System Release 3.5

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

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

Contents, Continued

About This Guide

Introduction

System Release 3.5 (SR 3.5) is a minor 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 3.5
- Information you need to prepare your site for an upgrade to SR 3.5
- Change requests (CRs) that were found in previous system releases and corrected in SR 3.5
- A summary of open issues for the standard version of SR 3.5
- A summary of open issues associated with optional features for SR 3.5
- General information on contacting Cisco
- A list of software versions installed with the base SR 3.5 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 3.5. If you have questions about this release or require more detailed information, contact Cisco Services.

Document Version

This is the second formal release of these release notes.

Chapter 1
Why Choose System Release 3.5?

Overview

Introduction

SR 3.5 includes many features and enhancements implemented at the request of our customers. Review this chapter to learn more about these exciting changes.

Note: 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**.

In This Chapter

This chapter contains the following topics.

SR 3.5 at a Glance

Overview

This section provides an "at-a-glance" look at the new features and enhancements for SR 3.5. Each feature and enhancement is described in detail later in this chapter.

DOCSIS (DSG): New "DOCSIS Only" Option Can Consolidate Administration of the Data Network

In addition to the previously supported DAVIC* and mixed DAVIC/DOCSIS® modes, SR 3.5 introduces the new DOCSIS* mode for transporting all set-top data over the DOCSIS infrastructure. 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 3.5 also introduces single-flow multicast support to help you conserve bandwidth on your data network.

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

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

SR 3.5 includes CableCARD™ module support for the following PKM600 PowerKEY® Conditional Access Module features:

- Automated Content Protection Binding for Two-Way Hosts
- Split Channels

Logging: New Logging Utility Makes Troubleshooting Even Easier

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

Instastaging: Stage On Demand in the Subscriber's Home

Two-way systems can use Instastaging to perform just-in-time staging from subscribers' homes. Instastaging offers two ways to stage set-tops: subscribers can pick up set-tops at retail centers, and then install and provision the set-tops in their homes; or technicians can install and provision set-tops in subscribers' homes.

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

A new GUI Servers button on the Utilities tab provides access to powerful user interface (UI) server monitoring tools.

Sessions: UI Enhancements Increase Usability of the Session List

New filtering options and more detailed session information make it easier to find the information you need from the session list screens.

More DNCS Enhancements: Improvements Make Familiar Tasks Easier

Several enhancements to existing features throughout the DNCS make common tasks even easier.

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

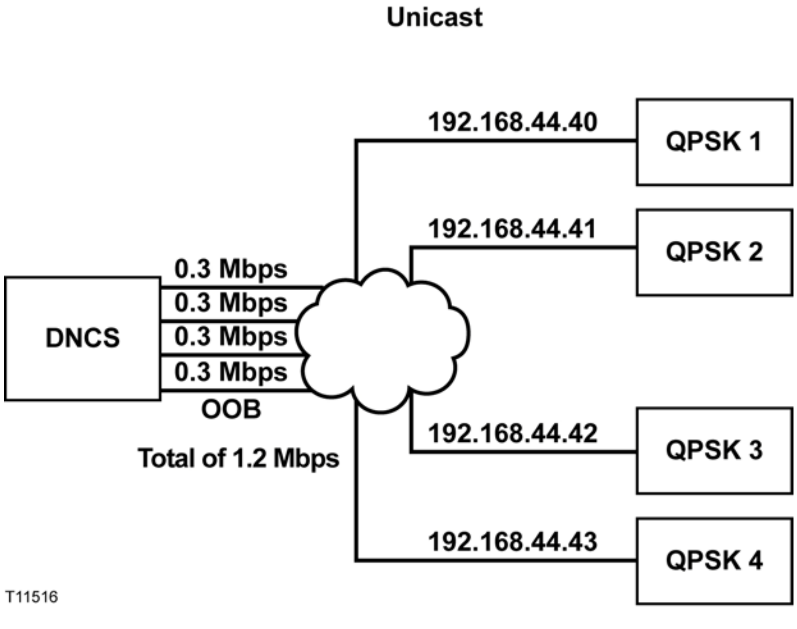
Overview

Existing support for DOCSIS-capable set-tops is enhanced with the introduction of DOCSIS mode and single-flow multicast. This chapter describes new network configurations and several UI changes associated with these new features.

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. Each physical bridge consumes additional network bandwidth for each additional OOB bridge.

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.

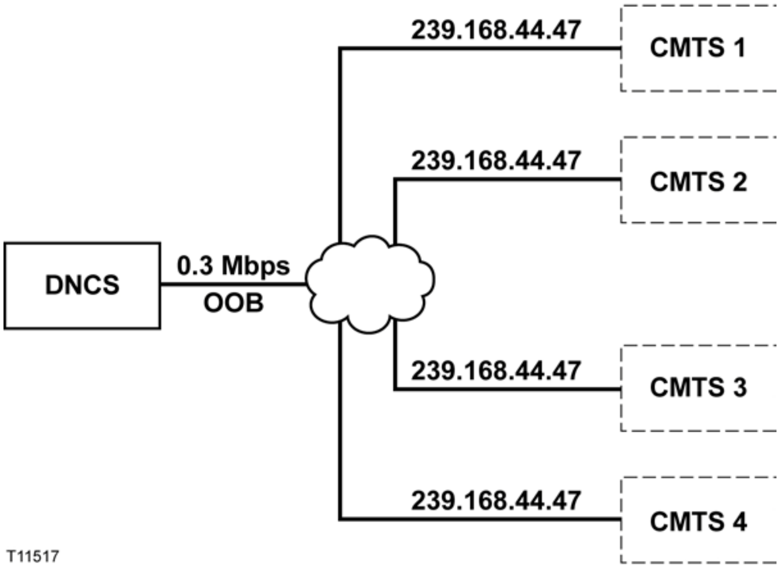


In SR 3.5, systems can continue to use unicast IP routing as necessary to support non-DOCSIS-capable set-tops. For DOCSIS-capable set-tops, SR 3.5 introduces support for "single-flow" multicast IP routing (multicasting). With single-flow multicast, the network uses one group destination IP address (GDA) 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.

Single-Flow Multicast



Editing the Time to Live for Multicasting

An IP multicast packet must “hop” or traverse routers to reach its final destination of a CMTS device. SR 3.5 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.

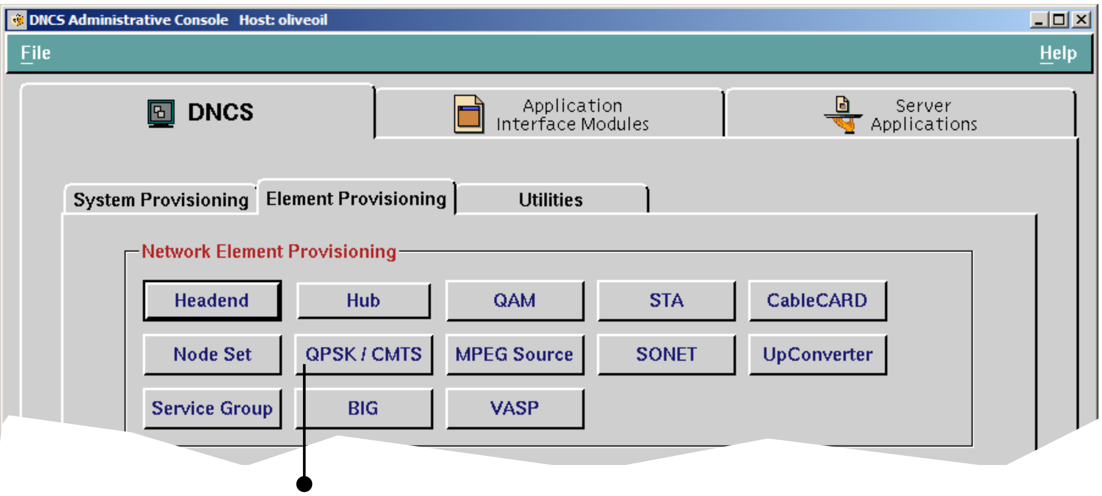
Which Set-Top Models Can I Use?

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.

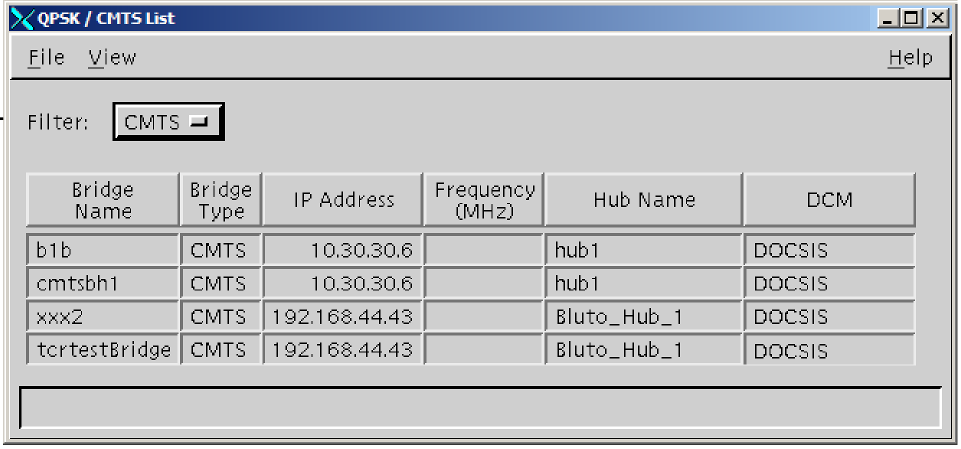
The New QPSK/CMTS Interface

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.



Filter: CMTS

Bridge Name	Bridge Type	IP Address	Frequency (MHz)	Hub Name	DCM
b1b	CMTS	10.30.30.6		hub1	DOCSIS
cmtsbh1	CMTS	10.30.30.6		hub1	DOCSIS
xxx2	CMTS	192.168.44.43		Bluto_Hub_1	DOCSIS
tcrtestBridge	CMTS	192.168.44.43		Bluto_Hub_1	DOCSIS

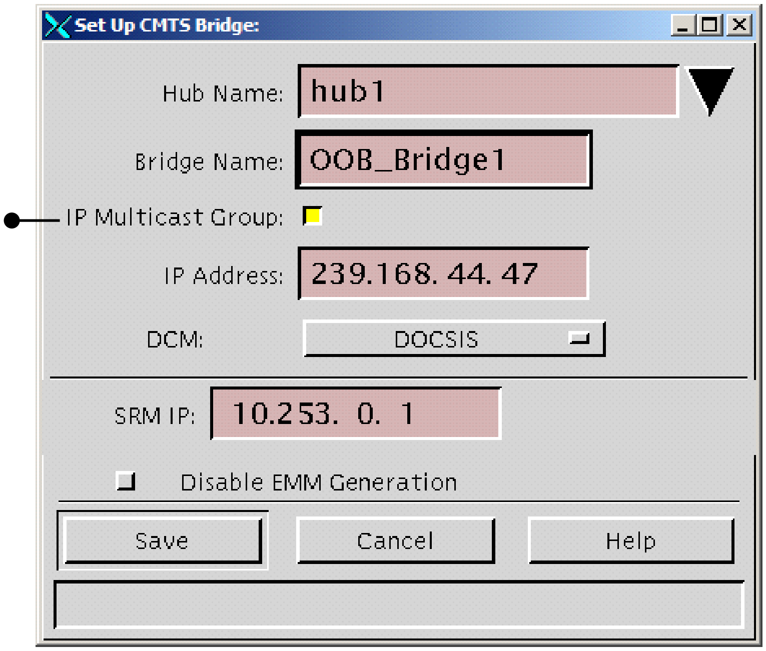
You can filter the list to show CMTS bridges only, QPSK bridges only, or both.

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.



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

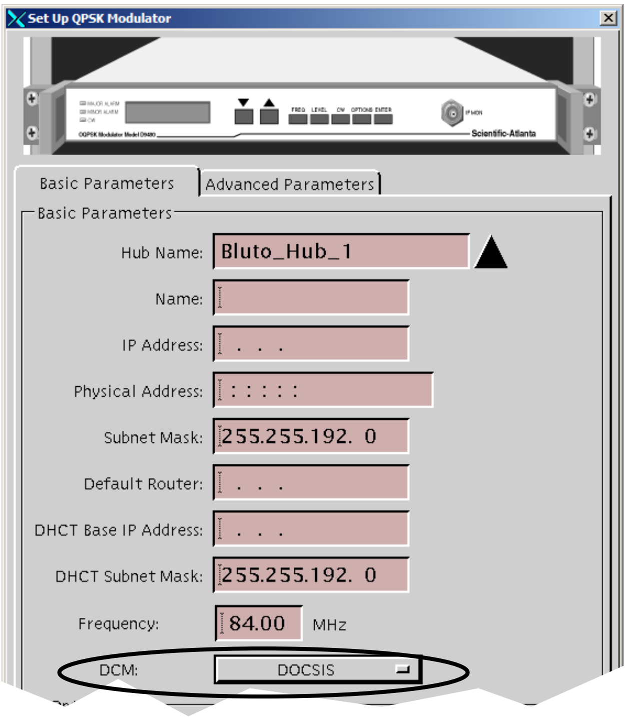
You can select this box to turn on multicast IP address validation. This validation ensures the IP Address is a multicast address.

In SR 3.5, 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*.

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 3.5 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.



Set Up QPSK Modulator

Basic Parameters

Hub Name: Bluto_Hub_1

Name:

IP Address: . . .

Physical Address: : : : : :

Subnet Mask: 255.255.192. 0

Default Router: . . .

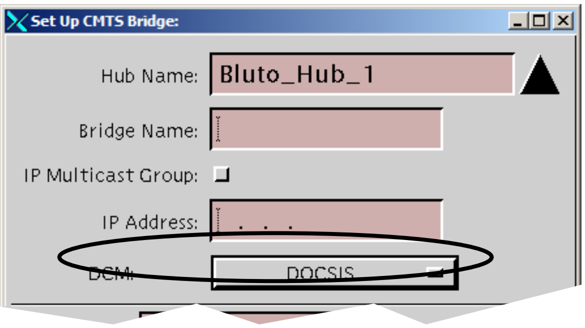
DHCT Base IP Address: . . .

DHCT Subnet Mask: 255.255.192. 0

Frequency: 84.00 MHz

DCM: DOCSIS

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



Set Up CMTS Bridge:

Hub Name: Bluto_Hub_1

Bridge Name:

IP Multicast Group: □

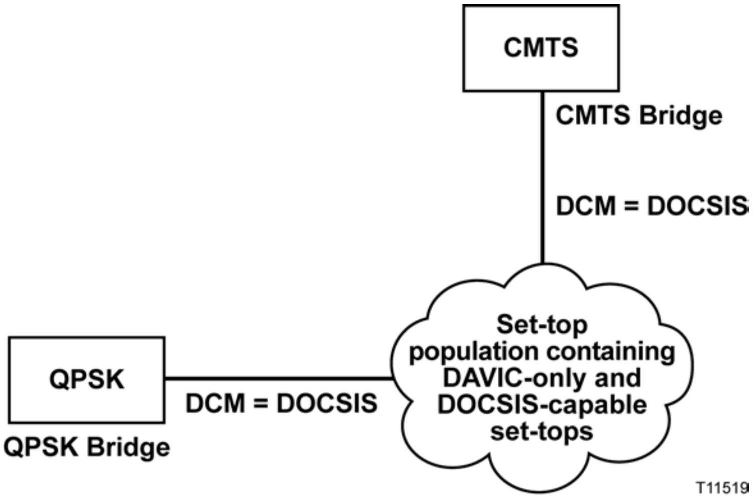
IP Address: . . .

DCM: DOCSIS

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.


CMTS
CMTS Bridge
DCM = DOCSIS
Set-top population containing DAVIC-only and DOCSIS-capable set-tops
QPSK
DCM = DOCSIS
QPSK Bridge
T11519

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)*
- *DNCS Online Help*
- *Getting Started With the Explorer® 8300 and 8300HD DVR*
- *Connecting the Explorer® 8300 Digital Video Recorder*

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

Overview

SR 3.5 adds two new features for CableCARD module support: automated content protection binding for two-way hosts and split channel support.

Automated Content Protection Binding for Two-Way Hosts Means Fewer Customer Calls

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

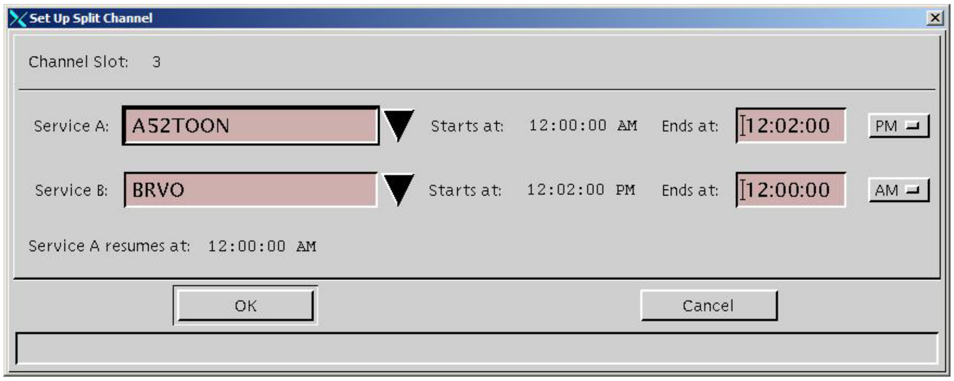
SR 3.5 supports content-protection binding for two-way OpenCable™ Host devices (Hosts). With two-way Hosts, content protection binding occurs automatically, assuming the CableCARD module is already loaded on the DNCS.

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. For detailed instructions, refer to the *DNCS Online Help* or to *Setting Up the PowerKey CableCARD Module on the DNCS for SR 4.0.*

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

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.



Channel Slot: 3

Service A: A52TOON Starts at: 12:00:00 AM Ends at: 12:02:00 PM

Service B: BRVO Starts at: 12:02:00 PM Ends at: 12:00:00 AM

Service A resumes at: 12:00:00 AM

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).

Logging: New Logging Utility Makes Troubleshooting Even Easier

Overview

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.

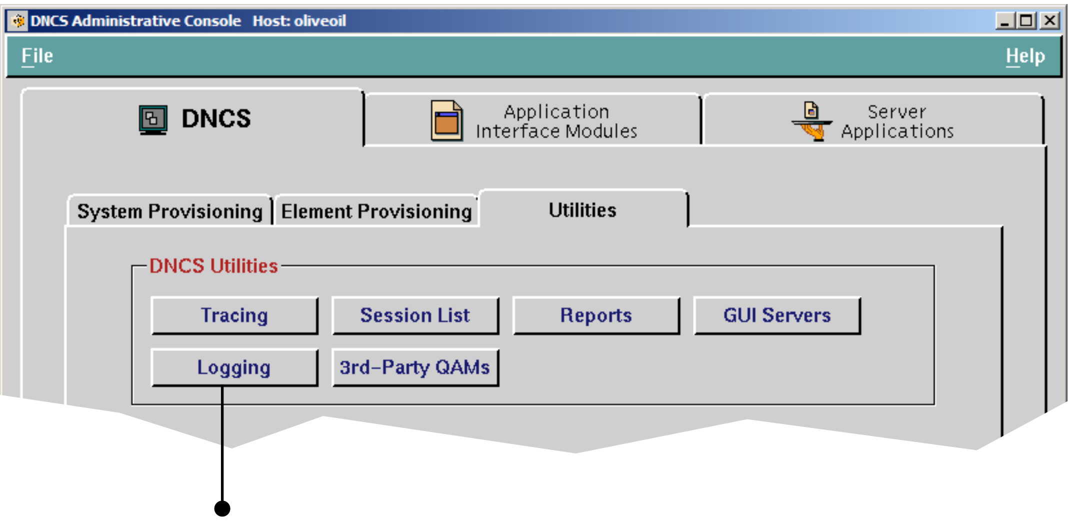
During normal operation, you may choose to log information at the Error Condition level only. If a problem occurs, you can turn on several additional log levels, such as the Alert and Debug levels, to capture more information in the dncsLog file and the individual process log files.

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*.

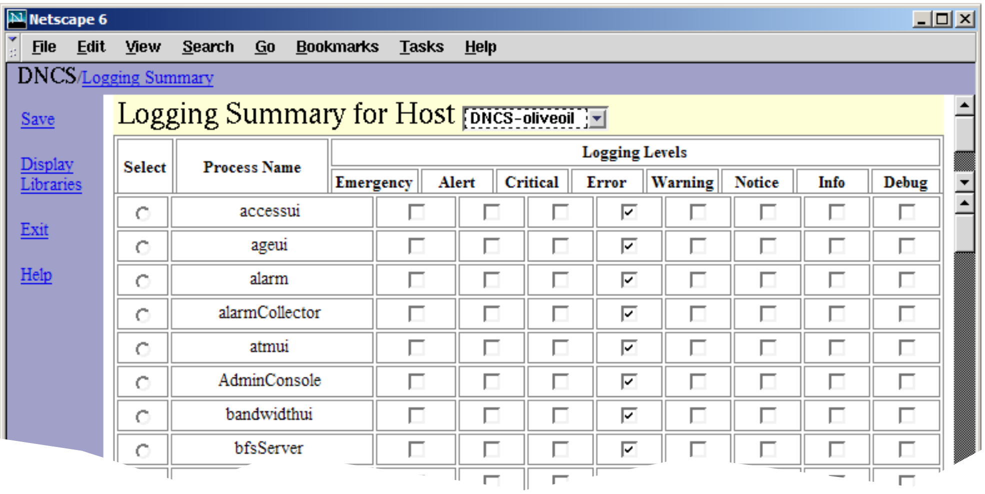
Welcome to the New Logging Interface

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).

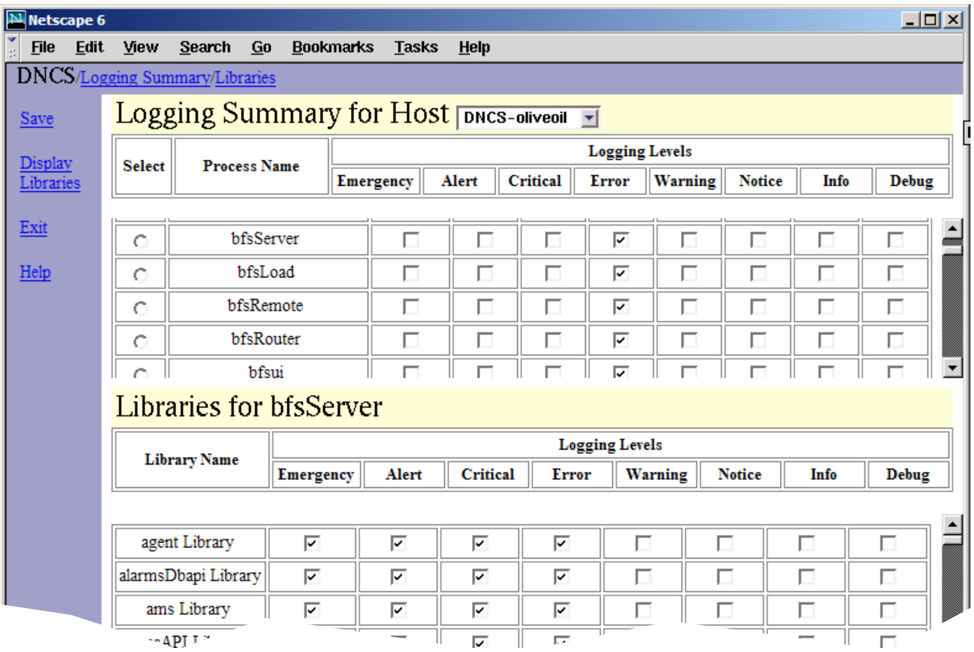
The Logging Summary page allows you to set logging levels for each process on a specific host. If you are using Cisco's Regional Control System (RCS) solution, you can set the log levels for each remote site.



Logging Summary for Host DNCS-oliveoil

Select	Process Name	Logging Levels							
		Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
○	accessui	□	□	□	☑	□	□	□	□
○	ageui	□	□	□	☑	□	□	□	□
○	alarm	□	□	□	☑	□	□	□	□
○	alarmCollector	□	□	□	☑	□	□	□	□
○	atmui	□	□	□	☑	□	□	□	□
○	AdminConsole	□	□	□	☑	□	□	□	□
○	bandwidthui	□	□	□	☑	□	□	□	□
○	bfsServer	□	□	□	☑	□	□	□	□

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.


Netscape 6
File Edit View Search Go Bookmarks Tasks Help
DNCS/Logging Summary/Libraries
Save
Display Libraries
Exit
Help

Logging Summary for Host DNCS-oliveoil

Select	Process Name	Logging Levels							
		Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
○	bfsServer	□	□	□	☑	□	□	□	□
○	bfsLoad	□	□	□	☑	□	□	□	□
○	bfsRemote	□	□	□	☑	□	□	□	□
○	bfsRouter	□	□	□	☑	□	□	□	□
○	bfsui	□	□	□	☑	□	□	□	□

Libraries for bfsServer

Library Name	Logging Levels							
	Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
agent Library	☑	☑	☑	☑	□	□	□	□
alarmsDbapi Library	☑	☑	☑	☑	□	□	□	□
ams Library	☑	☑	☑	☑	□	□	□	□

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).

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 and logManager 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.

Instastaging: Stage On Demand in the Subscriber's Home

Overview

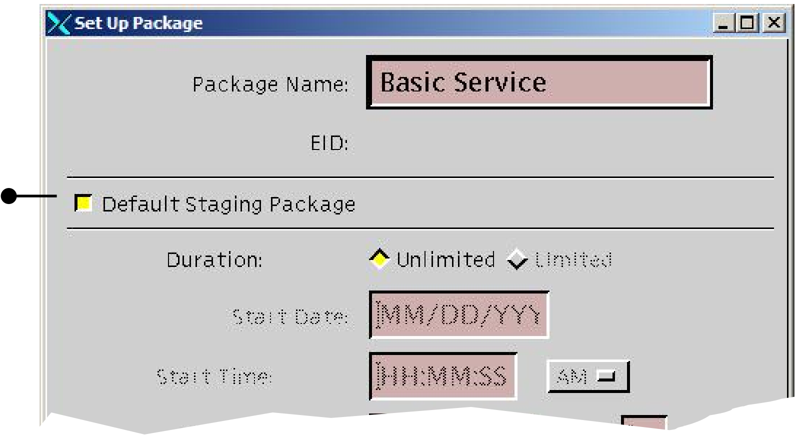
Instastaging streamlines the set-top staging process for two-way, PowerKEY® Conditional Access Systems. Rather than racking up large quantities of set-tops to stage from your warehouse, you can allow professional installers or your subscribers to stage set-tops on demand.

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.



Set Up Package

Package Name: Basic Service

EID:

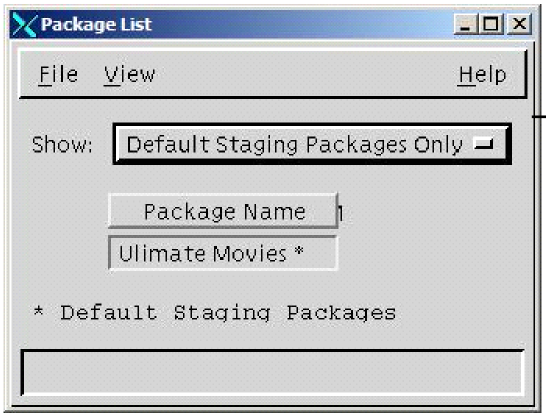
☑ Default Staging Package

Duration: ◆ Unlimited ◇ Limited

Start Date: MM/DD/YYY

Start Time: HH:MM:SS AM

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



Package List

Show: Default Staging Packages Only

Package Name
Ulimate Movies *

* Default Staging Packages

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

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 from a retail center. 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 command 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.

How Do I Configure a Churned Box to Be Instastaging Capable?

Simply take the box 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 Box to Receive EMMs?

Boxes 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 it critical to set these settings at the same time that the box 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

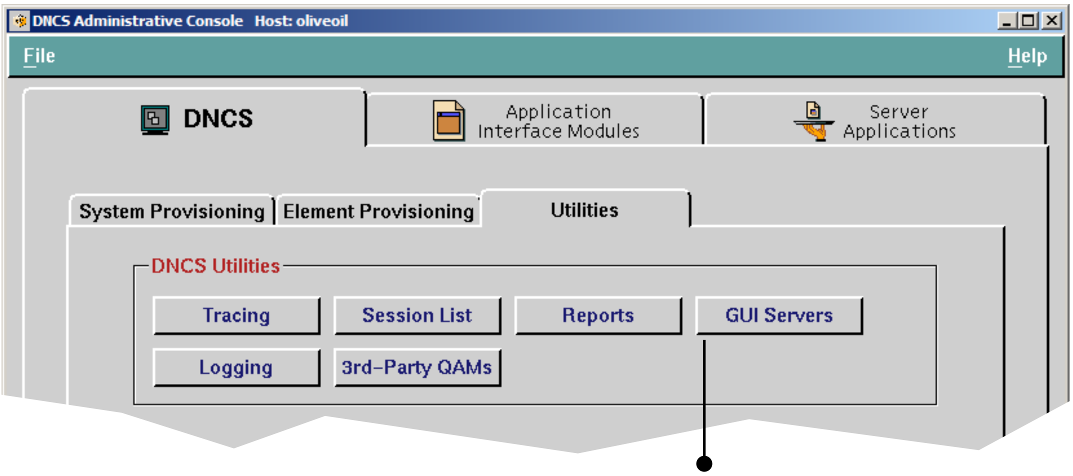
Simple Object Access Protocol (SOAP) is an XML-based messaging protocol for exchanging information over the Internet. The DNCS uses SOAP servers to integrate new Web-based interfaces with the legacy DNCS database and servers. As an example, the dbUIServer SOAP Server plays an important role in populating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

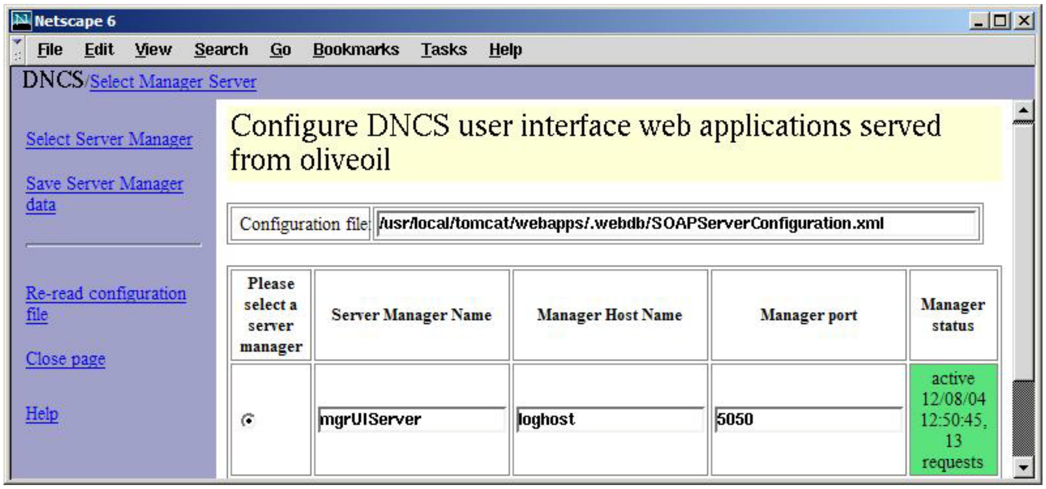
On occasion, you may need to check the status of a UI server. For example, if the CableCARD Web interface opens, but no data is populated, you can check to see if the UI server for the CableCARD module (dbUIServer) is running. For SR 3.5, all UI servers are managed by a single Server Manager. If the 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 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.

For SR 3.5, 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.


Netscape 6
File Edit View Search Go Bookmarks Tasks Help
DNCS/Select Manager Server
Select Server Manager
Save Server Manager data
Re-read configuration file
Close page
Help

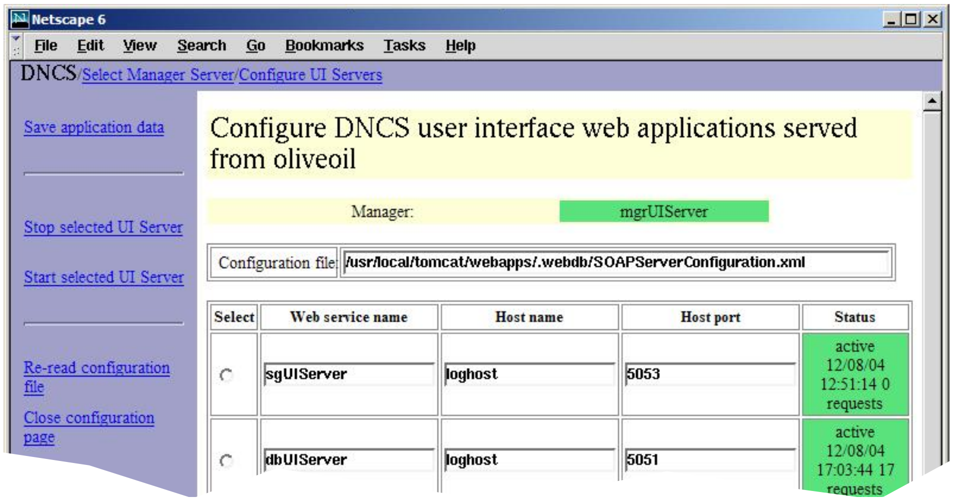
Configure DNCS user interface web applications served from oliveoil

Configuration file: /usr/local/tomcat/webapps/.webdb/SOAPServerConfiguration.xml

Please select a server manager	Server Manager Name	Manager Host Name	Manager port	Manager status
●	mgrUIServer	loghost	5050	active 12/08/04 12:50:45, 13 requests

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.


Netscape 6
File Edit View Search Go Bookmarks Tasks Help
DNCS/Select Manager Server/Configure UI Servers
Save application data
Stop selected UI Server
Start selected UI Server
Re-read configuration file
Close configuration page

Configure DNCS user interface web applications served from oliveoil

Manager: mgrUIServer

Configuration file: /usr/local/tomcat/webapps/.webdb/SOAPServerConfiguration.xml

Select	Web service name	Host name	Host port	Status
○	sgUIServer	loghost	5053	active 12/08/04 12:51:14 0 requests
○	dbUIServer	loghost	5051	active 12/08/04 17:03:44 17 requests

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

SR 3.5 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*.

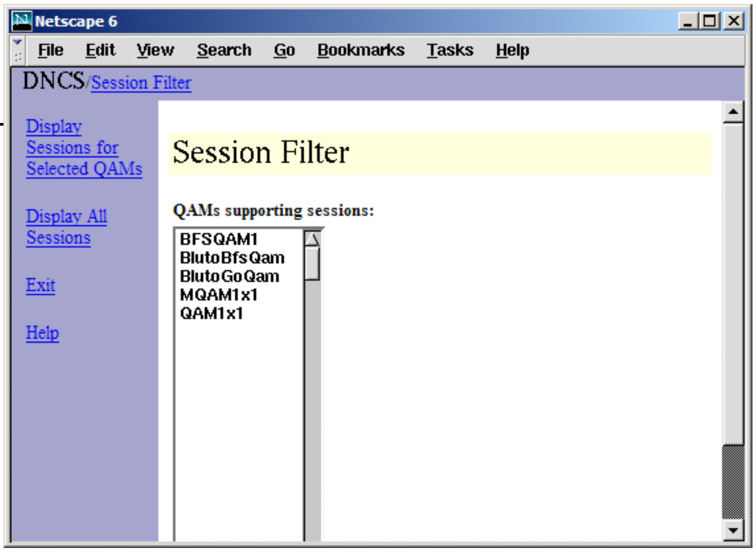
Sessions: UI Enhancements Increase Usability of the Session List

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> Sessions

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

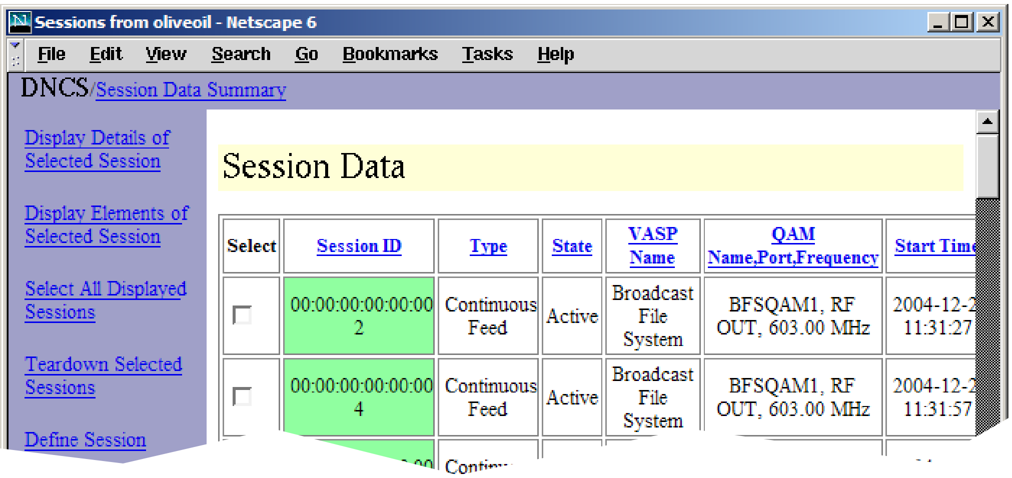


Focus the Session List with New Filtering Options

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.

Access Detailed Information for Selected Sessions

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



DNCS/Session Data Summary

Display Details of Selected Session

Display Elements of Selected Session

Select All Displayed Sessions

Teardown Selected Sessions

Define Session

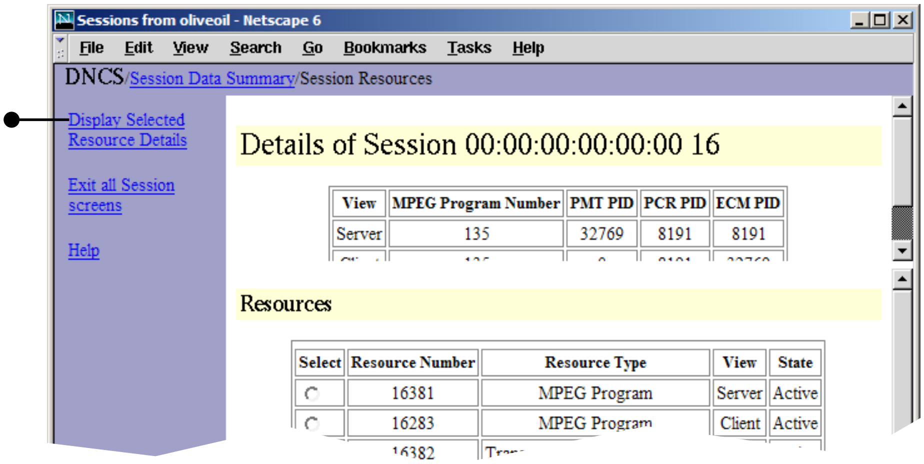
Session Data

Select	Session ID	Type	State	VASP Name	QAM Name,Port,Frequency	Start Time
□	00:00:00:00:00:00 2	Continuous Feed	Active	Broadcast File System	BFSQAM1, RF OUT, 603.00 MHz	2004-12-2 11:31:27
□	00:00:00:00:00:00 4	Continuous Feed	Active	Broadcast File System	BFSQAM1, RF OUT, 603.00 MHz	2004-12-2 11:31:57

You can display details or elements for a selected session.

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.


Sessions from oliveoil - Netscape 6
File
Edit
View
Search
Go
Bookmarks
Tasks
Help
Display Selected Resource Details
Exit all Session screens
Help

DNCS/Session Data Summary/Session Resources

Details of Session 00:00:00:00:00:00 16

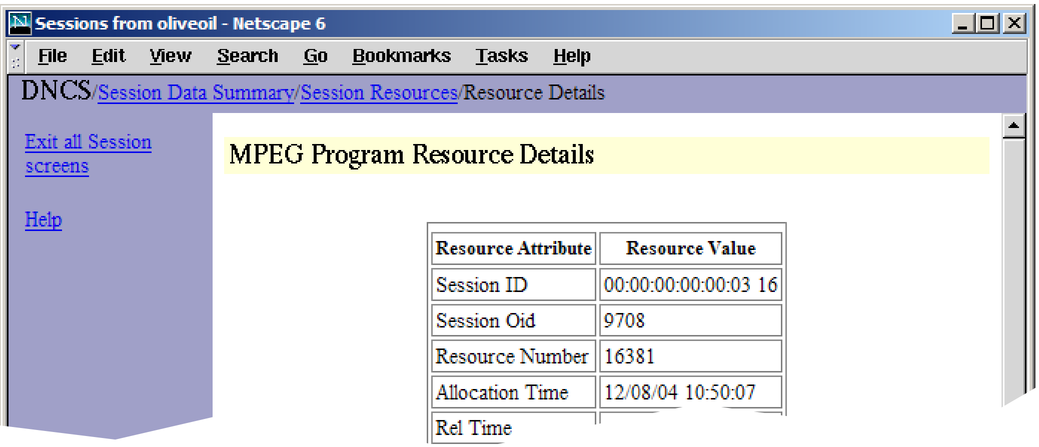
View	MPEG Program Number	PMT PID	PCR PID	ECM PID
Server	135	32769	8191	8191

Resources

Select	Resource Number	Resource Type	View	State
○	16381	MPEG Program	Server	Active
○	16283	MPEG Program	Client	Active
	16382			

Use this option to view details for a specific resource.

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.



DNCS/Session Data Summary/Session Resources/Resource Details

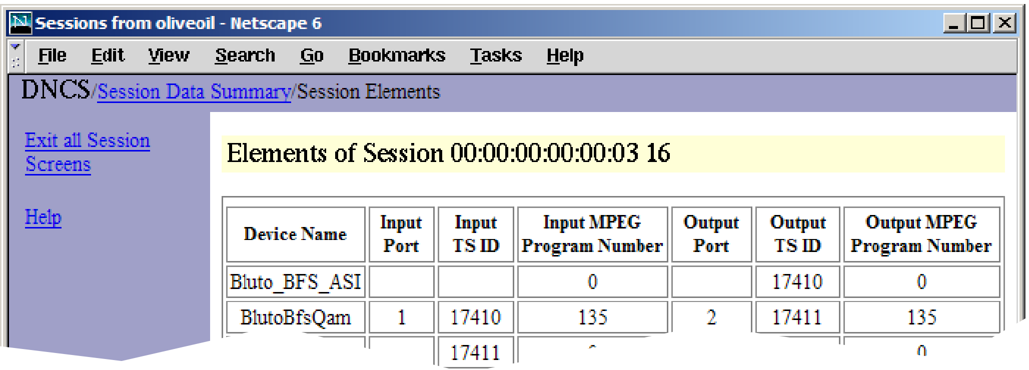
MPEG Program Resource Details

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	

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.


Sessions from oliveoil - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
DNCS/Session Data Summary/Session Elements
Exit all Session Screens
Help

Elements of Session 00:00:00:00:00:03 16

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

More DNCS Enhancements: Improvements Make Familiar Tasks Easier

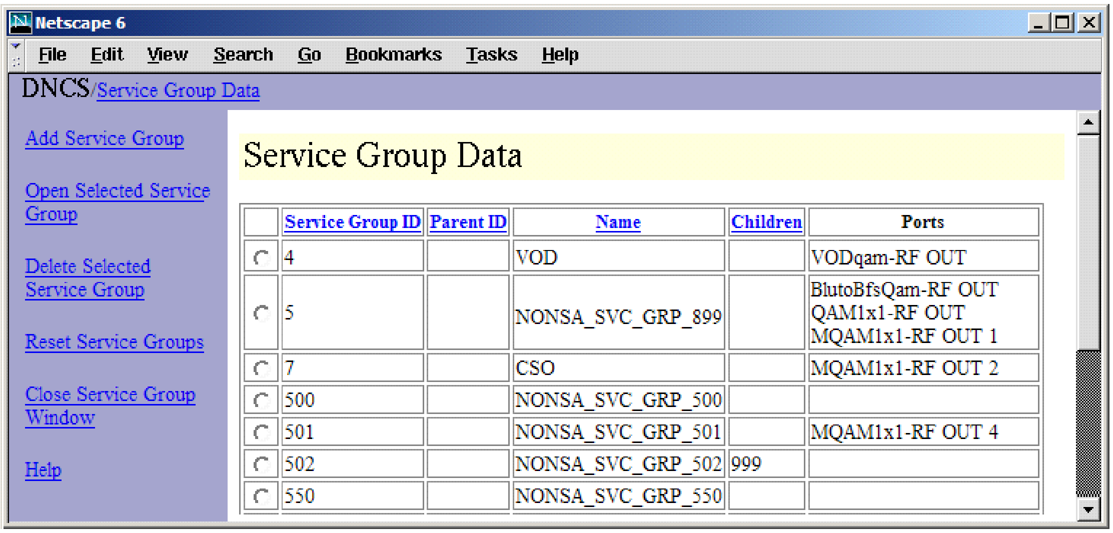
Overview

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



Service Group Data

	Service Group ID	Parent ID	Name	Children	Ports
○	4		VOD		VODqam-RF OUT
○	5		NONSA_SVC_GRP_899		BlutoBfsQam-RF OUT QAM1x1-RF OUT MQAM1x1-RF OUT 1
○	7		CSO		MQAM1x1-RF OUT 2
○	500		NONSA_SVC_GRP_500		
○	501		NONSA_SVC_GRP_501		MQAM1x1-RF OUT 4
○	502		NONSA_SVC_GRP_502	999	
○	550		NONSA_SVC_GRP_550		

Reference Data Rates and Block Sizes from a New Central Location

The *Recommendations for Data Carousel Rate Technical Bulletin* provides important guidelines for setting data rates, and most application installation guides provide guidelines for setting both the data rate and block size for inband and out-of-band sources. In previous releases, you had to open each individual source to view the data rate and block size for the source. SR 3.5 adds the **Data Rate** and **Block Size** columns to the **Sources** tab. These columns allow you to more quickly compare these values against documented recommendations and guidelines.

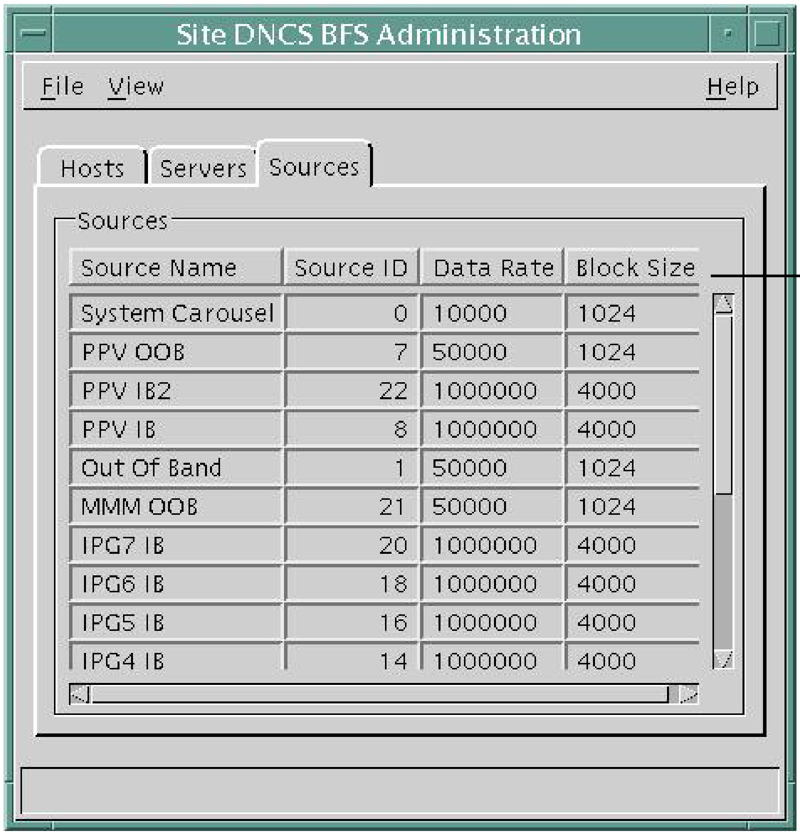
To ensure optimum performance as you add more applications to your system, review data rates and block sizes periodically. Depending on your system type (non-RCS or RCS), the following Quick Paths for the Sources path will vary.

- For non-RCS systems:

Quick Path: DNCS Administrative Console> Application Interface Modules tab> BFS Admin> Sources tab

- For RCS systems:

Quick Path: DNCS Administrative Console> Application Interface Modules tab> BFS Admin> (select Site) >File > Select > Sources tab



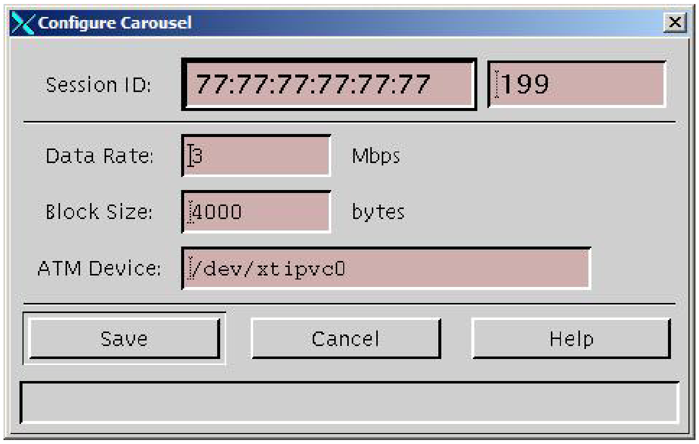
Source Name	Source ID	Data Rate	Block Size
System Carousel	0	10000	1024
PPV OOB	7	50000	1024
PPV IB2	22	1000000	4000
PPV IB	8	1000000	4000
Out Of Band	1	50000	1024
MMM OOB	21	50000	1024
IPG7 IB	20	1000000	4000
IPG6 IB	18	1000000	4000
IPG5 IB	16	1000000	4000
IPG4 IB	14	1000000	4000

The Data Rate and Block Size source parameters are more visible on the redesigned Sources tab.

Say Goodbye to the Configure Carousel Window and Duplicate Work

In SR 3.5, you still specify the Session ID and Inband Device Name (formerly known as the ATM Device) from the Hosts tab of the BFS Admin window, and you specify Block Sizes and Data Rates in the Sources tab of the BFS Admin window.

In previous system releases, you had to duplicate these entries in the Configure Carousel window for the Operating System Manager (OSM) session (for Code Version Table [CVT] downloads). To access the Configure Carousel window, shown below, you clicked **Image** on the Element Provisioning tab and then chose **Configure Carousel** from the **Advanced** menu option.



Session ID: 77:77:77:77:77:77 199

Data Rate: 3 Mbps

Block Size: 4000 bytes

ATM Device: /dev/xtipvc0

In SR 3.5, the OSM session is treated just like other BFS sessions rather than requiring its own unique carousel. 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-CISCO Digital Source Definition UI eliminates the need for mirror QAMs in PSIP configuration. Refer to the *Program and System Information Protocol Configuration for SR 2.5/SR 3.5* technical bulletin for details.

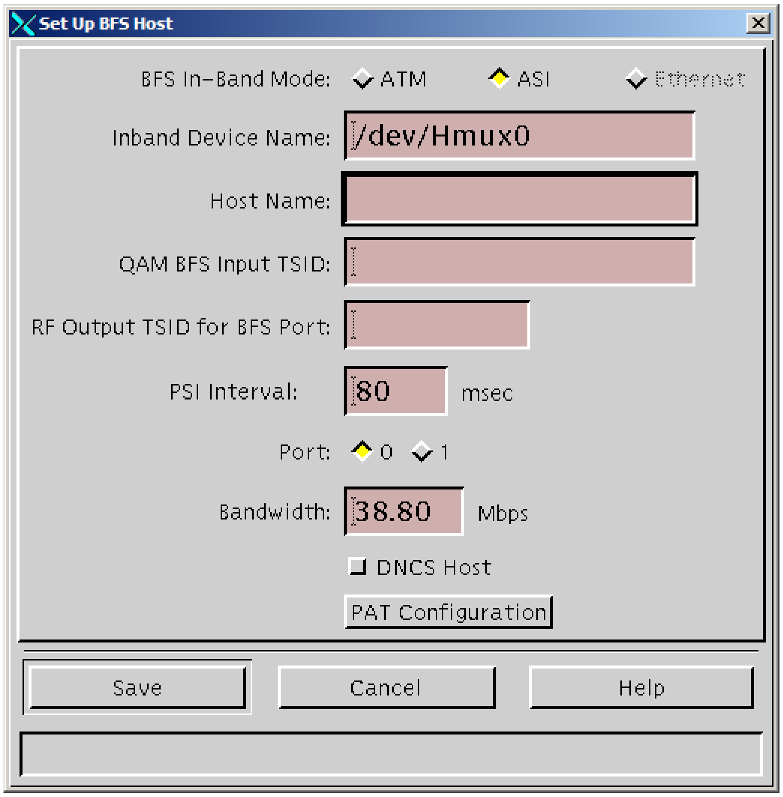
More DNCS Enhancements: Improvements Make Familiar Tasks Easier, Continued

Set Up the Inband Data Path from a More Logical Location

In previous releases, the inband data path was configured by clicking the **Inband Data Config** button on the Application Interface Module tab. However, setup 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 the Set Up BFS Host window (a machine-specific screen).

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



Set Up BFS Host

BFS In-Band Mode: ○ ATM ● ASI ○ Ethernet

Inband Device Name: /dev/Hmux0

Host Name:

QAM BFS Input TSID:

RF Output TSID for BFS Port:

PSI Interval: 80 msec

Port: ● 0 ○ 1

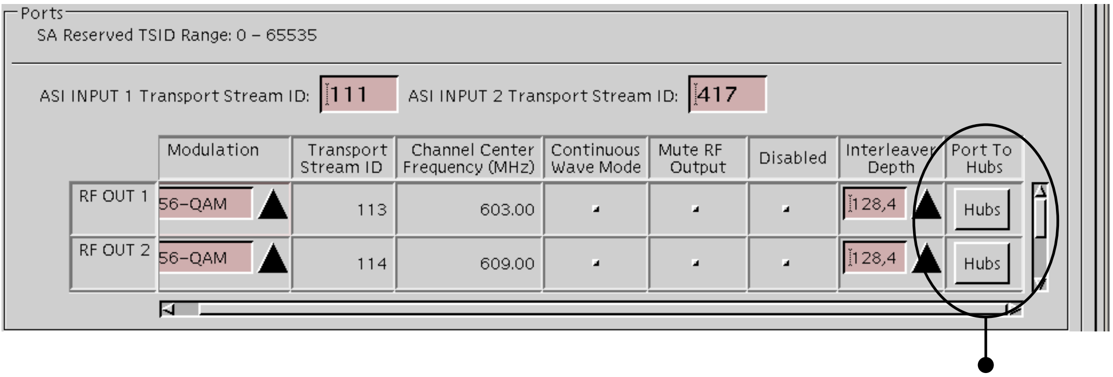
Bandwidth: 38.80 Mbps

□ DNCS Host

More DNCS Enhancements: Improvements Make Familiar Tasks Easier, Continued

Use MQAMs To Feed Multiple Hubs

A new user interface allows you to associate individual RF outputs in an MQAM with specific hubs. 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.



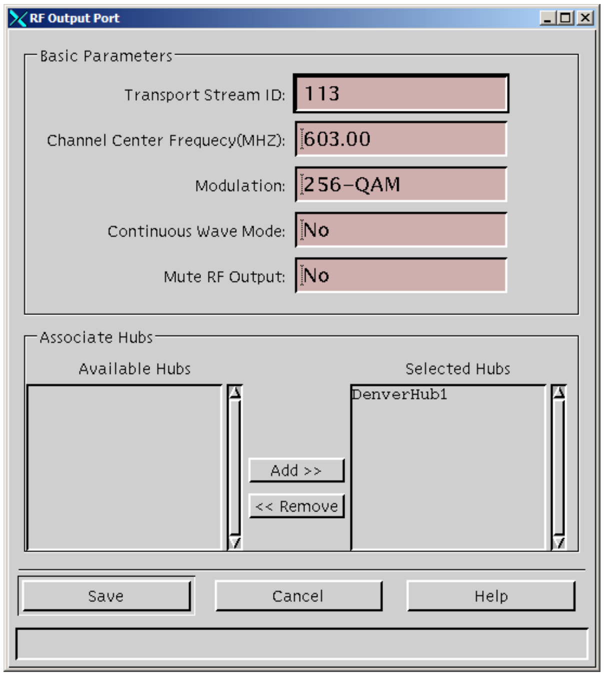
Ports

SA Reserved TSID Range: 0 – 65535

ASI INPUT 1 Transport Stream ID: 111   ASI INPUT 2 Transport Stream ID: 417

	Modulation	Transport Stream ID	Channel Center Frequency (MHz)	Continuous Wave Mode	Mute RF Output	Disabled	Interleaver Depth	Port To Hubs
RF OUT 1	56-QAM	113	603.00				128,4	Hubs
RF OUT 2	56-QAM	114	609.00				128,4	Hubs

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



RF Output Port

Basic Parameters

Transport Stream ID: 113

Channel Center Frequecy(MHZ): 603.00

Modulation: 256-QAM

Continuous Wave Mode: No

Mute RF Output: No

Associate Hubs

Available Hubs	Selected Hubs
	DenverHub1

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

To send data from this MQAM modulator 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 modulator.

If you want to send data from this MQAM modulator 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.

Chapter 2
New Optional Features

Overview

Introduction

SR 3.5 offers several new optional features, including Regional Control System (RCS), Direct ASI, 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 Services for more information.

In This Chapter

This chapter contains the following topics.

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 each remote site. 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.

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).

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 3.5.

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.

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:

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

Chapter 3
What Are the Site Requirements?

Overview

Introduction

This chapter provides information to help you prepare for the SR 3.5 upgrade. Please read this entire chapter before you install SR 3.5. This chapter includes important information to help you schedule the appropriate amount of time for the upgrade.

Application Testing

Application testing for SR 3.5 was completed using a sample of applications developed for SR 2.2. SR 3.5 did not affect the functionality of the applications tested.

In This Chapter

This chapter contains the following topics.

Hardware and Software Requirements

Introduction

This section provides the hardware and software requirements you must meet before upgrading your system to SR 3.5. You can check your system against these requirements by running the Doctor report.

Running the Doctor Report

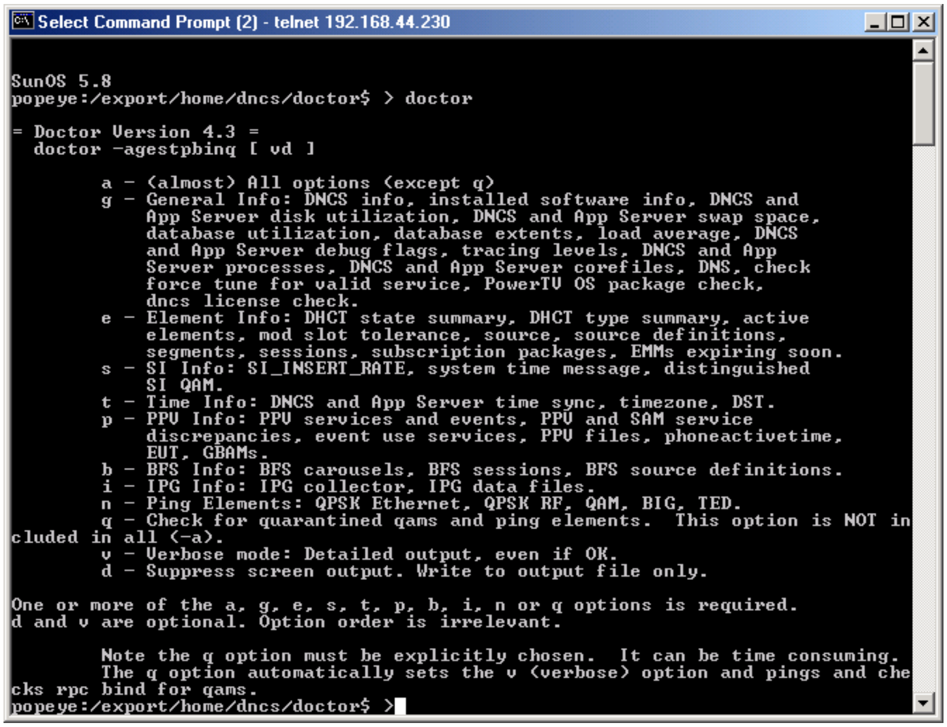
Use the following procedure to run the Doctor report on the DNCS.

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.



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

= Doctor Version 4.3 =
  doctor -agestpbinq [ 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, PowerTV OS package check,
            dncs 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 - PPV Info: PPV services and events, PPV and SAM service
            discrepancies, event use services, PPV 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.

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 3.5.

DNCS System Release

Your system must be running SR 2.2 at a minimum. 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 Requirements

Ensure your site meets the following DNCS hardware requirements before upgrading to SR 3.5.

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	• 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	• 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 3.5.

Note: If you are using another vendor's application server, contact the vendor to ensure the hardware and software compatibility with Cisco's SR 3.5.

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

Application Platform Release Dependencies

The following table shows the application platform release dependencies for SR 3.5.

Important: You must have these versions of application platform software *or later* installed on your system prior to upgrading to SR 3.5. If you do not install the correct application platform software *before* you upgrade to SR 3.5, 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)**	**PowerKEY (Minimum)**
8300 DVR 1.2.6a25g	6.8.9.4	1.85.17.3	3.7.5
8300 DVR 1.3.1a10	6.14.5	1.87.3.1	3.7.5
8000/8010 DVR 1.3.1a10	6.13.5	1.87.3.1	3.7.5
3250HD MR4 P1	3.12.8.1	1.57.8.1	3.7.5
2xxx, 31xx, 3200, 3100HD	3.10.9	1.54.23.1	1.0.6.20 (2000s), 1.0.7 (all others)
Pace	Pace to Provide OS Build	N/A	2.0.4.11
Pioneer	Pioneer to Provide OS Build	N/A	2.0.4.11

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 • 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.

Chapter 4
What CRs Are Included in SR 3.5?

Overview

Introduction

This chapter describes change requests (CRs) that were found in previous system releases and corrected in SR 3.5 to improve operational performance of the DNCS.

In This Chapter

This chapter contains the following topics.

Issues Corrected in SR 3.5: 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 3.5.

Quick Reference to Issues Corrected in SR 3.5

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

CR Number	Short Description of Fix
CR 36770	File names exceeding 100 characters are now supported in the dncsFilesBackup script
CR 38526-01	Size limitations for the SAM bulk table are managed effectively
CR 39857	EAS messages display at expected time intervals
CR 45626	Memory issues with Spectrum processes are corrected
CR 48759	Options -b and -s are implemented in the backupDatabase script

Want to Know More?

Overview

This section provides more detail about each fix in SR 3.5. The descriptions in this section are not intended to be comprehensive. If you have additional questions about a particular change request, contact Cisco Services.

File Names Greater Than 100 Characters in Length Now Supported in dncsFilesBackup Script

The DNCS key files consist of those files required to boot the DNCS. The script that backs up the DNCS key files is called **dncsFilesBackup**. Previously, if a DNCS key file name was greater than 100 characters, the dncsFilesBackup script was reporting an error. Although the script was reporting an error, the files were still backed up to tape.

To address this issue, reported in **CR 36770**, Cisco modified the dncsFilesBackup script to accept filenames greater than 100 characters in length.

Size Limitations for the SAM Bulk Table Are Managed Effectively

Each time you register a service with the SAM, the DNCS assigns the service a unique service ID and, in some cases, a new URL. These URLs are stored in the bulk.tbl file, which is located in the /dvs/dvsFiles/SAM directory. Previously, when the bulk.tbl size limitation of 65 KB was exceeded, a much smaller, incomplete bulk.tbl file was created by saManager. When set-tops downloaded this smaller, incomplete file from the BFS, the set-tops no longer received complete service information. As a result, set-tops displayed black screens and/or continuously rebooted.

To address this issue, reported in **CR 38526-01**, the DNCS code was updated to ensure a new SubTable is created anytime data threatens to push the size of bulk.tbl over 65 KB. In addition, a new 4-bit SubTable is created for extremely rare cases where the number of unique service IDs exceeds 65536.

Continued on next page

EAS Messages Display at Expected Time Intervals

By default, the DNCS resends EAS messages every 2 minutes, though you can reconfigure the resend timer using the MMM_CLEANUPSEC environment variable. The resend timer determines how often the DNCS resends an active EAS message to set-tops. Resends are necessary for recovery purposes and to ensure set-tops whose states have recently changed receive the message. Previously, when a new EAS message was sent, none of the resend timers for existing EAS messages were cancelled. Because multiple resend timers were active at the same time, the new EAS message was sent more frequently than necessary. Unpredictable timing issues with the EAS message are a result of the message being sent more frequently than necessary.

To address this timing issue, reported in **CR 39857**, all previous resend timers are now cancelled anytime a new EAS message is sent. When the new EAS message is sent, the only resend timer that is active is the timer for the current EAS message.

Memory Issues with Spectrum Processes Are Corrected

Customers reported that the SpectroSERVER and AlarmView processes associated with Spectrum were consuming upwards of 600 to 700 MB of resident memory each week. Customers had to regularly stop and restart the DNCS to thwart this aggressive memory growth.

To address these memory issues, reported in **CR 45626**, Cisco applied Aprisma’s patch P121 to customer systems. This patch corrected the AlarmView memory issue; however, SpectroSERVER continued to have memory issues. Aprisma issued a technical bulletin (TB0767-9) that indicated SpectroSERVER would leak under certain conditions. To correct the SpectroSERVER memory issue, Cisco followed the recommendations in this technical bulletin and changed the event_batch_max_size variable from 1 to 100.

Options -b and -s Are Implemented in the backupDatabase Script

The script that backs up the Informix database on the DNCS is called **backupDatabase**. You can run the backupDatabase script with a number of options, including the **-b** (block size) and **-s** (tape size) tape device options. Due to a discrepancy in what the script expected, you could not use the -b and -s options. Instead, a workaround had to be used for both options.

To address these issues, reported in **CR 48759**, Cisco modified the backupDatabase script to recognize the -b and -s options.

Chapter 5
Known Issues for Standard SR 3.5

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 3.5	5-2

Known Issues in the Standard Version of SR 3.5

Introduction

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

CR 27796: Image Files May Not Save Due to File Permissions Settings

The system allows the operator to copy image files with various permissions settings that do not satisfy the CVT user interface during the save operation. As an example, if the permissions of a software image file are set to 555 (read and execute for all users), you cannot save the image file from the Set Up Downloadable File window on the DNCS.

Workaround: When the Save fails to work, the Set Up Downloadable File window issues a “Save Failed” message. To determine if the save operation failed because of file permissions, you can check the dncsLog file for an “Unable to copy image” log message from osm.

To correct the file permissions, enter the following command. Replace <image> with the name of the image file that needs different permissions.

```
chmod 755 <image.name>
```

CR 27799: Quitting the Online Help Closes the Help and the DNCS Web-Based Interface

If you select **File** > **Quit** from the Help window for a Web-based UI, both the Help window and the Web-based UI close.

Workaround: To close the Help window only, select **File** > **Close** or click ☒ in the upper right corner of the Help window.

CR 28741: Files Are Not Automatically Moved to the Correct Carousel

If you add a file to a carousel as an inband file and then change the file to an OOB file, the file is not automatically moved to the OOB carousel. The same is true if you add a file to a carousel as an OOB file and then change the file to an inband file. The OOB file is not automatically moved to the inband carousel.

Workaround: Delete the file, and re-add the file to the correct carousel.

CR 31348: The Services Portal Cannot Be Disabled

Normally, if you set the access level for an application or feature to **None** from the Set Up User Access window, the button associated with the feature or application is disabled (greyed out). If you set the access level for Services Portal to **None**, the Services Portal button remains active on the Server Applications tab. Users can still open the SP Service Guide and edit the Services Portal.

CR 32103-03: "Reservation Only" PPV Events Display a Black Screen

For some sites, if you configure a pay-per-view (PPV) event as reservation only, subscribers see a black screen for the event. To resolve this issue, you must configure PPV events as both reservation PPV (RPPV) and impulse PPV (IPPV).

If you are experiencing this issue, contact Cisco Services for assistance.

CR 43063: If a Device Name Is in Use, You Must Close and Re-Open the User Interface Before Attempting to Enter a Unique Device Name

When you create a new device on the DNCS, such as a new QPSK, the system checks to ensure the name for the new device is not already used by an existing device. Device names must be unique to the entire system, not just unique to the device type.

If the device name is already in use, the system generates an error when you try to save the new device. If you try to create the device with a new name, the save fails again.

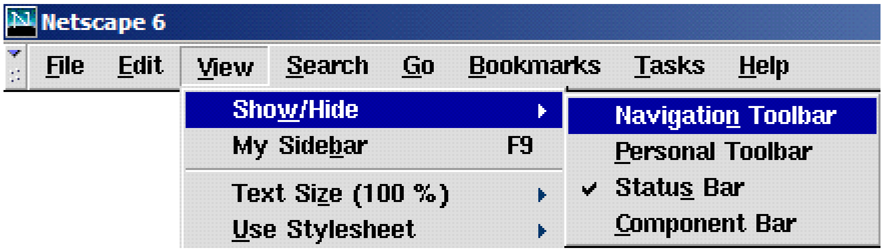
Workaround: In order to reverse this error condition, you must close and re-open the device user interface and then create the device with a unique name.

CR 44642: Use of Browser Navigation Buttons Creates Unexpected Results

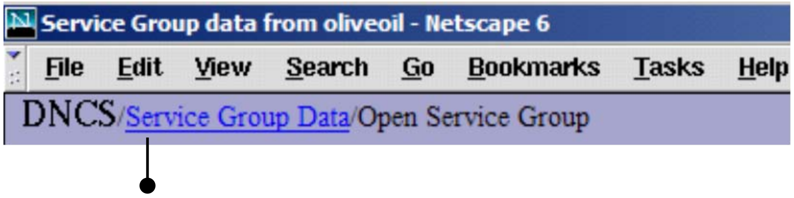
If you use Netscape buttons to navigate Web-based user interfaces, such as the Service Group interfaces, the results are not always consistent with typical Web page navigation. For example, clicking Back may not return both the navigation pane *and* the main window to the previous pane and window. The result is that the navigation and action choices on the left side of the screen do not match the window on the right side of the screen.

Note: The DNCS is migrating to a Web-based application, not simply Web pages. Therefore, it is preferable to use the navigation options provided within the application rather than navigating from the main browser window.

Workaround: Hide the Navigation Toolbar from Netscape as shown below. Not only does this hide the Back button, but it also adds valuable screen real estate for the Web-based UIs of the DNCS.



To go back to a previous screen in the Service Group Web interface, use the navigation path provided along the top of each Web-based UI. For example, to go back the Service Group Data window from the Open Service Group window, simply click the **Service Group Data** hyperlink at the top of the page.


Service Group data from oliveoil - Netscape 6
File
Edit
View
Search
Go
Bookmarks
Tasks
Help
DNCS/Service Group Data/Open Service Group

The hyperlink above provides the navigation path to the current window. You can go back to any window in the path by clicking the desired hyperlink.

CR 44947: Deleting Nested Packages Deletes a Segment with the Same Name as the Nested Package

If a nested package and a segment share the same name, both the nested package and the segment are removed from the parent package if you delete the nested package. As a result, you have to re-add the segment to the parent package.

Workaround: Do not give segments and nested packages the same name.

CR 46948: You Must Force the BRF to Regenerate to Ensure Set-Tops on New CMTS Bridges Receive OOB Data

The Bridge Resolution File (BRF) is not regenerated when you create a new CMTS bridge. As a result, set-tops on this new bridge do not receive OOB data.

Workaround: When you re-save a newly created CMTS bridge, the BRF is regenerated, and an entry for the bridge is added to the BRF. Complete the following steps to open and re-save a new CMTS bridge after you create it.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Element Provisioning** tab.
3. Click **QPSK/CMTS**.
4. From the QPSK/CMTS List window, select the CMTS associated with the new bridge.
5. Click **File** and select **Open**.
6. When the Set Up CMTS window opens, double-click the new bridge.
7. When the **Set Up CMTS Bridge** window opens, click **Save**.

CR 47869-01: You Cannot Select Input and Output Ports When Building MPEG Sources

Currently, you can define multiple output ports on a MPEG source and assign multiple ports to different MQAMs of GQAMs or the same MQAM or GQAM. However, when you build the source, the DNCS assumes you want to use the input TSID of the first port. You cannot select individual input ports to tell the MQAM or GQAM the appropriate input TSID to find PIDs. As a result, all sessions intended for port 1 build successfully, and all sessions on port 2 or other ports go into tabman, waiting for status on the MQAM or GQAM.

Workaround: Create a separate MPEG source for each port rather than creating multiple ports to the same source.

CR 48286: BFS Recovery Takes Longer than Expected

Rather than making the next session set up request as soon the current session set up succeeds, bfsServer waits for 30 seconds between making session setup requests. As a result, bfsServer may take a longer time to recover than expected.

CR 48495: Operators Must Define Split Channel Times Using the DNCS Time Zone

When you define the start and end times for split channel in the Set Up Split Channel window, you must enter times using the time zone of the DNCS. If you are configuring split channels for a hub in a different time zone, make sure to convert the times to display properly for the intended time zone.

Example: Your DNCS is on Eastern time, and you want to split a channel for a hub on Pacific time. To split a channel at 3:00 p.m. Pacific time, you would enter 6:00 p.m. as the start time in the Set Up Split Channel window.

CR 50600-03: The Session List May Load Slowly

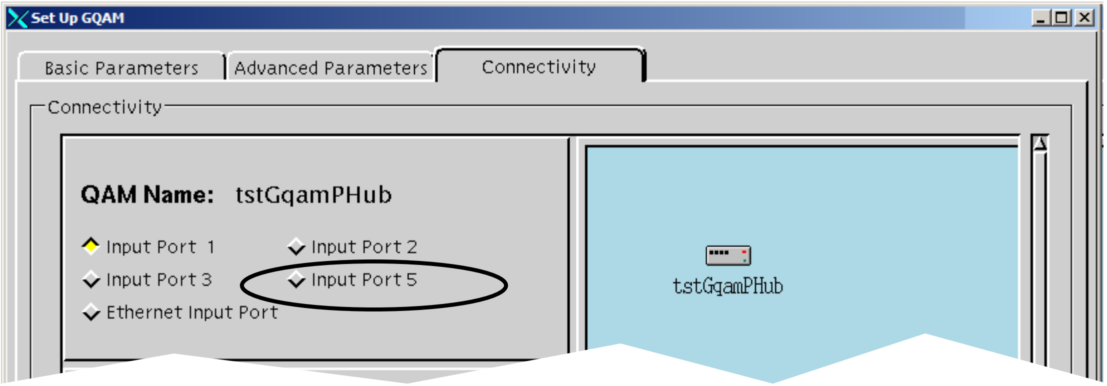
The more sessions you set up within a 24-hour period, the longer it takes for the Session List to load.

CR 51034: Split Channels On CableCARD Modules Transition Using DNCS Time Zone

CableCARD hosts with CableCARD modules transition between split channel services according to the time zone of the DNCS. However, set-tops on the same hub transition according to the hub’s time zone. Both CableCARD hosts and set-tops should transition between split channel services using the same time zone.

CR 51742-01: Port Label Is Incorrect on the Connectivity Tab for GQAMs

When configuring a GQAM, the Connectivity tab shows an incorrect label of “Input Port 5” for Input Port 4.



CR 51843: No Error Message Displays for Invalid Parent IDs

If you create a new service without assigning the service group to a valid parent ID, the system appears to accept the new service group upon saving. However, if you refresh or exit and re-open the Service Group user interface, the newly created service group does not appear. Throughout this process, no error message displays to warn you that the service group will not be saved without a valid parent ID.

CR 51853: Active BFS Sessions Among dsm, bfsServer, and the Database Are Not Synchronized

This CR describes a corner case. Typically, the active BFS sessions are always in sync. If you do experience problems with the BFS and find that the database table entries are out of sync with dsm and bfsServer, you can complete the following workaround to resolve the problem.

Workaround: Complete the following steps to correct synchronization issues with active BFS sessions.

1. Stop the bfsServer process.
2. Tear down all bfsSessions.
3. Run clearDbSessions –c.
4. Restart the bfsServer process.

CR 51927: Report Writer Does Not Display All Channels and Sources Correctly

Currently, the Report Writer does not display channels and sources for sessions going from Ethernet inputs to GQAMs.

CR 51974-01: When an Enabled BFS Admin Source Is Deleted, All BFS Sessions Are Torn Down

When you delete a source from the Sources tab of the BFS Administration window, the only sessions that should be torn down automatically are the session for the deleted source and any sessions numbered higher than the session for the deleted source. In addition, if the deletion for the source fails, no sessions should be torn down.

Currently, *all* BFS sessions are torn down when you delete sources from BFS Administration, even if the deletion of the source fails.

CR 52230-01: Existing OSM Images Are Not Populated Correctly

Currently, an OSM image audit at startup does not work if the BFS server is not available.

CR 52465-01: EAM Audio File Is Not Deleted from BFS

If the MMMServer process restarts during an active Emergency Alert Message (EAM), the aiff audio file for the EAM is not deleted from BFS after the EAM expires.

CR 52603-01: MMMServer May Not Recover and Register with BFS

Correct operation requires you to delete *both* the MMMAud and MMMCfg servers at the same time before stopping the MMMServer process. When you do this, both servers rebuild correctly when you restart the MMMServer process. If you delete only the MMMAud server (leave the MMMCfg server as is), then the following error conditions occur when you restart the MMMServer process:

- The MMMAud server does not rebuild.
- The MMMServer process does not recover and register with BFS. Instead, the following message appears multiple times in the dncsLog:

  ...MMMBfs::_registerServer(): BFS Error registering with BFS
- You cannot successful send an EAS message with both text and audio content. The user interface disappears without processing the message.

Workaround: Currently, if you want avoid these error conditions, you must delete *both* the MMMAud and MMMCfg servers from the Broadcast File Server List *before* you stop and restart the MMMServer process. If you have already experienced the error conditions previously detailed, complete the following workaround to correct the error conditions.

1. From the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Client**.
3. From the Broadcast File Server List, select the MMMCfg server.
4. Click **File** and choose **Delete**.
5. Stop and restart the MMMServer process again.

   Result: The MMMServer process registers *both* the MMMAud server and the MMMCfg server with the BFS.

CR 52833-03: Encrypted Service Content May Go in the Clear Due to sgManager Refresh Cache

This CR describes a corner case. Intermittently, the sgManager sends out a refresh cache to the drm that causes a mismatch between the drm and dsm. This mismatch results in segment information not being sent to the bsm; therefore, the content could go out in the clear.

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

CR 53495: System Information Is Not Being Sent in the In Band Stream

Upon recovery of siManager, the SI inserts are not cleared on the distinguished QAM.

CR 53552: RPC Error Messages Received When Using QAM User Interface or auditQam Utility to Reset QAMs

When using the QAM user interface or the auditQam utility to reset a QAM device, you will receive an RPC error message. However, the QAM device will eventually receive the reset command.

Chapter 6
Known Issues for Optional Features

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

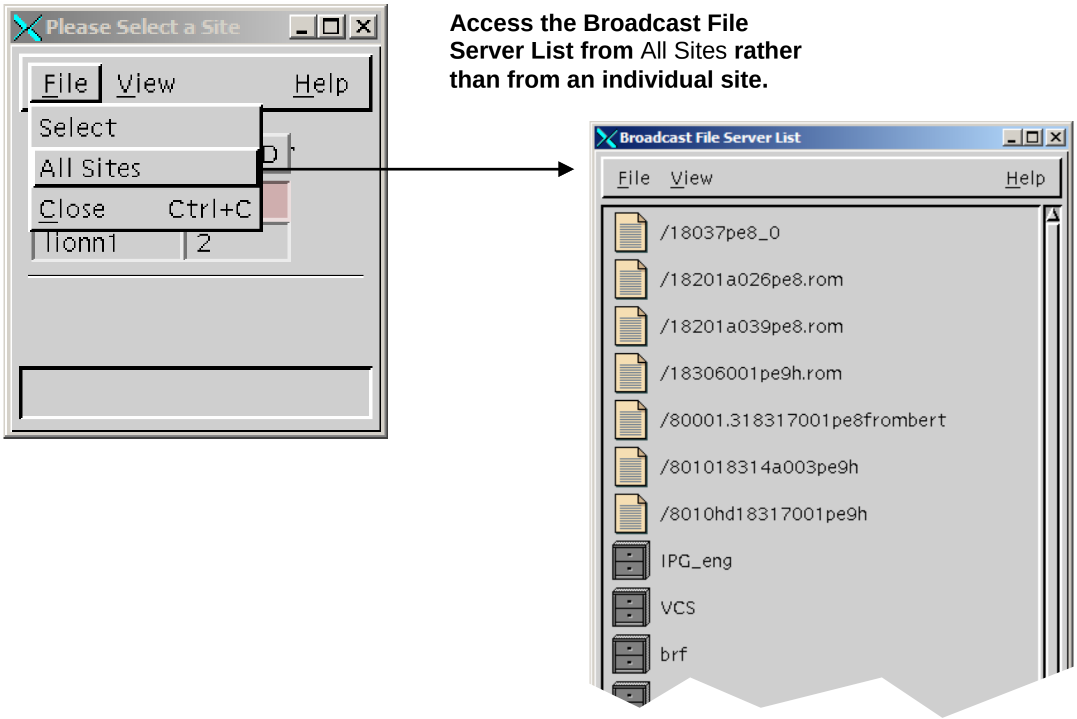
This chapter contains the following topics.

Known Issues for RCS in SR 3.5

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.



Access the Broadcast File Server List from All Sites **rather than from an individual site.**

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.

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: dncs_host Alias Added To /etc/host Files For RNCS and Object Carousel

The ntp.conf file uses the dncs_host alias for its server. The dncs_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.

bfsServer Will Not Go Active When a QAM Is Not Directly Connected to the DNCS

Some sites do not have headend equipment directly connected to the DNCS. If this scenario is in place, then all QAMs and QPSKs must be routed through a LIONN first.

Workaround: To enable this scenario, connect a QAM directly to the DNCS and allow the local BFS Sessions to go active. Once the BFS Sessions go active, you can remove and disable the QAM, then disable the sources for the DNCS. (Do not disable the sources for the RNCS.)

Chapter 7
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.

Appendix A
What's Installed with SR 3.5?

Overview

Introduction

This appendix provides a table of the versions of software that will be installed after you upgrade to SR 3.5.

Important: This appendix provides versions for software installed with the base SR 3.5 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.

A Snapshot of Your System Post-Upgrade

Post-Upgrade Version Information

The following table lists the software versions that are installed with base SR 3.5. 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	3.5.0.25
GUI	3.5.0.25
WUI	3.5.0.25
DNCS Application Patch	3.5.0.25p4
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	2.1.11
Backup/Restore CD	6.0.6
Unipack Install Scripts	1.3.0.11
DBDS Utilities	5.1.1
DNCS Utilities	5.1.0.3
Cool Tool (CT) Utilities	5.1.0.0
DHCT Status	5.1.0.0
Doctor	5.1.0.3
Spectrum Installation	3.5.0.0
Spectrum Enterprise Manager App Version	5.0 R1
Spectrum Supplement App.	CS3/MMS3 P122

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
Application Server	
Application Server	3.1.5.3
Application Server Support Software	
DNCS/App Server Tools	3.5.0.7
BFS Remote	3.2.0.5AS
MQAM	
Application	2.5.0a
Boot	1.2.2
QAM	
Application	2.3.5
GQAM	
GQAM	1.1.2
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. 678 277-1120
5030 Sugarloaf Parkway, Box 465447 800 722-2009
Lawrenceville, GA 30042 www.cisco.com

April 2012 Printed in USA Part Number 4001159 Rev B