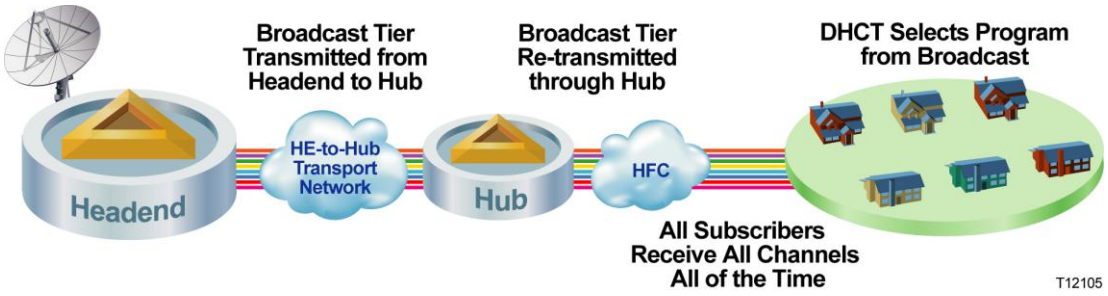
Switched Digital Video Benefits

The SDV solution provides the following benefits to cable service providers:

- Enhanced bandwidth management
  - Provides an immediate bandwidth savings, compared with the linear delivery of broadcast content
  - Increases in effective bandwidth allow for expansion of HD, VOD, Voice over Internet Protocol (VoIP), and high-speed data (HSD)
  - Allocated bandwidth demand is driven by viewership (not the number of programs offered)
- Specialized broadcast program tiers
  - Create additional specialized content tiers for smaller demographic groups
  - Potential source of new premium subscriptions
- Distributed resource management
  - Resources (QAM modulators and Ethernet switch/routers) supporting multiple applications are managed by a single (master) resource manager, thus enabling sharing of those resources by all the applications, including digital service, VOD, SDV, and traditional broadcast, to name a few
  - Channel changes for high-speed, real-time applications (such as SDV) are managed by distributed application-specific servers
- Performance
  - Channel change times are transparent to home consumers (SDV channel change times are essentially equivalent to digital broadcast channel change times)
- Viewership statistics
  - Track and report channel change information for optimal system performance and bandwidth management, pre-setting highly viewed programs
  - Use information to optimize your programming options

Traditional Linear Broadcasting

The following diagram illustrates the traditional method of "linear" broadcasting over HFC. Some "narrowcasting" is done in that not all hubs need to carry all the same content. However, any broadcast content that is selected for that hub is transmitted continuously to all subscribers.



This method of linear broadcasting is extremely simple and has worked reliably and cost-effectively for both cable service providers and consumers. However, increases in channel offerings and higher-bandwidth programming content, such as high-definition (HD) programming, have resulted in a greater demand for bandwidth. This bandwidth demand cannot be readily satisfied by continuous access network upgrades and rebuilds. It is no longer cost-effective to continuously increase bandwidth for services with low viewership. Cable service providers have a need for a new architecture that will reclaim wasted bandwidth and improve the subscriber's experience without requiring endless bandwidth expansion. SDV represents that new architecture.

The Switched Digital Solution

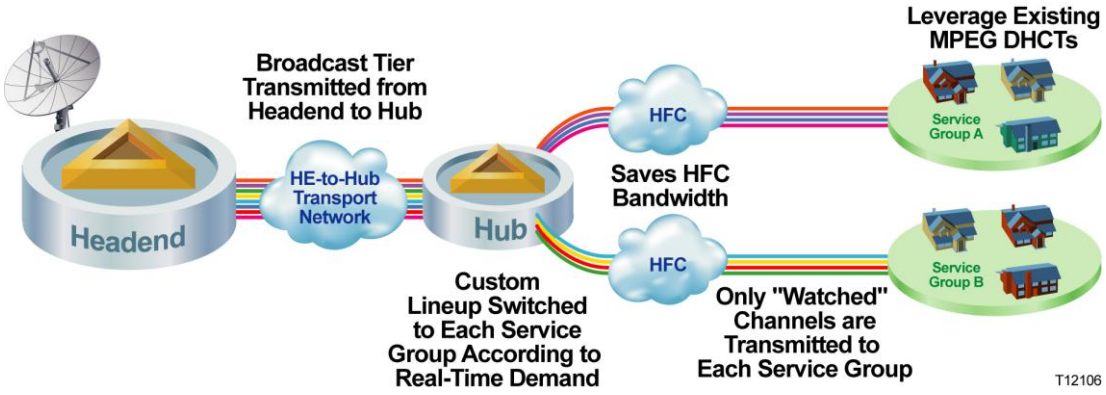
The advent of SDV technology promises to fundamentally change the way the industry delivers digital entertainment. With SDV, service providers have the ability to offer a wider variety of programming while managing HFC network bandwidth in a sustainable way.

In a manner similar to a telephone system, which switches a smaller number of lines upon the demand of a larger number of customers, the SDV architecture switches only selected content onto the HFC upon the demand of one or more viewers. Thus, content that is not requested by anyone in a service group does not occupy HFC bandwidth or require edge modulator resources.

With SDV, popular content continues to be broadcast continuously, while less popular content is held back and transmitted only upon request. Unlike video-on-demand (VOD), with SDV (after the content is transmitted) that stream is shared by any subsequent viewers requesting the same content within the same service group.

SDV also provides access to broadcast service while VOD is retrieving stored content from a server. As a result, SDV still uses the broadcaster's schedule to determine when a program airs.

The following diagram illustrates the typical SDV broadcast flow.



3

What Are the Site Requirements for SR 2.7?

Introduction

This chapter provides information that helps you prepare for the upgrade to SR 2.7. Read this entire chapter before you upgrade.

Application Testing

Application testing for SR 2.7 was completed using a sample of applications developed for SR 4.0. The functionality of the tested applications was not affected.

For More Information

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

In This Chapter

Upgrade Logistics

Introduction

This section contains information that can help system operators plan the upgrade to SR 2.7.

Supported Upgrade Path

Note these important upgrade requirements:

- Systems that upgrade to SR 2.7 must currently be operating with system software from SR 2.2 or SR 3.2, or later, as well as DHCT client operating system (OS) 3.1 or later. The upgrade software is contained in a UniPack due to significant changes contained in SR 2.7 and other time saving factors. Rollback procedures and software are included in the UniPack installation instructions in the event that the upgrade is unsuccessful.
- Cisco field service engineers or the system operator must have already installed the DNCS Utilities software onto the DNCS and should have already run the pre-upgrade checks to ensure system compatibility with SR 2.7 UniPack upgrade requirements. Refer to *DNCS Utilities Installation and Operation Guide* for instructions on installing and executing the DNCS Utilities.

Important: With the release of SR 2.7, Cisco introduces Live Upgrade with the Unipack. Through the use of Live Upgrade, engineers can upgrade an Enterprise 450 and Sun Fire V880 server without shutting down the system processes until you activate the new system software.

Time to Complete

The actual upgrade to SR 2.7 must be completed from within a 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 42) for additional details.

System Performance Impact

Interactive services will not be available during the maintenance window.

DNCS and Application Server Hardware Platforms

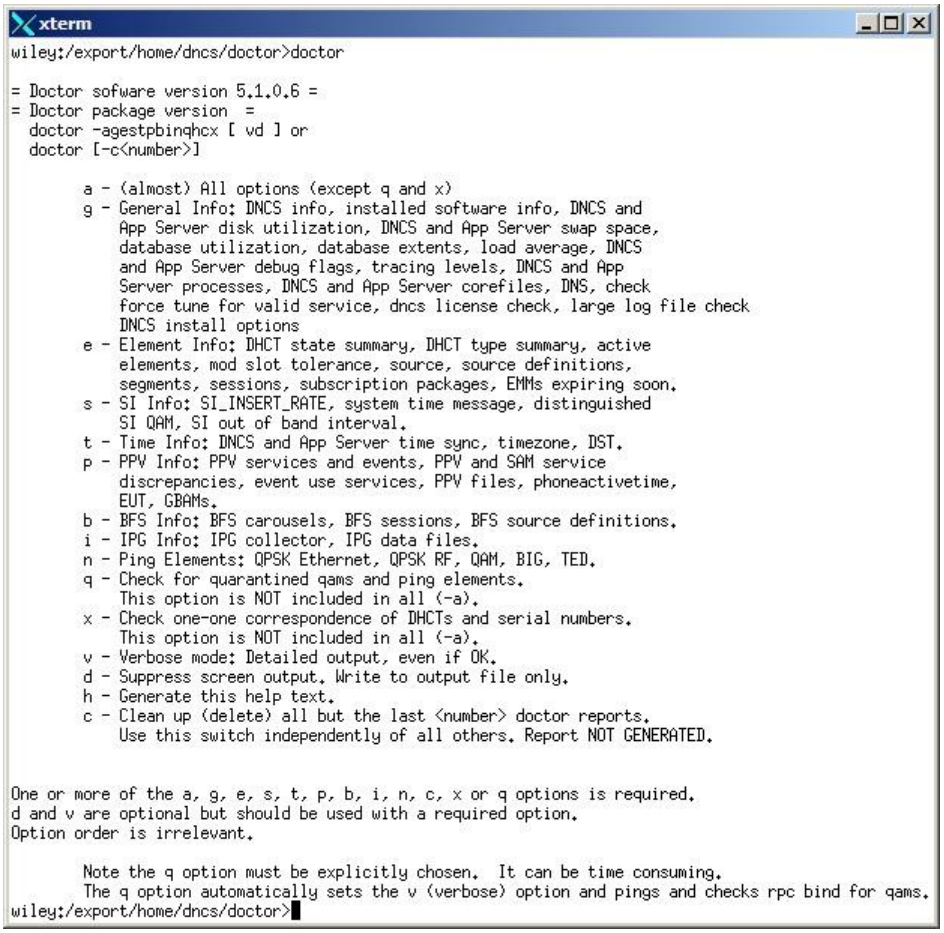
Introduction

This section describes the hardware configurations that are supported by SR 2.7.

Running the Doctor Report

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

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



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.

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 6.1 Installation Instructions and DNCS Utilities User's Guide*.

Important! DBDS Utilities 6.1 is required for SR 2.7.

DNCS System Release Required

Your system must be running SR 2.2, SR 3.2, or later. In the Doctor Report, look for the **SAIdncs** 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 Configurations

Ensure your site meets the following DNCS hardware requirements before upgrading to SR 2.7. The following table lists the minimum requirements for the DNCS hardware platforms that are supported by SR 2.7.

DNCS Server Platform	Hard Drive Configuration	Memory	Processor
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.
Sun Enterprise 450	■ 7 X 9 GB ■ 7 X 18 GB ■ 10 X 9 GB ■ 10 X 18 GB	1 GB min.	4 X 400 MHz min.

Application Server Hardware Configurations

The following table lists the Application Server hardware platforms that are supported by SR 2.7.

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 Blade 150	1 X 20 GB min.	512 MB min.	1 X 550 MHz min.
Sun Ultra 5	1 X 9 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 system release.

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, then subscribers may see video freezing and black screens when using VOD or *anything*-On-Demand (xOD) applications.

Note: This table does not apply if you are using Enhanced Channel Maps.

Set-Top Platform	Operating System (OS)	SARA*	PowerKEY Conditional Access Version
Explorer 8300 DVR v. 1.3.1a17 (or later)	OS 6.14.10.1	1.87.14.1	3.7.5
Explorer 8000/8010 DVR v. 1.3.1a17 (or later)	OS 6.12.7.1	1.87.13.1	3.7.5
Explorer 3250HD MR4 P1 (or later)	OS 3.12.8.1	1.57.8.1	3.7.5
Explorer 2xxx, 31xx, 3200, 3100HD	OS 3.10.9	1.54.23.1	1.0.6.20 (Explorer 2000s) 1.0.7 (all others)

* *Cisco Resident Application*

Important! If you are not using the Cisco Resident Application, contact your resident application provider to verify that you have the most recent version.

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: ■ 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 2.7.

Difference Between SR 2.7 and SR 3.7

SR 2.7 and SR 3.7 are identical *except* that SR 2.7 does not support DOCSIS functionality. SR 3.7 ships with DOCSIS functionality disabled. The Cisco installation engineer will enable DOCSIS functionality as part of the upgrade to SR 3.7.

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 2.7.

DBDS Component	**Version Number**
DNCS	
Application	4.2.0.24
GUI/WUI	4.2.0.24
DNCS Application Patch	4.2.0.24p1
DNCS Support Software	
DNCS & Application Server Tools	4.2.0.13
DNCS Spectrum Kit	2.0.0.8
DNCS Report Writer	4.2.0.4
DNCS Online Help	4.2.0.3
PPP Support CD	3.0.0.0
DBDS Maintenance CD (v3.0.14)	
Backup / Restore Scripts	6.0.11

DBDS Component	Version Number
DBDS Utilities (v6.1.0.4))	
DNCS Utilities	5.1.0.9
Doctor Package Version	5.1.0.8
CoolTools Utilities	5.1.0.5
Application Server Utilities	3.0.1.27
DHCT Status	5.1.0.6
Spectrum Installation (v.3.5.0.0)	
Spectrum Enterprise Manager App Version	5.0 R1
Spectrum Supplement App.	CS3 / MMS3i P122
Platform	
DNCS / Application Server Platform	4.2.0.6
Solaris	10 03/05 HW1
Solaris 10 Recommended / Security Patches	4.2.0.5
Prom Patches	2.3
Fore ATM Drivers	4.2.0.0
Informix	9.20 uc3
Video Propulsion DVB Direct ASI	1.0.0.6 (VP 2.43)
Application Server	
Application Server	3.4.1.2
Application Server Software Support	
DNCS & Application Server Tools	4.2.0.13
BFS Remote	3.2.0.5AS
QAM	
QAM App	2.5.1
QAM Boot	2.1.0
MultiQAM	
MQAM App	2.6.10
MQAM Boot	1.2.3

DBDS Component	Version Number
GQAM	
GQAM	4.0.6
GQAM Boot	4.0.6
GoQAM RF / GoQAM IF	
GoQAM RF / GoQAM IF	1.1.2
GoQAM Boot	1.0.0
GTQAM	
GTQAM	1.0
QPSK Mod/Demod	
QPSK Modulator	E14
QPSK Demodulator	E14
Netcrypt	
Netcrypt Bulk Encryptor	1.1.3
Switched Digital Services	
SDV Broadcast Application	1.3.3
Switched Digital Broadcast OS	1.0
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 D9476 App	0.8.2
GPI Card D9476 Boot	0.6.7
Automux Script	2.3

DBDS Component	Version Number
Sonet	
Sonet/ASI (STA)	1.3.4
RNCS DVD (v2.0.0.13)	
RNCS LIONN Application	1.2.0.24
RNCS LIONN Platform	2.0.0.4
RNCS Tools	2.0.0.3

4

Customer Information

Introduction

This chapter contains information on obtaining product support and returning products to Cisco.

In This Chapter

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

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

June 2012 Printed in USA

Part Number 4012155 Rev B