# Welcome to the DNCS Help

The DNCS Help provides the help information you need to use the DNCS. The Help contains the following:

- Overview information
- Conceptual information
- Reference information
- Instructions for completing tasks



## What do you want to do?

- Learn What's New In This Release?
- Learn About This Version of Help
- Learn about Additional Support and Resources
- View Help for New Users

# What's New In This Release?

This version of DNCS Online Help supports the following System Release (SR) 4.3.1. The new standard features that these releases offer are described below.

For information on the optional and specially licensed features these releases provide, contact your customer representative.

# Roll-Up for Emergency Patches

This release contains all of the emergency patches that were released for SR 2.8/3.8/4.3. These patches include:

- 4.3.0.14p5ep2 siManager deadlock between two threads
- 4.3.0.14p5ep3:
  - siManager memory leaks
  - siManager intermittent in sending information
  - qamManager running high on CPU due to audits between qamManager and QAMs
- 4.3.0.14p5ep6 emmDistributor remove noise level debug from "DE" level
- 4.3.0.14p5ep7 siManager fix for ADSG configuration
- 4.3.0.14p5ep9 Certain set-tops expect the UDP port in the UNCC to be 13818.
- 4.3.0.14p5ep10 Scripts to update the svc_group_rsr and the max bandwidth.
- 4.3.0.14p5ep11:
  - Delay in response by xDQA causes qamManager to audit xDQA twice.
  - qamManager needs to report information back to auditQAM
  - qamManager can core auditing generic QAMs.
  - qamManager failed to update disabled ports on xDQA or generic QAM.
- 4.3.0.14p5ep12 bsm connection logic to siManager retries too many times and incorrectly.
- 4.3.0.14p5ep15 When changing out a QAM with one that has already been provisioned, it does not update new information.
- 4.3.0.14p5ep16 EAS force tune/crawl for DTA systems - mmmServer change only.
- 4.3.0.14p5ep17:
  - siManager does not honor hidden channel number for nonSA sources.
  - Guide is missing the majority of the "Channel Call Letters".

# Proxy for Web Services Interface

A new service, loadDhctServer, provides an interface to the DNCS using a SOAP/XML web service.

# BFS QAM Frequency Changes

A new procedure for changing the output frequency for a BFS QAM has been added. See Change the BFS QAM Output Frequency for more information.

# Report Writer Updates

The Report Writer has gone through several updates. These include:

- The Channels, Sources, and Sessions report now supports SDV sources (multicast sessions built on Netcrypt).
- The Channels, Sources, and Sessions report now includes several new columns. These include:
  - Bandwidth
  - Headend Name
  - Hub Name
  - QAM Name
  - QAM MAC

For more information, see Reports.

## DNCS Security

A new section concerning DNCS security has been added. This section details adding and removing user accounts from the DNCS and password management. See DNCS Security for more information.

# About This Version of Help

DNCS Online Help version 4.3.1.1 supports System Release 4.3.1. For details about this version of DNCS Online Help, see the following topics:

- Help version and copyright information for this help document
- Terms and conditions for use of this version of DNCS Online Help
- Trademarks used in this version of DNCS Online Help

## Help Version and Copyright

DNCS Online Help Version 4.3.1.1 (PC)
March 2010

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



## Terms and Conditions

Following are the terms and conditions to which you agree by using the DNCS Help System.

**WARNING:**

**This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.**

## Acknowledgements

I understand that the information and materials provided in this DNCS Online Help System (the "System") by Scientific-Atlanta, LLC (hereafter "Cisco"), a wholly owned subsidiary of Cisco Systems, Inc. may not always be completely accurate and up-to-date. I agree to use the information provided in the System solely for the purpose of operating my company's Digital Network Control System and for no other purposes.

## Disclaimer

THE SYSTEM IS PROVIDED, "AS IS, WHERE IS, WITH ALL FAULTS." THERE ARE NO WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE SYSTEM OR ANY OF THE INFORMATION PROVIDED THEREIN, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CISCO ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS THAT MAY APPEAR IN THE SYSTEM. CISCO DOES NOT WARRANT THAT THE FUNCTIONS DESCRIBED IN THE SYSTEM WILL MEET THE USER'S REQUIREMENTS OR THAT THE OPERATION OF ANY EQUIPMENT PURSUANT TO THE GUIDELINES SET FORTH IN THE SYSTEM WILL BE UNINTERRUPTED OR ERROR-FREE. CISCO MAKES NO WARRANTY OF

NON-INFRINGEMENT, EXPRESSED OR IMPLIED. THE USER OF THE SYSTEM ACKNOWLEDGES ITS RESPONSIBILITY TO USE ALL REASONABLE METHODS TO PROVE OUT AND THOROUGHLY TEST THE OPERATION OF THE DNCS AND ALL OUTPUTS FROM THE DNCS PRIOR TO ITS USE IN THE USER'S OPERATIONS.

## Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL CISCO OR ITS SUBSIDIARIES BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, LOSS OF PROFITS, EXEMPLARY OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OF, OR INABILITY TO USE, THE SYSTEM OR USE OF ANY INFORMATION OR CONTENT INCLUDED IN THE SYSTEM. THIS LIMITATION APPLIES WHETHER THE ALLEGED LIABILITY IS BASED ON CONTRACT, TORT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER BASIS, REGARDLESS OF THE CAUSE OF SUCH DAMAGE AND EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Indemnification

Upon a request by Cisco, you, on behalf of your company, agree to defend, indemnify, and hold harmless Cisco and its subsidiaries and other affiliated companies, and their employees, contractors, officers, and directors from all liabilities, claims, and expenses, including attorneys' fees, that arise from your use or misuse of the System.

## Other Terms

Cisco reserves the right to change the System at any time without notice. The System 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 the System employs an invention claimed in any existing or later issued patent.

The information contained in the System is confidential and proprietary information intended for the use of authorized licensee's of the Cisco DNCS only. If you are not an authorized licensee of the Cisco DNCS, you are hereby notified that any disclosure, use, copying or the taking of any action in reliance on the information provided in the System is strictly prohibited. Information in the System is subject to change without notice. No part of the System may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco.

## Trademarks

The following list provides trademark information for products mentioned in this Help system:

- Cisco, Cisco Systems, the Cisco logo, the Cisco Systems logo, AllTouch, Continuum DVP, Explorer, Overlay, PowerKEY, and PowerTV are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- CableLabs and DOCSIS are registered trademarks of Cable Television Laboratories, Inc.
- CableCARD, M-Card, OpenCable, OCAP, and tru2way are trademarks of Cable Television Laboratories, Inc.
- HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.
- Macrovision is a registered trademark of Macrovision Corp.
- MoCA is a trademark of the Multimedia over Coax Alliance.
- All other trademarks mentioned in this document are the property of their respective owners.

## 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

## Help Version and Copyright

DNCS Online Help Version 4.3.1.1 (PC)
March 2010

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

## Terms and Conditions

Following are the terms and conditions to which you agree by using the DNCS Help System.

**WARNING:**

**This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.**

## Acknowledgements

I understand that the information and materials provided in this DNCS Online Help System (the "System") by Scientific-Atlanta, LLC (hereafter "Cisco"), a wholly owned subsidiary of Cisco Systems, Inc. may not always be completely accurate and up-to-date. I agree to use the information provided in the System solely for the purpose of operating my company's Digital Network Control System and for no other purposes.

## Disclaimer

THE SYSTEM IS PROVIDED, "AS IS, WHERE IS, WITH ALL FAULTS." THERE ARE NO WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE SYSTEM OR ANY OF THE INFORMATION PROVIDED THEREIN, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CISCO ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS THAT MAY APPEAR IN THE SYSTEM. CISCO DOES NOT WARRANT THAT THE FUNCTIONS DESCRIBED IN THE SYSTEM WILL MEET THE USER'S REQUIREMENTS OR THAT THE OPERATION OF ANY EQUIPMENT PURSUANT TO THE GUIDELINES SET FORTH IN THE SYSTEM WILL BE UNINTERRUPTED OR ERROR-FREE. CISCO MAKES NO WARRANTY OF NON-INFRINGEMENT, EXPRESSED OR IMPLIED. THE USER OF THE SYSTEM ACKNOWLEDGES ITS RESPONSIBILITY TO USE ALL REASONABLE METHODS TO PROVE OUT AND THOROUGHLY TEST THE OPERATION OF THE DNCS AND ALL OUTPUTS FROM THE DNCS PRIOR TO ITS USE IN THE USER'S OPERATIONS.

## Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL CISCO OR ITS SUBSIDIARIES BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, LOSS OF PROFITS, EXEMPLARY OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OF, OR INABILITY TO USE, THE SYSTEM OR USE OF ANY INFORMATION OR CONTENT INCLUDED IN THE SYSTEM. THIS LIMITATION APPLIES WHETHER THE ALLEGED LIABILITY IS BASED ON CONTRACT, TORT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER BASIS, REGARDLESS OF THE CAUSE OF SUCH DAMAGE AND EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Indemnification

Upon a request by Cisco, you, on behalf of your company, agree to defend, indemnify, and hold harmless Cisco and its subsidiaries and other affiliated companies, and their employees, contractors, officers, and directors from all liabilities, claims, and expenses, including attorneys' fees, that arise from your use or misuse of the System.

## Other Terms

Cisco reserves the right to change the System at any time without notice. The System 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 the System employs an invention claimed in any existing or later issued patent.

The information contained in the System is confidential and proprietary information intended for the use of authorized licensee's of the Cisco DNCS only. If you are not an authorized licensee of the Cisco DNCS, you are hereby notified that any disclosure, use, copying or the taking of any action in reliance on the information provided in the System is strictly prohibited. Information in the System is subject to change without notice. No part of the

## Trademarks

The following list provides trademark information for products mentioned in this Help system:

- Cisco, Cisco Systems, the Cisco logo, the Cisco Systems logo, AllTouch, Continuum DVP, Explorer, Overlay, PowerKEY, and PowerTV are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- CableLabs and DOCSIS are registered trademarks of Cable Television Laboratories, Inc.
- CableCARD, M-Card, OpenCable, OCAP, and tru2way are trademarks of Cable Television Laboratories, Inc.
- HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.
- Macrovision is a registered trademark of Macrovision Corp.
- MoCA is a trademark of the Multimedia over Coax Alliance.
- All other trademarks mentioned in this document are the property of their respective owners.

## 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.

# About This Version of Help

DNCS Online Help version 4.3.1.1 supports System Release 4.3.1. For details about this version of DNCS Online Help, see the following topics:

- Help version and copyright information for this help document
- Terms and conditions for use of this version of DNCS Online Help
- Trademarks used in this version of DNCS Online Help

## Help Version and Copyright

DNCS Online Help Version 4.3.1.1 (PC)
March 2010

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



## Terms and Conditions

Following are the terms and conditions to which you agree by using the DNCS Help System.

**WARNING:**

**This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.**

## Acknowledgements

I understand that the information and materials provided in this DNCS Online Help System (the "System") by Scientific-Atlanta, LLC (hereafter "Cisco"), a wholly owned subsidiary of Cisco Systems, Inc. may not always be completely accurate and up-to-date. I agree to use the information provided in the System solely for the purpose of operating my company's Digital Network Control System and for no other purposes.

## Disclaimer

THE SYSTEM IS PROVIDED, "AS IS, WHERE IS, WITH ALL FAULTS." THERE ARE NO WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE SYSTEM OR ANY OF THE INFORMATION PROVIDED THEREIN, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CISCO ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS THAT MAY APPEAR IN THE SYSTEM. CISCO DOES NOT WARRANT THAT THE FUNCTIONS DESCRIBED IN THE SYSTEM WILL MEET THE USER'S REQUIREMENTS OR THAT THE OPERATION OF ANY EQUIPMENT PURSUANT TO THE GUIDELINES SET FORTH IN THE SYSTEM WILL BE UNINTERRUPTED OR ERROR-FREE. CISCO MAKES NO

WARRANTY OF NON-INFRINGEMENT, EXPRESSED OR IMPLIED. THE USER OF THE SYSTEM ACKNOWLEDGES ITS RESPONSIBILITY TO USE ALL REASONABLE METHODS TO PROVE OUT AND THOROUGHLY TEST THE OPERATION OF THE DNCS AND ALL OUTPUTS FROM THE DNCS PRIOR TO ITS USE IN THE USER'S OPERATIONS.

## Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL CISCO OR ITS SUBSIDIARIES BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, LOSS OF PROFITS, EXEMPLARY OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OF, OR INABILITY TO USE, THE SYSTEM OR USE OF ANY INFORMATION OR CONTENT INCLUDED IN THE SYSTEM. THIS LIMITATION APPLIES WHETHER THE ALLEGED LIABILITY IS BASED ON CONTRACT, TORT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER BASIS, REGARDLESS OF THE CAUSE OF SUCH DAMAGE AND EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Indemnification

Upon a request by Cisco, you, on behalf of your company, agree to defend, indemnify, and hold harmless Cisco and its subsidiaries and other affiliated companies, and their employees, contractors, officers, and directors from all liabilities, claims, and expenses, including attorneys' fees, that arise from your use or misuse of the System.

## Other Terms

Cisco reserves the right to change the System at any time without notice. The System 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 the System employs an invention claimed in any existing or later issued patent.

The information contained in the System is confidential and proprietary information intended for the use of authorized licensee's of the Cisco DNCS only. If you are not an authorized licensee of the Cisco DNCS, you are hereby notified that any disclosure, use, copying or the taking of any action in reliance on the information provided in the System is strictly prohibited. Information in the System is subject to change without notice. No part of the System may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco.

## Trademarks

The following list provides trademark information for products mentioned in this Help system:

- Cisco, Cisco Systems, the Cisco logo, the Cisco Systems logo, AllTouch, Continuum DVP, Explorer, Overlay, PowerKEY, and PowerTV are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- CableLabs and DOCSIS are registered trademarks of Cable Television Laboratories, Inc.
- CableCARD, M-Card, OpenCable, OCAP, and tru2way are trademarks of Cable Television Laboratories, Inc.
- HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.
- Macrovision is a registered trademark of Macrovision Corp.
- MoCA is a trademark of the Multimedia over Coax Alliance.
- All other trademarks mentioned in this document are the property of their respective owners.

## 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

# Additional Support and Resources

The following additional resources are also available to help you:

- Technical support from our service engineers or customer service representatives
- Printed resources which can be ordered or viewed from the Internet

## Contact Us

## If You Have Questions

If you have questions about this product, contact the representative who handles your account for information.

If you have technical questions, telephone your nearest technical support office at one of the following telephone numbers.

| | | |
|---|---|---|
| **The Americas** | | |
| United States | Cisco® Services<br>Atlanta, Georgia | **Technical Support**<br>▪For Digital Broadband Delivery System products only, call:<br>•Toll-free: 1-866-787-3866<br>•Local: 770-236-2200<br>•Fax: 770-236-2488<br>▪For all products other than Digital Broadband Delivery System, call:<br>•Toll-free: 1-800-722-2009<br>•Local: 678-277-1120<br>•Fax: 770-236-2306<br>**Customer Service**<br>▪Toll-free: 1-800-722-2009<br>▪Local: 678-277-1120<br>▪Fax: 770-236-5477 |
| **The United Kingdom and Europe** | | |
| Europe | European Technical Assistance Center (EuTAC), Belgium | **Product Information**<br>▪Telephone: 32-56-445-444<br>**Technical Support**<br>▪Telephone: 32-56-445-197 or 32-56-445-155<br>▪Fax: 32-56-445-061 |
| **Asia-Pacific** | | |
| China | Hong Kong | **Technical Support**<br>Telephone: 011-852-2588-4745<br>Fax: 011-852-2588-3139 |
| **Australia** | | |
| Australia | Sydney | **Technical Support** |

| | | |
|---|---|---|
| | | Telephone: 011-61-2-8446-5374<br>Fax: 011-61-2-8446-8015 |
| **Japan** | | |
| Japan | Tokyo | **Technical Support**<br>Telephone: 011-81-3-5322-2067<br>Fax: 011-81-3-5322-1311 |

## Additional Information

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.

### Related Topics

- Help for New Users
- About This Version of Help

# Additional Support and Resources

The following additional resources are also available to help you:

- Technical support from our service engineers or customer service representatives
- Printed resources which can be ordered or viewed from the Internet

## Contact Us

## If You Have Questions

If you have questions about this product, contact the representative who handles your account for information.

If you have technical questions, telephone your nearest technical support office at one of the following telephone numbers.

| | | |
|---|---|---|
| **The Americas** | | |
| United States | Cisco® Services<br>Atlanta, Georgia | **Technical Support**<br>▪For Digital Broadband Delivery System products only, call:<br>•Toll-free: 1-866-787-3866<br>•Local: 770-236-2200<br>•Fax: 770-236-2488<br>▪For all products other than Digital Broadband Delivery System, call:<br>•Toll-free: 1-800-722-2009<br>•Local: 678-277-1120<br>•Fax: 770-236-2306<br>**Customer Service**<br>▪Toll-free: 1-800-722-2009<br>▪Local: 678-277-1120<br>▪Fax: 770-236-5477 |
| **The United Kingdom and Europe** | | |
| Europe | European Technical Assistance Center (EuTAC), Belgium | **Product Information**<br>▪Telephone: 32-56-445-444<br>**Technical Support**<br>▪Telephone: 32-56-445-197 or 32-56-445-155<br>▪Fax: 32-56-445-061 |
| **Asia-Pacific** | | |
| China | Hong Kong | **Technical Support**<br>Telephone: 011-852-2588-4745<br>Fax: 011-852-2588-3139 |
| **Australia** | | |

| | | |
|---|---|---|
| Australia | Sydney | **Technical Support**<br>Telephone: 011-61-2-8446-5374<br>Fax: 011-61-2-8446-8015 |
| **Japan** | | |
| Japan | Tokyo | **Technical Support**<br>Telephone: 011-81-3-5322-2067<br>Fax: 011-81-3-5322-1311 |

## Additional Information

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.

### Related Topics

- Help for New Users
- About This Version of Help

## Printed Resources

Visit our website (https://www.sciatl.com/subscriberextranet/techpubs) to view additional publications about our products.

You need a user name and password to access this website. If you do not have a user name and password, go to https://www.scientificatlanta.com/dsnexplorer/register.htm to complete and submit a registration form.

**Note:** You may need to install a PDF reader, such as Adobe Acrobat Reader, on your system to view these publications.

### Related Topics

- Help for New Users
- About This Version of Help

# Network Overview

## Introduction

This section provides an overview of how you can use the DNCS Administrative Console to view the network status and manage the network.

## What do you want to do?

- View Network Status
- Manage the Network

# View Network Status

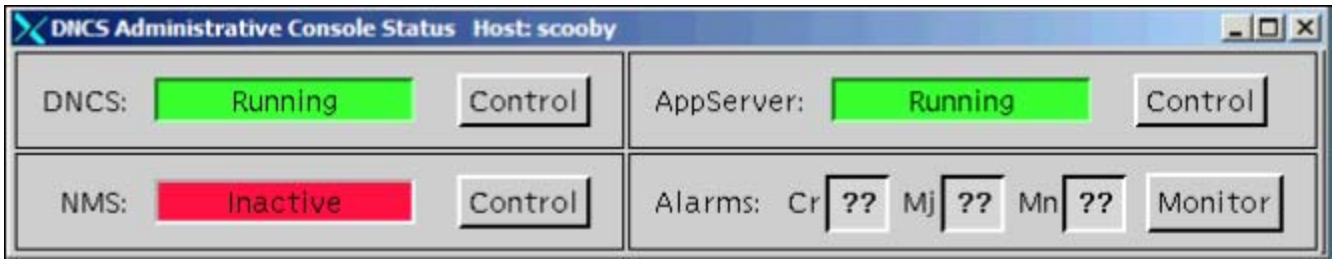
## DNCS Administrative Console Status

The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.


For more information, click on a specific section name in the following list.

- DNCS section
- AppServer section

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console window also displays the **NMS** and **Alarms** sections.




- The **NMS** section indicates whether or not the Spectrum NMS software is in operation.
- The **Alarms** section indicates the number of critical, major, and minor alarm conditions, if any, which are present in the DBDS as reported by the Spectrum NMS.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Status

The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- **Running** the DNCS software package is present and in operation
- **Inactive** the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

## Application Server Status

The **AppServer** section of the Administrative Console Status window indicates whether or not the Application Server is in operation based on the following conditions:

- **Running** the Application Server software package is present and in operation
- **Inactive** the Application Server software package is present, but not in operation
- **Not Responding** the Application Server does not respond when the DNCS tries to communicate with it
- **Not Installed** a Application Server host is defined in the host table, but the Application Server software package is not present; this usually indicates that you are not using our Application Server, but the application server of another vendor
- **Blank** no Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using our Application Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the Application Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major Application Server processes.

**WARNING:**

**Do NOT attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.**

The Application Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server (DHCT Configuration Server**) Generates the files containing the global, hub-specific, and staging configuration values and places the files on the broadcast server.
- **IPGServer - language supported (Interactive Program Guide Server)** Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, and Japanese.

  **Note:** Each language that is supported has its own application. For example, if English is supported, the application would be listed as **IPGServer- eng**.

- **ppvfileserver (Pay-per-view File Server)** Generates PPV files and places those files on the Broadcast File Server.
- **ppvServer (Pay-per-view Server)** Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.
- **vcServer (Virtual Channel Server)** Places the files for all configured virtual channels on the Broadcast File Server.
- **bfsRouter (Broadcast File Server Router)** For a Regional Control System (RCS), routes BFS Application Program Interface (API) calls from the SARA Server, such as IPG, PPV, or VCS, to the BFS on the DNCS at the central RCS site. The BFS Server on the central RCS site is site-aware. The BFS router converts any non-site BFS calls to site-specific calls and passes them along to the BFS server. This includes calls from Application Server processes, such as IPG, PPV, VCS, and any other third-party applications using the BFS API.

For more information on the SARA Server, refer to the SARA Application Server 3.4.1 User Guide (part number 4012159). See Printed Resources for information on obtaining documentation.

### Related Topics

- Manage the Network
- Network Setup Overview

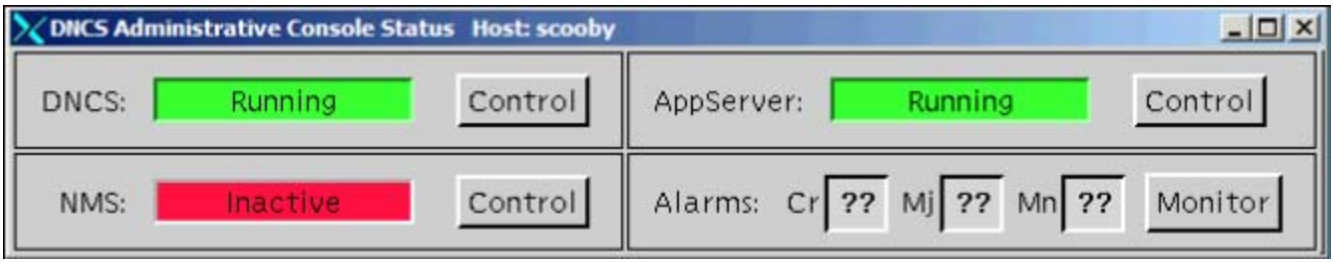
## DNCS Administrative Console Status

The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.


For more information, click on a specific section name in the following list.

- DNCS section
- AppServer section

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console window also displays the **NMS** and **Alarms** sections.




- The **NMS** section indicates whether or not the Spectrum NMS software is in operation.
- The **Alarms** section indicates the number of critical, major, and minor alarm conditions, if any, which are present in the DBDS as reported by the Spectrum NMS.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Status

The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- **Running** — the DNCS software package is present and in operation
- **Inactive** — the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

## Application Server Status

The **AppServer** section of the Administrative Console Status window indicates whether or not the Application Server is in operation based on the following conditions:

- **Running** — the Application Server software package is present and in operation
- **Inactive** — the Application Server software package is present, but not in operation
- **Not Responding** — the Application Server does not respond when the DNCS tries to communicate with it
- **Not Installed** — a Application Server host is defined in the host table, but the Application Server software package is not present; this usually indicates that you are not using our Application Server, but the application server of another vendor
- **Blank** — no Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using our Application Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the Application Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major Application Server processes.

**WARNING:**

**Do NOT attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.**

The Application Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server (DHCT Configuration Server**) — Generates the files containing the global, hub-specific, and staging configuration values and places the files on the broadcast server.
- **IPGServer - language supported (Interactive Program Guide Server)** — Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, and Japanese.

  **Note:** Each language that is supported has its own application. For example, if English is supported, the application would be listed as **IPGServer- eng**.

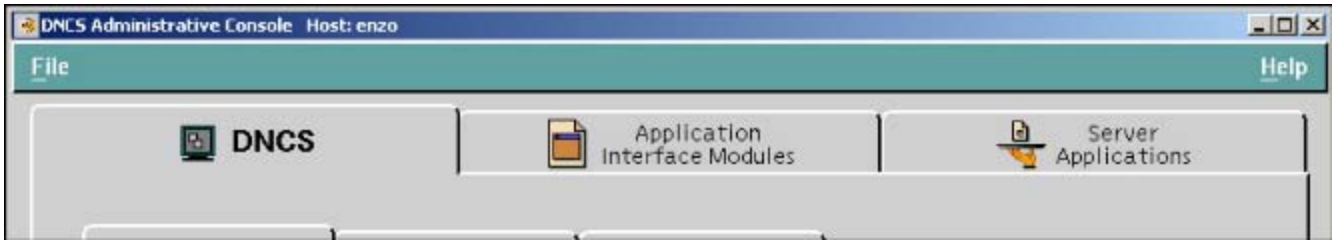
- **ppvfileserver (Pay-per-view File Server)** — Generates PPV files and places those files on the Broadcast File Server.
- **ppvServer (Pay-per-view Server)** — Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.
- **vcServer (Virtual Channel Server)** — Places the files for all configured virtual channels on the Broadcast File Server.
- **bfsRouter (Broadcast File Server Router)** — For a Regional Control System (RCS), routes BFS Application Program Interface (API) calls from the SARA Server, such as IPG, PPV, or VCS, to the BFS on the DNCS at the central RCS site. The BFS Server on the central RCS site is site-aware. The BFS router converts any non-site BFS calls to site-specific calls and passes them along to the BFS server. This includes calls from Application Server processes, such as IPG, PPV, VCS, and any other third-party applications using the BFS API.

For more information on the SARA Server, refer to the SARA Application Server 3.4.1 User Guide (part number 4012159). See Printed Resources for information on obtaining documentation.

# Manage the Network

## DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.




For more information, click on a specific tab name in the following list.

- DNCS tab
- Application Interface Modules tab
- Server Applications tab

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console Status window also displays the Network Management tab.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Tab

The **DNCS** tab on the DNCS Administrative Console provides access to certain functions that DNCS software directly controls. These functions are separated into sub-tabs:

- System Provisioning
- Network Element Provisioning
- Home Element Provisioning
- Utilities

### System Provisioning Sub-Tab

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **System Provisioning** sub-tab on the DNCS tab is divided into four functional sections:

- Service Provisioning
- RF Spectrum Management
- System Management
- EAS message

### Service Provisioning

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **Service Provisioning** section of the System Provisioning sub-tab has three buttons that allow you to set up

aspects of different kinds of services as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| Source | ▪Add, modify, or delete analog and digital service sources<br>▪Encrypt or un-encrypt service sources<br>▪Add, modify, or delete analog and digital service source definitions<br>▪Add, modify, or delete segments for individual sources<br>▪View segments of all sources |
| Package | ▪Add, modify, or delete service packages<br>▪Create packages within packages |
| ATM PVC | ▪Add, modify, or delete ATM PVC maps |

### RF Spectrum Management

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **RF Spectrum Management** section of the System Provisioning sub-tab contains the Bandwidth Allocation button, which allows you to perform the following tasks:

- ▪Add, modify, or delete upper and lower frequency allocations for various service types (analog, digital, and so forth)
- ▪View QPSK modulator/demodulator frequency allocations
- ▪View QAM sessions, frequency allocations, and transport stream IDs

### System Management

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **System Management** section of the System Provisioning sub-tab has four buttons that allow you to manage various aspects of the DBDS as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| DNCS System | ▪Set up DHCT session signalling parameters<br>▪Set up Network session signalling parameters<br>▪Establish the system channel plan: STD, HRC, or IRC<br>▪Establish whether or not the system is compliant with Open Cable standards |
| UN-Config | ▪Initiate UN-Config for a single DHCT<br>▪Initiate UN-Config for a DHCT type<br>▪Reboot a single DHCT<br>**Note:** For assistance in using this feature, refer to Downloading New Client Application Platform Installation Instructions (part number 4003052). To obtain a copy of this document, see Printed Resources. |
| User Access | Add, modify, or delete users with differing levels of access to the DNCS. |

| | |
|---|---|
| | **Note:** For assistance in using this feature, refer to Guidelines for System Security Passwords (part number 738188). To obtain a copy of this document, see Printed Resources. |
| DHCT Mgr | ▪Establish the DHCT registration mode: Administrative Gateway or Open<br>▪Establish the method by which IP addresses are assigned to DHCTs: Dynamic, Override, or Static<br>▪Establish how often UN-Config messages are sent to DHCTs in the system<br>**Note:** For assistance in using this feature, refer to Explorer Digital Home Communications Terminal Staging Guide (part number 734375) or Separable Security Host Staging Guide for System Release 4.2.1 and Earlier (part number 736107). To obtain a copy of either of these documents, see Printed Resources. |
| DST | Set up 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. |

### EAS Message

**Quick Path: Administrative Console > DNCS tab > System Provisioning tab**

The **EAS message** section of the System Provisioning sub-tab allows you to manage the EAS (Emergency Alert System).

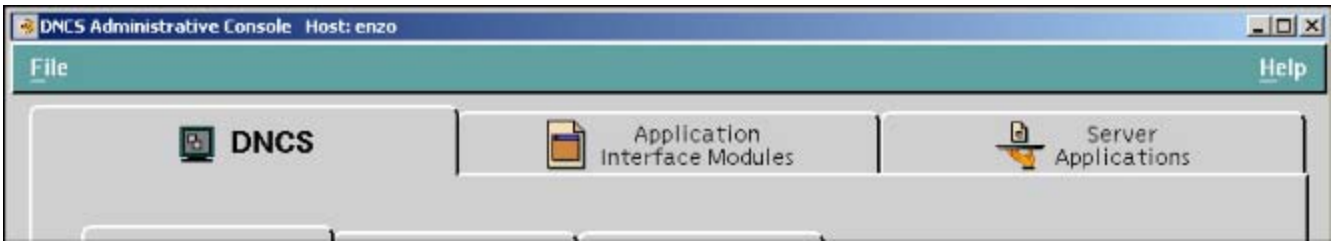
**WARNING:**

**Do not modify any of the Emergency Alert System settings in the DNCS unless you are specifically instructed to do so by the Federal Communications Commission (FCC), National Weather Service, local weather authority, or us. Otherwise, you could cause the EAS to perform improperly or not at all.**

**Note:** For more information about the Emergency Alert System, see Manage a Digital Emergency Alert System.

## DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.




For more information, click on a specific tab name in the following list.

- DNCS tab
- Application Interface Modules tab
- Server Applications tab

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console Status window also displays the Network Management tab.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Tab

The **DNCS** tab on the DNCS Administrative Console provides access to certain functions that DNCS software directly controls. These functions are separated into sub-tabs:

- System Provisioning
- Network Element Provisioning
- Home Element Provisioning
- Utilities

### System Provisioning Sub-Tab

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **System Provisioning** sub-tab on the DNCS tab is divided into four functional sections:

- Service Provisioning
- RF Spectrum Management
- System Management
- EAS message

### Service Provisioning

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **Service Provisioning** section of the System Provisioning sub-tab has three buttons that allow you to set up aspects of different kinds of services as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| Source | ▪Add, modify, or delete analog and digital service sources<br>▪Encrypt or un-encrypt service sources<br>▪Add, modify, or delete analog and digital service source definitions<br>▪Add, modify, or delete segments for individual sources<br>▪View segments of all sources |
| Package | ▪Add, modify, or delete service packages<br>▪Create packages within packages |
| ATM PVC | ▪Add, modify, or delete ATM PVC maps |

### RF Spectrum Management

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **RF Spectrum Management** section of the System Provisioning sub-tab contains the Bandwidth Allocation button, which allows you to perform the following tasks:

- Add, modify, or delete upper and lower frequency allocations for various service types (analog, digital, and so forth)
- View QPSK modulator/demodulator frequency allocations
- View QAM sessions, frequency allocations, and transport stream IDs

### System Management

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

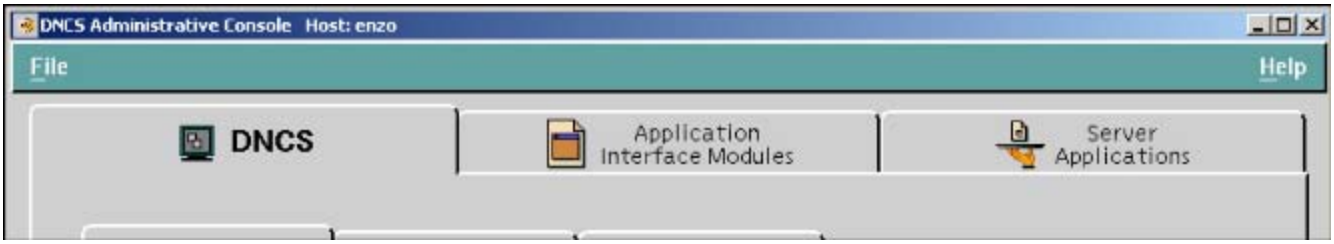
The **System Management** section of the System Provisioning sub-tab has four buttons that allow you to manage various aspects of the DBDS as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| DNCS System | ▪Set up DHCT session signalling parameters<br>▪Set up Network session signalling parameters<br>▪Establish the system channel plan: STD, HRC, or IRC<br>▪Establish whether or not the system is compliant with Open Cable standards |
| UN-Config | ▪Initiate UN-Config for a single DHCT<br>▪Initiate UN-Config for a DHCT type<br>▪Reboot a single DHCT<br>**Note:** For assistance in using this feature, refer to Downloading New Client Application Platform Installation Instructions (part number 4003052). To obtain a copy of this document, see Printed Resources. |
| User Access | Add, modify, or delete users with differing levels of access to the DNCS.<br>**Note:** For assistance in using this feature, refer to Guidelines for System Security Passwords (part number 738188). To obtain a copy of this document, see Printed Resources. |
| DHCT Mgr | ▪Establish the DHCT registration mode: Administrative Gateway or Open<br>▪Establish the method by which IP addresses are assigned to DHCTs: Dynamic, Override, or Static<br>▪Establish how often UN-Config messages are sent to DHCTs in the system<br>**Note:** For assistance in using this feature, refer to Explorer Digital Home Communications Terminal Staging Guide (part number 734375) or Separable Security Host Staging Guide for System Release 4.2.1 and Earlier (part number 736107). To obtain a copy of either of these documents, see Printed Resources. |
| DST | Set up 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. |

# Manage the Network

## DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.




For more information, click on a specific tab name in the following list.

- DNCS tab
- Application Interface Modules tab
- Server Applications tab

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console Status window also displays the Network Management tab.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Tab

The **DNCS** tab on the DNCS Administrative Console provides access to certain functions that DNCS software directly controls. These functions are separated into sub-tabs:

- System Provisioning
- Network Element Provisioning
- Home Element Provisioning
- Utilities

### System Provisioning Sub-Tab

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **System Provisioning** sub-tab on the DNCS tab is divided into four functional sections:

- Service Provisioning
- RF Spectrum Management
- System Management
- EAS message

### Service Provisioning

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **Service Provisioning** section of the System Provisioning sub-tab has three buttons that allow you to set up

aspects of different kinds of services as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| Source | ▪Add, modify, or delete analog and digital service sources<br>▪Encrypt or un-encrypt service sources<br>▪Add, modify, or delete analog and digital service source definitions<br>▪Add, modify, or delete segments for individual sources<br>▪View segments of all sources |
| Package | ▪Add, modify, or delete service packages<br>▪Create packages within packages |
| ATM PVC | ▪Add, modify, or delete ATM PVC maps |

**RF Spectrum Management**

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **RF Spectrum Management** section of the System Provisioning sub-tab contains the Bandwidth Allocation button, which allows you to perform the following tasks:

- ▪Add, modify, or delete upper and lower frequency allocations for various service types (analog, digital, and so forth)
- ▪View QPSK modulator/demodulator frequency allocations
- ▪View QAM sessions, frequency allocations, and transport stream IDs

**System Management**

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab**

The **System Management** section of the System Provisioning sub-tab has four buttons that allow you to manage various aspects of the DBDS as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| DNCS System | ▪Set up DHCT session signalling parameters<br>▪Set up Network session signalling parameters<br>▪Establish the system channel plan: STD, HRC, or IRC<br>▪Establish whether or not the system is compliant with Open Cable standards |
| UN-Config | ▪Initiate UN-Config for a single DHCT<br>▪Initiate UN-Config for a DHCT type<br>▪Reboot a single DHCT<br>**Note:** For assistance in using this feature, refer to Downloading New Client Application Platform Installation Instructions (part number 4003052). To obtain a copy of this document, see Printed Resources. |
| User Access | Add, modify, or delete users with differing levels of access to the DNCS. |

| | |
|---|---|
| | **Note:** For assistance in using this feature, refer to Guidelines for System Security Passwords (part number 738188). To obtain a copy of this document, see Printed Resources. |
| DHCT Mgr | ▪Establish the DHCT registration mode: Administrative Gateway or Open<br>▪Establish the method by which IP addresses are assigned to DHCTs: Dynamic, Override, or Static<br>▪Establish how often UN-Config messages are sent to DHCTs in the system<br>**Note:** For assistance in using this feature, refer to Explorer Digital Home Communications Terminal Staging Guide (part number 734375) or Separable Security Host Staging Guide for System Release 4.2.1 and Earlier (part number 736107). To obtain a copy of either of these documents, see Printed Resources. |
| DST | Set up 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. |

### EAS Message

**Quick Path: Administrative Console > DNCS tab > System Provisioning tab**

The **EAS message** section of the System Provisioning sub-tab allows you to manage the EAS (Emergency Alert System).

**WARNING:**

**Do not modify any of the Emergency Alert System settings in the DNCS unless you are specifically instructed to do so by the Federal Communications Commission (FCC), National Weather Service, local weather authority, or us. Otherwise, you could cause the EAS to perform improperly or not at all.**

**Note:** For more information about the Emergency Alert System, see Manage a Digital Emergency Alert System.

### Network Element Provisioning Sub-Tab

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

The **Network Element Provisioning** sub-tab on the DNCS tab has several buttons that allow you to set up hardware elements in your system (excluding DHCTs) as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| Headend | Add, modify, or delete a headend |
| Node Set | Add, modify, or delete a node set and its associated hub |
| Service Group | ▪Add, modify, or delete service groups<br>▪Reset service groups |
| Hub | ▪Add, modify, or delete a hub<br>▪Define the time zone where a hub is located<br>▪If daylight saving time is observed at this hub, define the DST Zone ID |
| QPSK/CMTS | ▪Add, modify, or delete a QPSK modulator<br>▪Add, modify, or delete a QPSK demodulator<br>▪Reset a QPSK modulator or QPSK demodulator<br>▪View a list of QPSK modulator/demodulator (modem) pairs<br>**Note:** We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data. For more information about this software product, contact the representative who handles your account. |
| BIG | ▪Add, modify, or delete a BIG<br>▪Assign program numbers and PIDs for each BFS session |
| QAM | ▪Add, modify, or delete a QAM, MQAM, GQAM, RF GoQAM, or IF GoQAM<br>▪Reset a QAM, MQAM, GQAM, RF GoQAM, or IF GoQAM |
| MPEG Source | Add, modify, or delete an MPEG source |
| VASP | Add, modify, or delete a VASP |
| SONET | Add, modify, or delete a SONET ring and its connections |
| UpConverter | Add, modify, or delete an UpConverter |
| GbE Transport | |
| Table-Based QAM | Add, modify, or delete table-based QAM modulators |

### Home Element Provisioning Sub-Tab

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

The **Home Element Provisioning** sub-tab on the DNCS tab allows you to manage the devices deployed within a subscriber's home.

### Related Topics

- Set-Tops
- PowerKEY CableCARD Modules
- Utilities Sub-Tab

### DHCT Provisioning

The **DHCT Provisioning** area has five buttons that allow you to work with the set-top and CableCARD modules in your system as described in the following table. You may find the Downloading New Client Application Platform Installation Instructions (part number 4003052) useful for more information on using this part of the DNCS.

**Important:** Except for testing purposes, you should set up (stage) the DHCTs in your system as described in the Explorer Digital Home Communications Terminal Staging Guide (part number 734375). See Printed Resources for information on obtaining these guides.

| This button... | ...allows you to perform these tasks |
|---|---|
| Type | ▪View a list of the set-top types contained in your DNCS database, along with the revision level and OUI for each.<br>▪Add, modify, or delete a set-top type.<br>▪Associate software TOC files with or unassociate them from older set-tops that use the OSM method to download software.<br>▪Download specific operating systems to the set-tops in your DBDS. |
| DHCT | ▪Add, modify, or delete an individual set-top or CableCARD module.<br>▪Send service or system information to an individual set-top within a few minutes.<br>▪Assign service packages to an individual set-top.<br>▪Enable an individual set-top to display secure analog, IPPV, PPV, and VOD services.<br>▪Authorize a set-top or CableCARD module for service.<br>**Note:** Your billing system normally authorizes the set-tops and CableCARD modules in your system for all services. Although you can authorize set-tops and CableCARD modules for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops and CableCARD modules for services with your billing system vendor. |

| | |
|---|---|
| Boot Page | This feature is reserved for future use. |
| OS | ▪Add OS files for older set-tops that use the OSM software download method.<br>▪View the names of files that currently reside on the BFS. |
| Image<br>**Note:** Although this button is in the DHCT Provisioning area, you can use this button to download software to CableCARD modules and set-tops that use the CVT download method. | ▪Load the set-top resource file (set-top.res) into the DNCS database.<br>▪View a list of the current set of image files on your system.<br>▪Load new image files for CVT downloads onto the BFS, or remove old image files that are no longer used.<br>▪Create test groups of set-tops and CableCARD modules.<br>▪Set up and download client software to set-tops and CableCARD modules on your system that use the CVT software download method. |

### CableCARD Module Provisioning

The CableCARD button in the CableCARD Provisioning area allows you to manage the CableCARD modules in your system.

**Important:** Except for testing purposes, you should set up (stage) the CableCARD modules as described in the Separable Security Host Staging Guide for System Release 4.2.1 and Earlier (part number 736107). See Printed Resources for information on obtaining this guide.

| This button... | ...allows you to perform these tasks |
|---|---|
| CableCARD | ▪View a list of summary information about all PowerKEY CableCARD modules and their host devices in your system.<br>▪Add, modify, or delete a CableCARD module and its host device.<br>▪Configure the server process that controls communications with the CableCARD modules in your system.<br>▪Revoke recording privileges of a CableCARD module so the host device can record copy-protected content according to the copy protection settings of each program or event.<br>▪Restore recording privileges of a CableCARD module so the host device can record copy-protected content according to the copy protection settings of each program or event.<br>▪View a list of all revoked host devices and their associated CableCARD modules.<br>▪Configure the CP MMI screen that is displayed on CableCARD hosts. |

### DHCT Provisioning

The **DHCT Provisioning** area has five buttons that allow you to work with the set-top and CableCARD modules in your system as described in the following table. You may find the Downloading New Client Application Platform Installation Instructions (part number 4003052) useful for more information on using this part of the DNCS.

**Important:** Except for testing purposes, you should set up (stage) the DHCTs in your system as described in the Explorer Digital Home Communications Terminal Staging Guide (part number 734375). See Printed Resources for information on obtaining these guides.

| This button... | ...allows you to perform these tasks |
|---|---|
| Type | ▪View a list of the set-top types contained in your DNCS database, along with the revision level and OUI for each.<br>▪Add, modify, or delete a set-top type.<br>▪Associate software TOC files with or unassociate them from older set-tops that use the OSM method to download software.<br>▪Download specific operating systems to the set-tops in your DBDS. |
| DHCT | ▪Add, modify, or delete an individual set-top or CableCARD module.<br>▪Send service or system information to an individual set-top within a few minutes.<br>▪Assign service packages to an individual set-top.<br>▪Enable an individual set-top to display secure analog, IPPV, PPV, and VOD services.<br>▪Authorize a set-top or CableCARD module for service.<br>**Note:** Your billing system normally authorizes the set-tops and CableCARD modules in your system for all services. Although you can authorize set-tops and CableCARD modules for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops and CableCARD modules for services with your billing system vendor. |
| Boot Page | This feature is reserved for future use. |
| OS | ▪Add OS files for older set-tops that use the OSM software download method.<br>▪View the names of files that currently reside on the BFS. |
| Image<br>**Note:** Although this button is in the DHCT Provisioning area, you can use this button to download software to CableCARD modules and set-tops that use | ▪Load the set-top resource file (set-top.res) into the DNCS database.<br>▪View a list of the current set of image files on your system.<br>▪Load new image files for CVT downloads onto the BFS, or remove old image files that are no longer used.<br>▪Create test groups of set-tops and CableCARD modules. |

| | |
|---|---|
| the CVT download method. | ▪Set up and download client software to set-tops and CableCARD modules on your system that use the CVT software download method. |

## Home Element Provisioning Sub-Tab

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

The **Home Element Provisioning** sub-tab on the DNCS tab allows you to manage the devices deployed within a subscriber's home.

### Related Topics

- Set-Tops
- PowerKEY CableCARD Modules
- Utilities Sub-Tab

### DHCT Provisioning

The **DHCT Provisioning** area has five buttons that allow you to work with the set-top and CableCARD modules in your system as described in the following table. You may find the Downloading New Client Application Platform Installation Instructions (part number 4003052) useful for more information on using this part of the DNCS.

**Important:** Except for testing purposes, you should set up (stage) the DHCTs in your system as described in the Explorer Digital Home Communications Terminal Staging Guide (part number 734375). See Printed Resources for information on obtaining these guides.

| This button... | ...allows you to perform these tasks |
|---|---|
| Type | ▪View a list of the set-top types contained in your DNCS database, along with the revision level and OUI for each.<br>▪Add, modify, or delete a set-top type.<br>▪Associate software TOC files with or unassociate them from older set-tops that use the OSM method to download software.<br>▪Download specific operating systems to the set-tops in your DBDS. |
| DHCT | ▪Add, modify, or delete an individual set-top or CableCARD module.<br>▪Send service or system information to an individual set-top within a few minutes.<br>▪Assign service packages to an individual set-top.<br>▪Enable an individual set-top to display secure analog, IPPV, PPV, and VOD services.<br>▪Authorize a set-top or CableCARD module for service.<br>**Note:** Your billing system normally authorizes the set-tops and CableCARD modules in your system for all services. Although you can authorize set-tops and CableCARD modules for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops and CableCARD modules for services with your billing system vendor. |

| | |
|---|---|
| Boot Page | This feature is reserved for future use. |
| OS | ▪Add OS files for older set-tops that use the OSM software download method.<br>▪View the names of files that currently reside on the BFS. |
| Image<br>**Note:** Although this button is in the DHCT Provisioning area, you can use this button to download software to CableCARD modules and set-tops that use the CVT download method. | ▪Load the set-top resource file (set-top.res) into the DNCS database.<br>▪View a list of the current set of image files on your system.<br>▪Load new image files for CVT downloads onto the BFS, or remove old image files that are no longer used.<br>▪Create test groups of set-tops and CableCARD modules.<br>▪Set up and download client software to set-tops and CableCARD modules on your system that use the CVT software download method. |

### CableCARD Module Provisioning

The CableCARD button in the CableCARD Provisioning area allows you to manage the CableCARD modules in your system.

**Important:** Except for testing purposes, you should set up (stage) the CableCARD modules as described in the Separable Security Host Staging Guide for System Release 4.2.1 and Earlier (part number 736107). See Printed Resources for information on obtaining this guide.

| This button... | ...allows you to perform these tasks |
|---|---|
| CableCARD | ▪View a list of summary information about all PowerKEY CableCARD modules and their host devices in your system.<br>▪Add, modify, or delete a CableCARD module and its host device.<br>▪Configure the server process that controls communications with the CableCARD modules in your system.<br>▪Revoke recording privileges of a CableCARD module so the host device can record copy-protected content according to the copy protection settings of each program or event.<br>▪Restore recording privileges of a CableCARD module so the host device can record copy-protected content according to the copy protection settings of each program or event.<br>▪View a list of all revoked host devices and their associated CableCARD modules.<br>▪Configure the CP MMI screen that is displayed on CableCARD hosts. |

### Utilities Sub-Tab

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab**

The **Utilities** sub-tab on the DNCS tab allows you to perform a variety of useful tasks as described in the following table.

| This button... | ...allows you to perform these tasks |
|---|---|
| Tracing | Set the tracing level for each DNCS process so that you can define how much debugging information is displayed in the dncsLog file for each process. |
| Reports | Run various reports to see how the system is functioning.<br>For more information, see the .<br>**Note:** To obtain this guide, see Printed Resources. |
| GUI Servers | ▪See the location of a particular web user interface (UI) server file.<br>▪Modify the web UI application name, server name, and server port.<br>▪View the status of a web UI server (for example, active). If the server does not respond to a system request for its status, the display indicates a status of unknown.<br>▪Stop or restart a web UI server. |
| Logging | Access the Logging utility to fine-tune log levels for processes and their libraries. |
| Session List | Control sessions and resources within the network. |
| xterm | Open an xterm window to perform troubleshooting activities. |

### Open an xterm Window

An xterm window gives you enter UNIX commands to manipulate, view, and edit various program files within the DNCS operating system.

Complete these steps to open an xterm window on the DNCS workstation.

1. On the Administrative Console, click the **Utilities** tab.
2. Click **xterm**. An xterm window opens and displays a root user prompt ($).

## Application Interface Modules Tab

The **Application Interface Modules** tab on the Administrative Console provides an interface between the server applications and the set-tops as described in the following table.

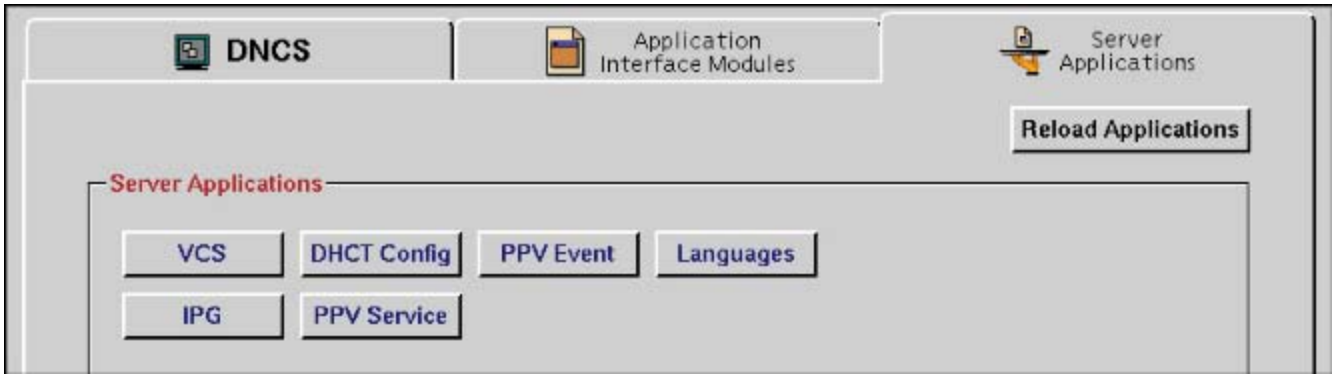
| This button... | ...allows you to perform these tasks |
|---|---|
| BFS Admin | ▪Add, modify, or delete BFS servers, sources, and hosts. For assistance, see Manage a Third-Party Application. |
| Channel Maps | ▪Add, modify, or delete channel maps.<br>▪Add services to specific channel slots on specific channel maps.<br>▪Assign specific channel maps to specific hubs. |
| Non-Channel Services | ▪Retrieve (view) the list of non-channel services assigned to a specific hub or bouquet.<br>▪Add, modify, or delete non-channel services for specific hubs or bouquets.<br>▪Assign non-channel services to specific hubs or bouquets. |
| BFS Client | Add, modify, or delete new servers, directories, files, and links to the BFS that allow DHCTs to access application information. |
| SAM Service | ▪View a list of services that are registered with the SAM, along with their Service IDs and application URLs.<br>▪Register (add) a service with the SAM.<br>▪Assign a logo to a service that subscribers will see when they tune to the service<br>▪Modify or delete a service that is registered with the SAM.<br>**Important:** Before you delete a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the set-tops that tune to that channel may lock up and reboot. |

### Related Topics

- Server Applications Tab

## Server Applications Tab

The **Server Applications** tab on the DNCS Administrative Console provides access to applications that reside on the SARA Server so that you can configure services associated with SARA applications. The options that appear on this tab vary depending on the applications available on your system. The following illustration provides some examples of options you might see on this tab. Refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for more information. To obtain this guide, refer to Printed Resources.



## Network Management Tab

If you are using the Spectrum NMS, the **Network Management** tab appears on the DNCS Administrative Console. This tab provides access to the Spectrum NMS windows, including the DHCT Monitor, so that you can monitor and manage activity on your system

**Notes:**

- The Spectrum NMS contains its own Help documentation. If you have questions on how to use the Spectrum NMS beyond this discussion, click the **Help** button that appears in the upper right corner of the Spectrum Control Panel.
- We offers the DBDS Alarm Management System to help you monitor your network elements instead of using Spectrum. For more information, contact the representative who handles your account.

# Network Setup Overview

## Introduction

The first step in managing the elements in your DBDS network is to set up the DNCS software so that it recognizes and can communicate with those elements. You do this by entering information about each element into the DNCS database.

This section describes how to set up your network using specific elements.

## What do you want to do?

- Set Up Your Network
- Learn about your Network Map
- Learn about Setting Up Logical Elements
- Learn about Setting Up Elements that Process System Data
- Learn about Setting Up Elements that Process Content
- Learn about Setting Up Set-Tops
- Learn about Optional Network Configurations

# Set Up Your Network

In most cases, we set up your network hardware and services in the DNCS for you. However, if you need to set up your network yourself, you can use these procedures. You can also use these procedures if you need to add elements to an existing network.

**Note:** When we first install your system, we configure the routes that are needed for all of the network elements to communicate with each other. However, if you add new network elements, new routes will need to be configured. In this case, we encourage you to have a service agreement or other means available for having these routes configured by qualified personnel.

**You Need to Know**

Before You Begin

Before you set up your network in the DNCS, you must do the following:

- Make sure that all the hardware to be managed by the DNCS is physically installed in your system
- Have your network map available

## Setting Up Your Network

**Important:** Unless noted otherwise, the steps listed below can be used for any type of system, standard or custom.

If you are setting up your network for the first time, you must complete ALL of these procedures in the order listed.

Complete these procedures to set up your network elements:

1. Get your network map; you will refer to it frequently throughout this process.
2. Set up the following logical elements in your system by adding them to your network:
   - Remote sites (needed if using an RCS)
   - Site billing references (needed if using an RCS)
   - Headends
   - Headends to RCS sites
   - Hubs
   - Hubs to RCS headends
   - Node Sets

   **Note:** If you are setting up elements in an RCS, you will follow a slightly different method to set up headends and hubs because these logical elements must be associated with another logical element, called a "site."

3. Set up the following elements that process system data for your system:
   - BFS BIG (NOT NEEDED for networks using Direct ASI)
   - DNCS ASI card (only for networks using Direct ASI)
   - One ASI card for each RNCS/LIONN in your RCS
   - BFS QAM modulator (for an RCS, set up one BFS QAM modulator for the DNCS and one for each RNCS/LIONN)

- VASP entries for a typical DBDS or VASP entries for a DBDS using RCS
- ATM PVC Maps (NOT NEEDED for networks using Direct ASI)

4. Set up a QPSK modulator.

5. If your system uses two-way communication, set up a QPSK demodulator.

6. If applicable, set up the PowerKEY Conditional Access system to support secure services, such as IPPV, VOD, or Web applications.

7. Set up the following elements that process content:
   - MPEG sources
   - Content QAM, MQAM, or GQAM modulators
   - Content RF GoQAM modulators or IF GoQAM modulators (for only systems using the Overlay option)
   - UpConverters
   - Service groups for VOD service

**Note:** GQAM modulators were first introduced in SR 2.1.1.

8. If applicable, set up SONET in your network.

9. If applicable, set up your network for OpenCable compliance.

10. Set up your services (clear, secure, PPV, VOD, and so on).

11. Set up the set-tops in your network.

12. If applicable, set up the PowerKEY CableCARD Modules in your network.

13. Set up the Emergency Alert System (EAS).

14. Update your network map to reflect changes you made to your network.

# Set Up Your Network

In most cases, we set up your network hardware and services in the DNCS for you. However, if you need to set up your network yourself, you can use these procedures. You can also use these procedures if you need to add elements to an existing network.

**Note:** When we first install your system, we configure the routes that are needed for all of the network elements to communicate with each other. However, if you add new network elements, new routes will need to be configured. In this case, we encourage you to have a service agreement or other means available for having these routes configured by qualified personnel.

**You Need to Know**

Before You Begin

Before you set up your network in the DNCS, you must do the following:

- Make sure that all the hardware to be managed by the DNCS is physically installed in your system
- Have your network map available

## Setting Up Your Network

**Important:** Unless noted otherwise, the steps listed below can be used for any type of system, standard or custom.

If you are setting up your network for the first time, you must complete ALL of these procedures in the order listed.

Complete these procedures to set up your network elements:

1. Get your network map; you will refer to it frequently throughout this process.
2. Set up the following logical elements in your system by adding them to your network:
   - Remote sites (needed if using an RCS)
   - Site billing references (needed if using an RCS)
   - Headends
   - Headends to RCS sites
   - Hubs
   - Hubs to RCS headends
   - Node Sets

   **Note:** If you are setting up elements in an RCS, you will follow a slightly different method to set up headends and hubs because these logical elements must be associated with another logical element, called a "site."

3. Set up the following elements that process system data for your system:
   - BFS BIG (NOT NEEDED for networks using Direct ASI)
   - DNCS ASI card (only for networks using Direct ASI)
   - One ASI card for each RNCS/LIONN in your RCS
   - BFS QAM modulator (for an RCS, set up one BFS QAM modulator for the DNCS and one for each RNCS/LIONN)

- VASP entries for a typical DBDS or VASP entries for a DBDS using RCS
- ATM PVC Maps (NOT NEEDED for networks using Direct ASI)

4. Set up a QPSK modulator.

5. If your system uses two-way communication, set up a QPSK demodulator.

6. If applicable, set up the PowerKEY Conditional Access system to support secure services, such as IPPV, VOD, or Web applications.

7. Set up the following elements that process content:
   - MPEG sources
   - Content QAM, MQAM, or GQAM modulators
   - Content RF GoQAM modulators or IF GoQAM modulators (for only systems using the Overlay option)
   - UpConverters
   - Service groups for VOD service

**Note:** GQAM modulators were first introduced in SR 2.1.1.

8. If applicable, set up SONET in your network.

9. If applicable, set up your network for OpenCable compliance.

10. Set up your services (clear, secure, PPV, VOD, and so on).

11. Set up the set-tops in your network.

12. If applicable, set up the PowerKEY CableCARD Modules in your network.

13. Set up the Emergency Alert System (EAS).

14. Update your network map to reflect changes you made to your network.

# Network Map

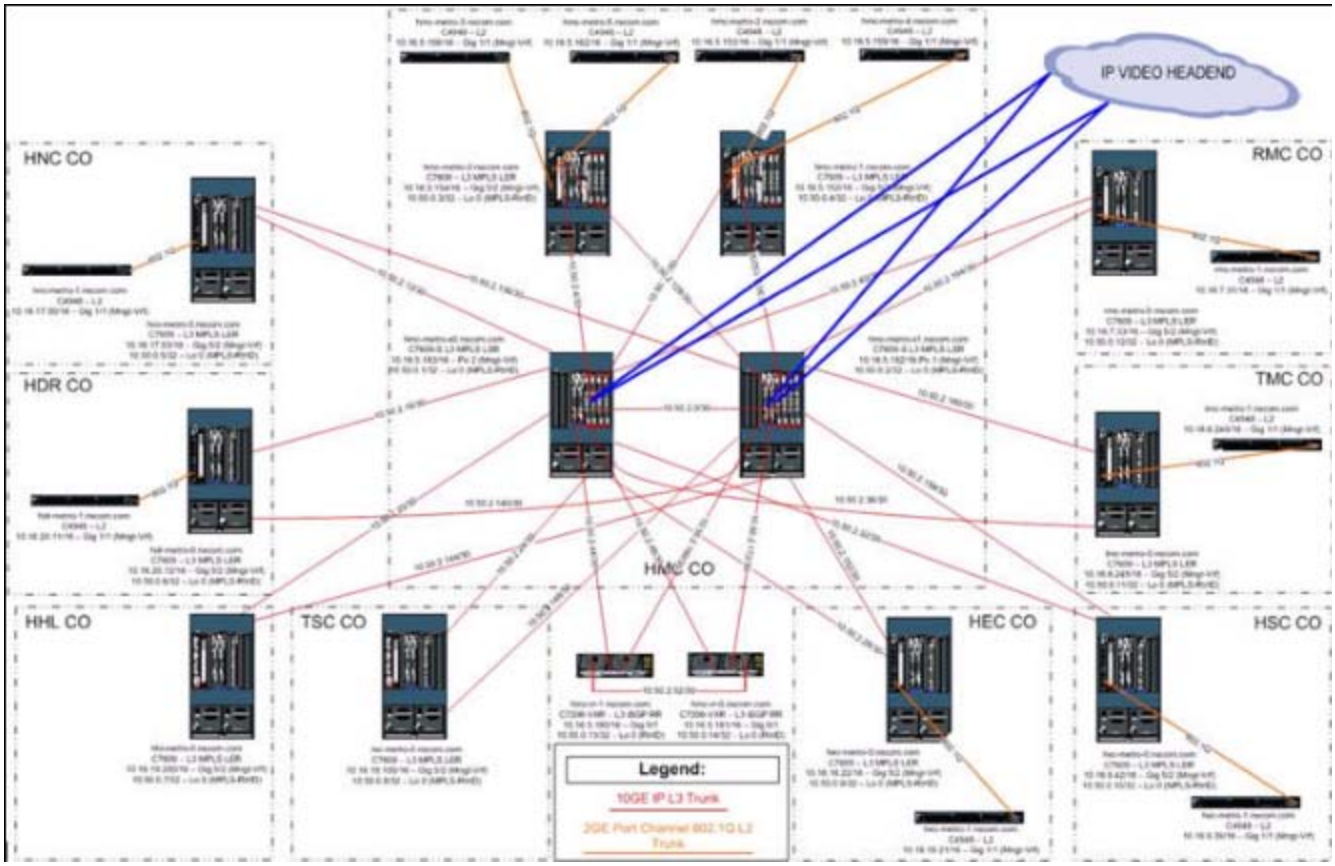
When we install a DBDS network, we prepare customized network maps (sometimes called "spider diagrams") that provide detailed information about the equipment layout of the site. After your equipment was installed, the installer should have given your system administrator a Network Planning Package. One of the items in that package is a copy of your network map.

Depending on your system, you may have several maps for your network. Keep your network maps readily available when you are using the DNCS to manage your network.

**Note:** If you are setting up your DBDS network yourself, you must create your own network maps.

## Network Map Example

The following illustration is an example of a typical network map.




## Naming and Numbering Scheme

**Important:** Each name must be unique for each piece of equipment within your system.

When you look at your network map, you will notice that each hardware element is labeled with a unique IP address, MAC address, and name. You may also see individual transport streams identified.

Note that there is a pattern to the naming and numbering scheme for these elements. The pattern may be as simple as numbering the individual elements, such as Hub1, Hub2, and so on. Conversely, the pattern may be more specific

by identifying the function or location of each element, such as Denver Hub.

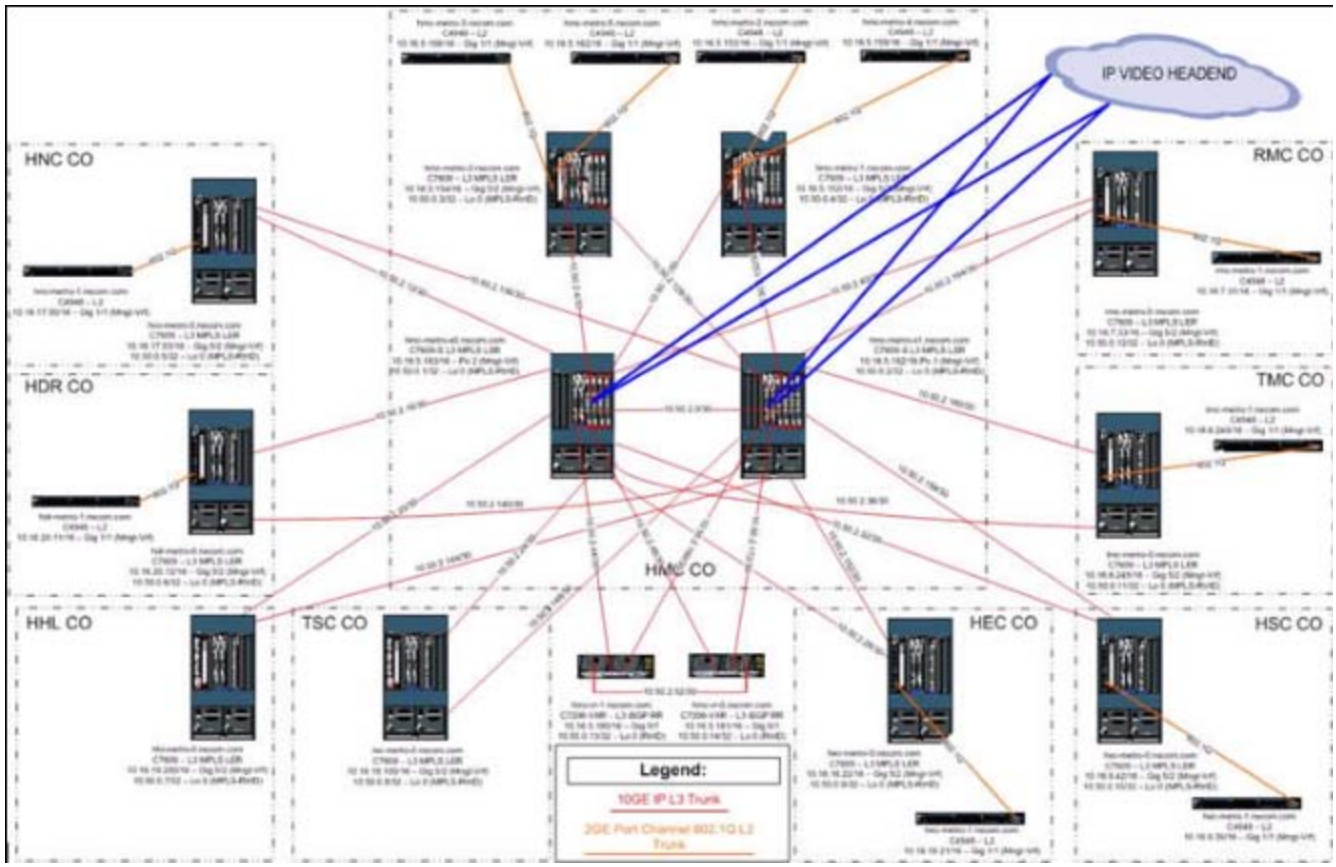
When you make additions or changes to your network, We strongly recommend that you use a naming and numbering scheme that follows the scheme used in your network map. Doing so will make it easier for you to identify where individual elements are located within your network, as well as what specific data is coming from and going to those elements. Additionally, you will be less likely to duplicate element names within your system, which can cause numerous data transport errors.

## Updating Network Maps

Whenever you make a change to your network, update your network map. This will allow you to troubleshoot your system more effectively and efficiently, should the need arise.

## Network Map Example

The following illustration is an example of a typical network map.



## Naming and Numbering Scheme

**Important:** Each name must be unique for each piece of equipment within your system.

When you look at your network map, you will notice that each hardware element is labeled with a unique IP address, MAC address, and name. You may also see individual transport streams identified.

Note that there is a pattern to the naming and numbering scheme for these elements. The pattern may be as simple as numbering the individual elements, such as Hub1, Hub2, and so on. Conversely, the pattern may be more specific by identifying the function or location of each element, such as Denver Hub.

When you make additions or changes to your network, We strongly recommend that you use a naming and numbering scheme that follows the scheme used in your network map. Doing so will make it easier for you to identify where individual elements are located within your network, as well as what specific data is coming from and going to those elements. Additionally, you will be less likely to duplicate element names within your system, which can cause numerous data transport errors.

# Network Map

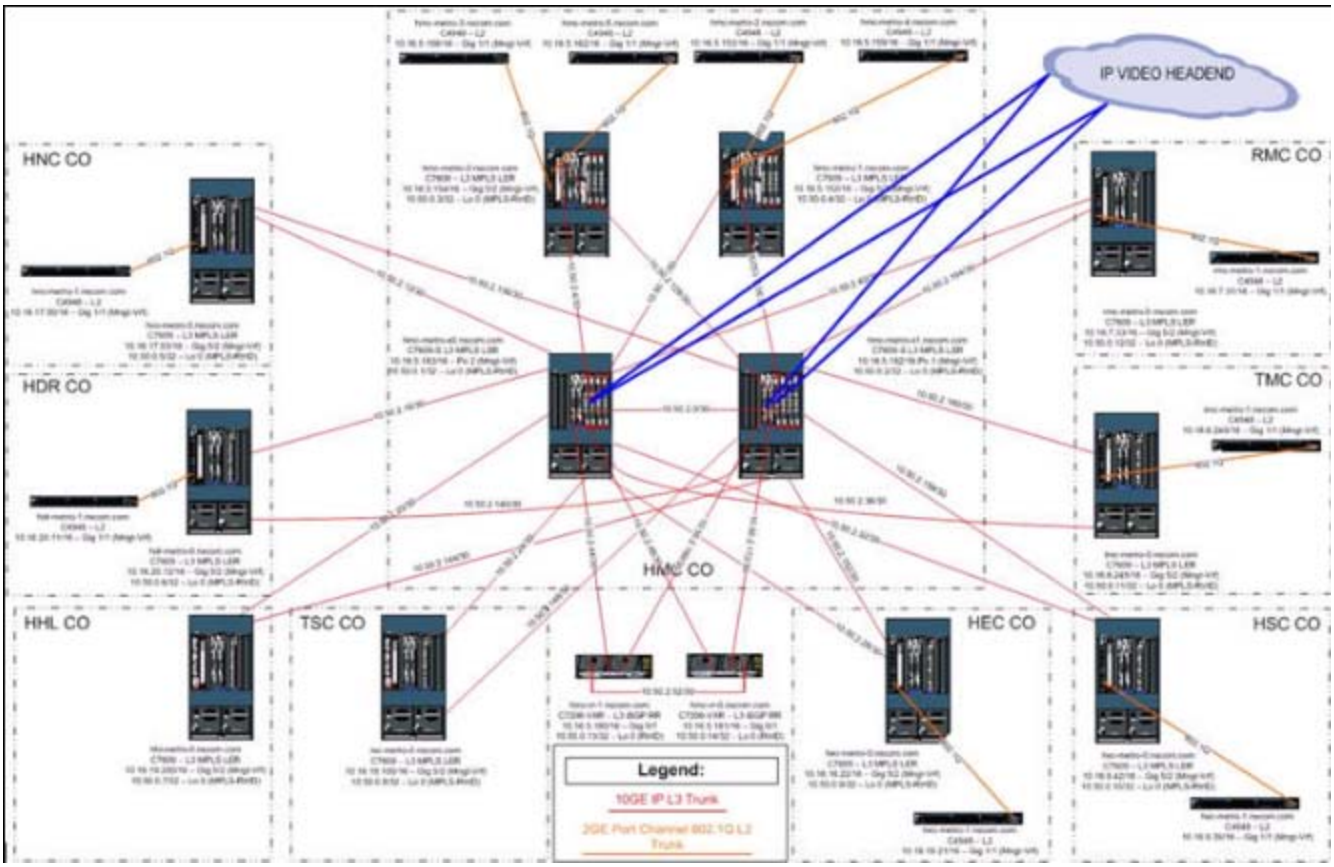
When we install a DBDS network, we prepare customized network maps (sometimes called "spider diagrams") that provide detailed information about the equipment layout of the site. After your equipment was installed, the installer should have given your system administrator a Network Planning Package. One of the items in that package is a copy of your network map.

Depending on your system, you may have several maps for your network. Keep your network maps readily available when you are using the DNCS to manage your network.

**Note:** If you are setting up your DBDS network yourself, you must create your own network maps.

## Network Map Example

The following illustration is an example of a typical network map.




## Naming and Numbering Scheme

**Important:** Each name must be unique for each piece of equipment within your system.

When you look at your network map, you will notice that each hardware element is labeled with a unique IP address, MAC address, and name. You may also see individual transport streams identified.

Note that there is a pattern to the naming and numbering scheme for these elements. The pattern may be as simple as numbering the individual elements, such as Hub1, Hub2, and so on. Conversely, the pattern may be more specific

by identifying the function or location of each element, such as Denver Hub.

When you make additions or changes to your network, We strongly recommend that you use a naming and numbering scheme that follows the scheme used in your network map. Doing so will make it easier for you to identify where individual elements are located within your network, as well as what specific data is coming from and going to those elements. Additionally, you will be less likely to duplicate element names within your system, which can cause numerous data transport errors.

## Updating Network Maps

Whenever you make a change to your network, update your network map. This will allow you to troubleshoot your system more effectively and efficiently, should the need arise.

# Setting Up Logical Elements

After obtaining a copy of your network map, the next step in setting up your network elements in the DNCS is to set up all of the logical elements. A logical element represents a group of devices, rather than a single, specific device. Logical elements are not actual hardware elements, but represent a group of QAM modulators, QPSK modulators, and QPSK demodulators that service a particular area of your network.

To set up your network elements in the DNCS, you must first set up a headend, at least one hub for each headend, and a node set for each demodulator in your system.

**Important:** Before you begin, you must have your network map.

## Guidelines for Setting Up Logical Elements

Keep in mind the following guidelines as you set up logical elements in your network:

- If you are setting up elements in an RCS, each site must have at least one headend.
- Each headend must have at least one hub.
- Node sets are necessary only if the headend supports reverse data, for example, PPV services and email. (We recommend that you have only one node set per demodulator on your system.)
- Do not assign demodulators with the same frequency to the same node set.

## Process Overview

To set up logical elements in the DNCS, you must complete the following steps. For step-by-step instructions for a particular task, click on that task.

1. If you are using an RCS, set up each remote site. (You do not need to set up the central DNCS site because the system automatically sets up this site for you.)
2. If you are using an RCS, set up a billing reference for each site, including one for the central DNCS site.
3. Set up a headend for your network. Note that adding a headend to an RCS uses a slightly different process:
   - Add a headend
   - Add a headend to each remote site in your RCS
4. Set up a headend for your network. Note that adding a headend to an RCS uses a slightly different process:
   - Add a hub
   - Add a hub to each headend in your RCS
   - Add a node set

## Guidelines for Setting Up Logical Elements

Keep in mind the following guidelines as you set up logical elements in your network:

- If you are setting up elements in an RCS, each site must have at least one headend.
- Each headend must have at least one hub.
- Node sets are necessary only if the headend supports reverse data, for example, PPV services and email. (We recommend that you have only one node set per demodulator on your system.)
- Do not assign demodulators with the same frequency to the same node set.

# Setting Up Logical Elements

After obtaining a copy of your network map, the next step in setting up your network elements in the DNCS is to set up all of the logical elements. A logical element represents a group of devices, rather than a single, specific device. Logical elements are not actual hardware elements, but represent a group of QAM modulators, QPSK modulators, and QPSK demodulators that service a particular area of your network.

To set up your network elements in the DNCS, you must first set up a headend, at least one hub for each headend, and a node set for each demodulator in your system.

**Important:** Before you begin, you must have your network map.

## Guidelines for Setting Up Logical Elements

Keep in mind the following guidelines as you set up logical elements in your network:

- If you are setting up elements in an RCS, each site must have at least one headend.
- Each headend must have at least one hub.
- Node sets are necessary only if the headend supports reverse data, for example, PPV services and email. (We recommend that you have only one node set per demodulator on your system.)
- Do not assign demodulators with the same frequency to the same node set.

## Process Overview

To set up logical elements in the DNCS, you must complete the following steps. For step-by-step instructions for a particular task, click on that task.

1. If you are using an RCS, set up each remote site. (You do not need to set up the central DNCS site because the system automatically sets up this site for you.)
1. If you are using an RCS, set up a billing reference for each site, including one for the central DNCS site.
1. Set up a headend for your network. Note that adding a headend to an RCS uses a slightly different process:
    - Add a headend
    - Add a headend to each remote site in your RCS
1. Set up a headend for your network. Note that adding a headend to an RCS uses a slightly different process:
    - Add a hub
    - Add a hub to each headend in your RCS
    - Add a node set

# Setting Up Elements that Process System Data

After you set up all of the logical elements in the DNCS, you must set up all of the elements that process system data for your network. There are two types of system data that must be transmitted from the DNCS:

- **System information (SI) data** essentially tuning information; provides the information that DHCTs need to be able to tune to a particular service
- **Broadcast File Server (BFS) data** consists of files, such as IPG and PPV information, operating system/resident application images, and application data files

The DNCS sends system data in one of two ways, depending upon your system configuration:

- In a system that does NOT use Direct ASI, the DNCS sends the data through the ATM Switch to the BFS BIG, and from there to the BFS QAM modulator. The modulator then processes the data and delivers it to DHCTs over the inband forward data channel (FDC).
- In a system that uses Direct ASI, the DNCS sends the data from the ASI card installed on the DNCS directly to the BFS QAM modulator, which delivers data to DHCTs over the inband forward data channel.

**Note:** If your system uses the RCS option, each RNCS/LIONN sends BFS data from the ASI card installed on the RNCS/LIONN directly to the BFS QAM modulator.

Before the DNCS can send system data to these elements, you must add information about each element into the DNCS database. In addition, the DNCS must be aware of all Value Added Service Provider (VASP) servers in your system.

**Note:** We recommend that you set up your BFS QAM modulator to also be your Distinguished QAM modulator.

**Important:** Before you begin, you must have your network map.

## Process Overview

To set up elements that process system data in the DNCS, you must complete the following tasks in order. For step-by-step instructions for a particular task, click on that task.

### Systems Without Direct ASI

1. Add a BFS BIG.
2. Add a BFS QAM modulator.
3. Verify your VASP configuration.
4. Add ATM PVC Maps.
5. Add a QPSK Modulator to the DNCS.

### Systems Using Direct ASI

1. Add an MPEG BFS Source.
2. Add a BFS QAM modulator. Note that adding a BFS QAM modulator to an RCS uses a different procedure:
   - Add a BFS QAM modulator
   - Add a BFS QAM modulator to an RCS
3. Verify the VASP configuration by referring to one of the following procedures:
   - Verify your VASP configuration

- Verify the VASP configuration in your RCS

**Note:** If you are using Direct ASI in an RCS, repeat these steps for each remote site in your network.

4. Add a QPSK Modulator to the DNCS.

# Setting Up Elements that Process System Data

After you set up all of the logical elements in the DNCS, you must set up all of the elements that process system data for your network. There are two types of system data that must be transmitted from the DNCS:

- **System information (SI) data** essentially tuning information; provides the information that DHCTs need to be able to tune to a particular service
- **Broadcast File Server (BFS) data** consists of files, such as IPG and PPV information, operating system/resident application images, and application data files

The DNCS sends system data in one of two ways, depending upon your system configuration:

- In a system that does NOT use Direct ASI, the DNCS sends the data through the ATM Switch to the BFS BIG, and from there to the BFS QAM modulator. The modulator then processes the data and delivers it to DHCTs over the inband forward data channel (FDC).
- In a system that uses Direct ASI, the DNCS sends the data from the ASI card installed on the DNCS directly to the BFS QAM modulator, which delivers data to DHCTs over the inband forward data channel.

**Note:** If your system uses the RCS option, each RNCS/LIONN sends BFS data from the ASI card installed on the RNCS/LIONN directly to the BFS QAM modulator.

Before the DNCS can send system data to these elements, you must add information about each element into the DNCS database. In addition, the DNCS must be aware of all Value Added Service Provider (VASP) servers in your system.

**Note:** We recommend that you set up your BFS QAM modulator to also be your Distinguished QAM modulator.

**Important:** Before you begin, you must have your network map.

## Process Overview

To set up elements that process system data in the DNCS, you must complete the following tasks in order. For step-by-step instructions for a particular task, click on that task.

### Systems Without Direct ASI

1. Add a BFS BIG.
2. Add a BFS QAM modulator.
3. Verify your VASP configuration.
4. Add ATM PVC Maps.
5. Add a QPSK Modulator to the DNCS.

### Systems Using Direct ASI

1. Add an MPEG BFS Source.
2. Add a BFS QAM modulator. Note that adding a BFS QAM modulator to an RCS uses a different procedure:
   - Add a BFS QAM modulator
   - Add a BFS QAM modulator to an RCS
3. Verify the VASP configuration by referring to one of the following procedures:
   - Verify your VASP configuration

- Verify the VASP configuration in your RCS

**Note:** If you are using Direct ASI in an RCS, repeat these steps for each remote site in your network.

4. Add a QPSK Modulator to the DNCS.

# Setting Up Elements that Process Content

After you set up the two-way communication path and, if applicable, the PowerKEY CA system, you must set up the elements that process content for your network. The following DBDS elements process content, such as audio/video programming and Web services:

- MPEG source equipment (for example, IRTs, MDRs, and RTEs)
- Content QAM, MQAM, or GQAM modulators
- For systems using the Overlay option, RF or IF GoQAM modulators (When using IF GoQAM modulators, also add UpConverters.)

The most common source of television programming is a digital feed from a satellite to some type of MPEG source equipment. The MPEG source equipment sends the MPEG transport streams containing content from the satellite to either a content QAM, MQAM, GQAM, or if using Overlay technology a GoQAM modulator. The modulator then modulates this data onto an RF signal, which ultimately is sent to DHCTs.

**Important:** Before you begin, you must have your network map.

## Process Overview

To set up elements that process content data in the DNCS, you must complete the following procedures in order. For step-by-step instructions for a particular procedure, click on that task:

1. Add an MPEG source.
2. Add the following, as appropriate:
   - Content QAM, content MQAM modulator, content GQAM modulator
   - If using Overlay technology, a content RF GoQAM or content IF GoQAM.
   - If you are offering VOD to your subscribers, add at least one service group.

     **Important:** If your system uses the Overlay option and provides VOD, add QAM modulators from other vendors to the DNCS. (These are sometimes called "third-party" QAM modulators.) Otherwise, DHCTs may be unable to tune to the correct channel to receive a VOD event because these modulators are not part of a VOD service group.

   - If using IF GoQAM modulators, add UpConverters.

**Notes:**

- You can add up to four MPEG sources per GQAM modulator, two MPEG sources per MQAM or GoQAM modulator, and one MPEG source per QAM modulator.
- If you are offering VOD services, you must install one VOD server in your network per VOD service.

# Setting Up Elements that Process Content

After you set up the two-way communication path and, if applicable, the PowerKEY CA system, you must set up the elements that process content for your network. The following DBDS elements process content, such as audio/video programming and Web services:

- MPEG source equipment (for example, IRTs, MDRs, and RTEs)
- Content QAM, MQAM, or GQAM modulators
- For systems using the Overlay option, RF or IF GoQAM modulators (When using IF GoQAM modulators, also add UpConverters.)

The most common source of television programming is a digital feed from a satellite to some type of MPEG source equipment. The MPEG source equipment sends the MPEG transport streams containing content from the satellite to either a content QAM, MQAM, GQAM, or if using Overlay technology a GoQAM modulator. The modulator then modulates this data onto an RF signal, which ultimately is sent to DHCTs.

**Important:** Before you begin, you must have your network map.

## Process Overview

To set up elements that process content data in the DNCS, you must complete the following procedures in order. For step-by-step instructions for a particular procedure, click on that task:

1. Add an MPEG source.
2. Add the following, as appropriate:
   - Content QAM, content MQAM modulator, content GQAM modulator
   - If using Overlay technology, a content RF GoQAM or content IF GoQAM.
   - If you are offering VOD to your subscribers, add at least one service group.

     **Important:** If your system uses the Overlay option and provides VOD, add QAM modulators from other vendors to the DNCS. (These are sometimes called "third-party" QAM modulators.) Otherwise, DHCTs may be unable to tune to the correct channel to receive a VOD event because these modulators are not part of a VOD service group.

   - If using IF GoQAM modulators, add UpConverters.

**Notes:**

- You can add up to four MPEG sources per GQAM modulator, two MPEG sources per MQAM or GoQAM modulator, and one MPEG source per QAM modulator.
- If you are offering VOD services, you must install one VOD server in your network per VOD service.

# Setting Up Set-Tops

After you have set up all of your other network elements, you are ready to set up your set-tops in the DNCS.

**You Need to Know**

Before You Begin

Before you begin setting up your set-top, you must make sure that you have set up all of your network elements and defined your system as being OpenCable compliant (if applicable).

## Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
2. Set up existing DHCTs.
3. Set up Aptiv Digital networks.

## Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

## Setting Up Existing DHCTs

To upgrade the operating system (OS) and Resident Application (ResApp) software on DHCTs that are already deployed, refer to the appropriate upgrade instructions for each DHCT model. If you cannot locate these instructions, contact Cisco Services.

To use the DHCT Configuration change or authorize services for an existing DHCT, see Authorizing a DHCT or CableCARD Module for Service.

## Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
2. Set up existing DHCTs.
3. Set up Aptiv Digital networks.

## Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

# Setting Up Set-Tops

After you have set up all of your other network elements, you are ready to set up your set-tops in the DNCS.

**You Need to Know**

Before You Begin

Before you begin setting up your set-top, you must make sure that you have set up all of your network elements and defined your system as being OpenCable compliant (if applicable).

## Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
1. Set up existing DHCTs.
1. Set up Aptiv Digital networks.

## Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

## Setting Up Existing DHCTs

To upgrade the operating system (OS) and Resident Application (ResApp) software on DHCTs that are already deployed, refer to the appropriate upgrade instructions for each DHCT model. If you cannot locate these instructions, contact Cisco Services.

To use the DHCT Configuration change or authorize services for an existing DHCT, see Authorizing a DHCT or CableCARD Module for Service.

# Optional Network Configurations

Network configurations often start from a standard, or typical, network configuration and are modified from this basic configuration according to the needs of each cable service provider. In addition to any unique modifications made for a particular provider or site, We provide the following optional configurations that can be combined with a typical network configuration.

**Note:** For an overview of the elements used in a typical configuration and in any of the following options, see Setting Up Your Network.

- Direct Asynchronous Serial Interface (ASI) - Networks using Direct ASI allow you to send Broadcast File System (BFS) data directly to your BFS QAM modulator, providing you have installed an ASI card on the DNCS. With Direct ASI, you eliminate the need for a BFS BIG. Support for Direct ASI requires the installation of SR 2.5 (or later), SR 3.5 (or later), and the installation of an ASI card on your DNCS. (Our RCS option includes the use of Direct ASI.)
- Overlay Technology - Networks using the Overlay option are able to deploy in the same network, DHCTs manufactured by us or by other vendors. Support for Overlay technology requires the installation of SR 2.5 (or later), SR 3.5 (or later), and enabling the SR software license and the Overlay software license. GoQAM modulators are key components of Overlay technology. GoQAM modulators receive both the clear and encrypted content data, combine the two data streams into a single transport stream, and then send this partially encrypted stream to hubs that feed DHCTs manufactured by us or another vendor.
- Regional Control System - Networks running a Regional Control System manage remote sites from a centrally located DNCS. Because all system management is done from a central location, there is no need for system operators to be physically located at remote sites. An RCS must be used with Direct ASI, and may be used in conjunction with Overlay technology. Support for an RCS requires the installation of SR 2.5 (or later), SR 3.5 (or later), and enabling the software license.

**Important:** When we first install your system, we configure the routes that are needed for all of the network elements to communicate with each other. However, if you add new network elements, new routes will need to be configured. In this case, we encourage you to have a service agreement or other means available for having these routes configured by qualified personnel.

# Manage Network Elements

## Introduction

The topics in this section can help you set up standard elements used in a typical DBDS.

## What do you want to do?

- Manage a Headend
- Manage a Hub
- Manage a Node Set
- Manage a BFS QAM Modulator
- Manage VASPs
- Manage ATM PVC Maps
- Manage an MPEG Content Source
- Manage a QAM Modulator for Content
- Manage an MQAM Modulator for Content
- Manage a GQAM Modulator for Content
- Manage Generic QAM Models
- Manage Generic QAMs
- Manage a Table-Based QAM
- Manage a QPSK Modulator
- Manage a QPSK Demodulator
- Manage Set-Tops
- Manage PowerKEY CableCARD Modules
- Manage Content Sources and Sessions
- Manage Channel Maps and Channels
- Manage the SARA Server
- Manage Service Groups

# Headend

The first logical element you must set up in your network is a headend. You can add an unlimited number of headends to the DNCS.

A headend is a logical element that represents a group of QAM modulators, QPSK modulators, and QPSK demodulators that provide services to a particular group of DHCTs.

## What do you want to do?

- Add a Headend
- Modify a Headend
- Delete a Headend

## Add a Headend

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Headend > File > New**

### Adding a Headend

Complete these steps to add a headend to your network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Headend**. The Headend List window opens.
4. Click **File > New**. The Set Up Headend window opens.
5. Click in the **Headend Name** field and type the name you will use to identify this headend (for example, **HE1**). You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

6. Click **Save**. The system saves the headend information in the DNCS database and closes the Set Up Headend window. The Headend List updates to include the new headend.
7. Add the new headend to your network map.
8. Do you need to add another headend?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the Headend List window and return to the DNCS Administrative Console. Go to Adding a Hub.

### Related Topics

- Modify a Headend
- Delete a Headend

### Adding a Headend

Complete these steps to add a headend to your network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Headend**. The Headend List window opens.
4. Click **File > New**. The Set Up Headend window opens.
5. Click in the **Headend Name** field and type the name you will use to identify this headend (for example, **HE1**). You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

6. Click **Save**. The system saves the headend information in the DNCS database and closes the Set Up Headend window. The Headend List updates to include the new headend.
7. Add the new headend to your network map.
8. Do you need to add another headend?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the Headend List window and return to the DNCS Administrative Console. Go to Adding a Hub.

## Modify a Headend

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Headend > [Headend Name] > File > Open**

You can modify only the name of a headend. You may want to do this, for example, if the name entered previously does not comply with the naming convention established for other elements in your network.

**Important:** This procedure can be used for all systems except an RCS. A different method is required because RCS headends must be associated with a particular site.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Headend**. The Headend List window opens.
4. Click once on the row containing the headend name you want to modify.
5. Click **File > Open**. The Set Up Headend window opens for the headend you selected.
6. Click in the **Headend Name** field and change the name as desired. You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

7. Click **Save**. The system saves the new headend name in the DNCS database and closes the Set Up Headend window. The Headend List window updates to include the new headend name. Any devices connected to this headend are updated automatically with the new headend name information.
8. Change the headend name on your network map.
9. Do you need to modify another headend?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the Headend List window and return to the DNCS Administrative Console.

**Related Topics**

- Add a Headend
- Delete a Headend

# Delete a Headend

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Headend > [Headend Name] > File > Delete**

### You Need to Know

Before You Begin

Before you can delete a headend, you must delete all of the network elements associated with that headend. In addition, you must have your network map readily available.

### Deleting a Headend

**Important:** This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to delete headends from an RCS site. A different method is required because these headends must be associated with a particular site.

In a live system, there is usually no reason to delete a headend. Therefore, this procedure is provided for test situations only.

1. Are there any hubs associated with this headend?
   - If **yes**, delete those hubs first. Go to Delete a Hub. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Headend**. The Headend List window opens.
5. Click once on the row containing the headend you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the headend information from the DNCS database and from the Headend List window.
8. Delete the headend from your network map.
9. Click **File > Close** to close the Headend List window and return to the DNCS Administrative Console.
10. Do you need to delete another headend?
    - If **yes**, repeat this procedure.
    - If **no**, continue making any other changes that you need to make to your network.

### Related Topics

- Add a Headend
- Modify a Headend

### Deleting a Headend

**Important:** This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to delete headends from an RCS site. A different method is required because these headends must be associated with a particular site.

In a live system, there is usually no reason to delete a headend. Therefore, this procedure is provided for test situations only.

1. Are there any hubs associated with this headend?
   - If **yes**, delete those hubs first. Go to Delete a Hub. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Headend**. The Headend List window opens.
5. Click once on the row containing the headend you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the headend information from the DNCS database and from the Headend List window.
8. Delete the headend from your network map.
9. Click **File > Close** to close the Headend List window and return to the DNCS Administrative Console.
10. Do you need to delete another headend?
    - If **yes**, repeat this procedure.
    - If **no**, continue making any other changes that you need to make to your network.

# Hub

After you add a headend to the DNCS database, you must assign at least one hub to that headend. You can have an unlimited number of hubs per headend.

A hub is a logical element that represents the point at which out-of-band (QPSK-modulated) frequencies combine with inband (QAM) frequencies to be transmitted to subscribers through the radio frequency (RF) network.

## What do you want to do?

- Review the Hub Settings (Add a Hub, Hub Settings)
- Add a Hub
- Add a Hub to an RCS Headend
- Modify a Hub
- Delete a Hub

## Hub Settings

Use the following fields when you manage hubs in the DNCS.

| Field | Description |
|---|---|
| Hub Name | The name you will use to identify this hub (for example, **HE1_Hub1**). You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Hub ID | The number you will use to identify this hub<br><br>You can use up to eight numerical characters. Be sure to use an ID number that is consistent with the numbering scheme used on your network map.<br><br>For example, you might type **11** as a numerical representation for Headend 1, Hub 1.<br><br>**Important:** You will not be able to modify this field later. |
| Headend Name | The headend associated with this hub. |
| Timezone | The time zone where this hub is located. |
| DST Zone ID | The DST Zone ID for this hub.<br><br>**Important:** To manage time correctly on your network, you must install the Digital System Time Kit, if not installed previously. Refer to the DBDS System Time Installation and Maintenance Guide (part number 4011510) for more information. To obtain a copy of this publication, see Printed Resources.<br><br>For more information, see:<br><br>▪Daylight Saving Time Rules Settings<br>▪Configure Daylight Saving Time Rules Window |

### Related Topics

- Add a Hub
- Modify a Hub
- Delete a Hub

## Add a Hub

**Important:** This procedure can be used for all systems except an RCS. If you are using an RCS, follow a different method to add hubs to an RCS headend. A different method is required because RCS hubs must be associated with a particular site. See Add a Hub to an RCS Site for more information.

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > Add Hub**

### Adding a Hub

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub Summary window opens.
4. Click **Add Hub**. The Set Up Hub window opens.
5. Complete the fields on the screen as described in Hub Settings.

Use the following fields when you manage hubs in the DNCS.

| Field | Description |
|---|---|
| Hub Name | The name you will use to identify this hub (for example, **HE1_Hub1**). You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Hub ID | The number you will use to identify this hub<br>You can use up to eight numerical characters. Be sure to use an ID number that is consistent with the numbering scheme used on your network map.<br>For example, you might type **11** as a numerical representation for Headend 1, Hub 1.<br>**Important:** You will not be able to modify this field later. |
| Headend Name | The headend associated with this hub. |
| Timezone | The time zone where this hub is located. |
| DST Zone ID | The DST Zone ID for this hub.<br>**Important:** To manage time correctly on your network, you must install the Digital System Time Kit, if not installed previously. Refer to the DBDS System Time Installation and Maintenance Guide (part number 4011510) for more information. To obtain a copy of this publication, see Printed Resources.<br>For more information, see:<br>▪ Daylight Saving Time Rules Settings<br>▪ Configure Daylight Saving Time Rules Window |

6. Click **Save**. A confirmation message opens.
7. Click **OK**. The system saves the hub information in the DNCS database and the Hub Summary window

updates to include the new hub.

8. Add the new hub to your network map.

9. Do you need to add another hub?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **Exit** to close the Hub Summary window.

10. Does this hub support reverse data (for example, PPV services and e-mail)?

- If **yes**, your next step is to add at least one node set to this hub. Go to Add a Node Set.
- If **no**, go to step 11.

11. Are you are setting up your network for the first time?

- If **yes**, your next step is to set up the elements that process system data for your network. Go to Setting Up Elements that Process System Data.
- If **no**, continue making any other changes that you need to make to your network.

**Related Topics**

- Hub Settings (Add a Hub, Hub Settings)
- Add a Hub to an RCS Headend
- Modify a Hub
- Delete a Hub

### Adding a Hub

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub Summary window opens.
4. Click **Add Hub**. The Set Up Hub window opens.
5. Complete the fields on the screen as described in Hub Settings.

Use the following fields when you manage hubs in the DNCS.

| Field | Description |
|---|---|
| Hub Name | The name you will use to identify this hub (for example, **HE1_Hub1**). You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Hub ID | The number you will use to identify this hub<br>You can use up to eight numerical characters. Be sure to use an ID number that is consistent with the numbering scheme used on your network map.<br>For example, you might type **11** as a numerical representation for Headend 1, Hub 1.<br>**Important:** You will not be able to modify this field later. |
| Headend Name | The headend associated with this hub. |
| Timezone | The time zone where this hub is located. |
| DST Zone ID | The DST Zone ID for this hub.<br>**Important:** To manage time correctly on your network, you must install the Digital System Time Kit, if not installed previously. Refer to the DBDS System Time Installation and Maintenance Guide (part number 4011510) for more information. To obtain a copy of this publication, see Printed Resources.<br>For more information, see:<br>▪ Daylight Saving Time Rules Settings<br>▪ Configure Daylight Saving Time Rules Window |

6. Click **Save**. A confirmation message opens.
7. Click **OK**. The system saves the hub information in the DNCS database and the Hub Summary window updates to include the new hub.
8. Add the new hub to your network map.
9. Do you need to add another hub?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Exit** to close the Hub Summary window.
10. Does this hub support reverse data (for example, PPV services and e-mail)?
    - If **yes**, your next step is to add at least one node set to this hub. Go to Add a Node Set.
    - If **no**, go to step 11.

11. Are you are setting up your network for the first time?

- If **yes**, your next step is to set up the elements that process system data for your network. Go to Setting Up Elements that Process System Data.
- If **no**, continue making any other changes that you need to make to your network.

## Modify a Hub

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Make Changes] > Save > OK**

**Important:** This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to modify hubs in an RCS headend. A different method is required because these hubs must be associated with a particular site.

After a hub has been saved in the DNCS, you can modify only the following parameters for that hub:

- Hub name
- Timezone information
- DST Zone ID information

To change any other parameters, you must delete the hub, and re-add it to the DNCS, using the new information.

### Modifying a Hub

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub List window opens.
4. Click once on the row containing the hub you want to modify.
5. Click **File > Open**. The Set Up Hub window opens.
6. To change the name of this hub, click in the **Hub Name** field and change the name as desired. You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

7. To change the time zone information for this hub, click the **Timezone** arrow and select the time zone where this hub is located.
8. To change the daylight saving time setting for this hub, click the **DST Zone ID** arrow and select the DST Zone ID for the hub. (For more information on DST Zone ID, see the **DST Zone ID** field in Daylight Saving Time Rules Settings. For more information on DST rules, see Configure Daylight Saving Time Rules Window.)
9. When you finish making changes, click **Save**. A confirmation message opens.
10. Click **OK**. The Set Up Hub window updates to include the new hub information. Set-tops receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a set-top causes it to apply updates immediately.
11. Update your network map to reflect these changes.
12. Do you need to modify another hub?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Hub List window.

### Related Topics

- Hub Settings
- Add a Hub

- Delete a Hub

### Modifying a Hub

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub List window opens.
4. Click once on the row containing the hub you want to modify.
5. Click **File > Open**. The Set Up Hub window opens.
6. To change the name of this hub, click in the **Hub Name** field and change the name as desired. You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

7. To change the time zone information for this hub, click the **Timezone** arrow and select the time zone where this hub is located.
8. To change the daylight saving time setting for this hub, click the **DST Zone ID** arrow and select the DST Zone ID for the hub. (For more information on DST Zone ID, see the **DST Zone ID** field in Daylight Saving Time Rules Settings. For more information on DST rules, see Configure Daylight Saving Time Rules Window.)
9. When you finish making changes, click **Save**. A confirmation message opens.
10. Click **OK**. The Set Up Hub window updates to include the new hub information. Set-tops receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a set-top causes it to apply updates immediately.
11. Update your network map to reflect these changes.
12. Do you need to modify another hub?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Hub List window.

# Delete a Hub

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Select Hub] > Delete Selected Hub > OK**

**Important:** This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to delete hubs from an RCS headend. A different method is required because these hubs must be associated with a particular site.

You may want to delete a hub because you are no longer using it, or because you need to redefine the headend or hub ID.

## You Need to Know

Before You Begin

Before you can delete a hub, you must delete all of the network elements that are associated with it. In addition, you must have your network map readily available.

## Deleting a Hub

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to Delete a Node Set. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Hub**. The Hub List window opens.
5. Click once on the hub you want to delete.
6. Click **File > Delete**. A confirmation message opens.
7. Click **OK**. The message closes. The system removes the hub information from the DNCS database and from the Hub List window.
8. Delete the hub from your network map.
9. Do you need to delete another hub?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the Hub Summary window.

## Related Topics

- Hub Settings (Add a Hub, Hub Settings)
- Add a Hub
- Modify a Hub

### Deleting a Hub

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to Delete a Node Set. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Hub**. The Hub List window opens.
5. Click once on the hub you want to delete.
6. Click **File > Delete**. A confirmation message opens.
7. Click **OK**. The message closes. The system removes the hub information from the DNCS database and from the Hub List window.
8. Delete the hub from your network map.
9. Do you need to delete another hub?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the Hub Summary window.

# Node Set

After you add a hub to a headend, you must add at least one node set to that hub if the hub provides services that receive data from DHCTs and send this data to the DNCS.

A node set represents the point at which reverse data from a collection of upstream transmitters is combined and sent to a single QPSK demodulator. The QPSK demodulator then sends the data through the QPSK modulator to the DNCS for processing.

**Important:** We recommend that you have only one node set for each demodulator on your system. For more recommendations on setting up node sets refer to the Configuring Node Sets for the Digital Broadband Delivery System Technical Bulletin (part number 738169).

**Related Topics**

- Add a Node Set
- Modify a Node Set
- Delete a Node Set

## Add a Node Set

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Node Set > File > New**

### Adding a Node Set

Complete these steps to add a node set to your network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Node Set**. The Node Set List window opens.
4. Click **File > New**. The Set Up Node Set window opens.
5. Type the **Node Set Name** that you will use to identify this node set. You can use up to 20 alphanumeric characters. Be sure to use a name that contains no spaces and that is consistent with the naming scheme used on your network map.
6. Select the **Hub Name** that is associated with this node set from the list.
7. Click **Save**. The system saves the node set information in the DNCS database and closes the Set Up Node Set window. The Node Set List window updates to include the new node set.
8. Add the new node set to your network map.
9. Do you need to add another node set?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Node Set List window and return to the DNCS Administrative Console.

### Related Topics

- Modify a Node Set
- Delete a Node Set

### Adding a Node Set

Complete these steps to add a node set to your network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Node Set**. The Node Set List window opens.
4. Click **File > New**. The Set Up Node Set window opens.
5. Type the **Node Set Name** that you will use to identify this node set. You can use up to 20 alphanumeric characters. Be sure to use a name that contains no spaces and that is consistent with the naming scheme used on your network map.
6. Select the **Hub Name** that is associated with this node set from the list.
7. Click **Save**. The system saves the node set information in the DNCS database and closes the Set Up Node Set window. The Node Set List window updates to include the new node set.
8. Add the new node set to your network map.
9. Do you need to add another node set?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Node Set List window and return to the DNCS Administrative Console.

## Modify a Node Set

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Node Set > [Node Set Name] > File > Open**

After a node set has been saved in the DNCS, you can modify the node set name or the hub with which it is associated.

### Modifying a Node Set

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Node Set**. The Node Set List window opens.
4. Click once on the row containing the node set you want to modify.
5. Click **File > Open**. The Set Up Node Set window opens for the node set you selected.
6. To change the name of this node set, click in the **Node Set Name** field and change the name as desired. You can use up to 20 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

7. To change the hub associated with this node set, click the **Hub Name** arrow and select the desired hub.
8. When you finish making changes, click **Save**. The system saves the new node set information in the DNCS database and closes the Set Up Node Set window. The Node Set List window updates to include the new node set information.
9. Change your network map to reflect these changes.
10. Do you need to modify another node set?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Node Set List window and return to the DNCS Administrative Console.

### Related Topics

- Add a Node Set
- Delete a Node Set

### Modifying a Node Set

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Node Set**. The Node Set List window opens.
4. Click once on the row containing the node set you want to modify.
5. Click **File > Open**. The Set Up Node Set window opens for the node set you selected.
6. To change the name of this node set, click in the **Node Set Name** field and change the name as desired. You can use up to 20 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

7. To change the hub associated with this node set, click the **Hub Name** arrow and select the desired hub.
8. When you finish making changes, click **Save**. The system saves the new node set information in the DNCS database and closes the Set Up Node Set window. The Node Set List window updates to include the new node set information.
9. Change your network map to reflect these changes.
10. Do you need to modify another node set?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Node Set List window and return to the DNCS Administrative Console.

## Delete a Node Set

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Node Set > [Node Set Name] > File > Delete**

Before you can delete a node set, you must delete any QPSK demodulators that are associated with it.

### Deleting a Node Set

1. Are there any QPSK demodulators associated with this node set?
   - If **yes**, delete those demodulators first. Go to Deleting a QPSK Demodulator. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Node Set**. The Node Set List window opens.
5. Click once on the row containing the node set you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the node set information from the DNCS database and from the Node Set List.
8. Delete the node set from your network map.
9. Click **File > Close** to close the Node Set List window and return to the DNCS Administrative Console.
10. Do you need to delete another node set?
    - If **yes**, repeat this procedure.
    - If **no**, you are finished with this procedure.

### Related Topics

- Add a Node Set
- Modify a Node Set

### Deleting a Node Set

1. Are there any QPSK demodulators associated with this node set?
   - If **yes**, delete those demodulators first. Go to Deleting a QPSK Demodulator. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Node Set**. The Node Set List window opens.
5. Click once on the row containing the node set you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the node set information from the DNCS database and from the Node Set List.
8. Delete the node set from your network map.
9. Click **File > Close** to close the Node Set List window and return to the DNCS Administrative Console.
10. Do you need to delete another node set?
    - If **yes**, repeat this procedure.
    - If **no**, you are finished with this procedure.

# BFS QAM Modulator

A BFS QAM modulator receives BFS data, modulates the data onto an RF carrier, and then sends it downstream to all DHCTs on the headend. Each headend in your network must have a BFS QAM modulator associated with ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

A Distinguished QAM modulator that carries SI data to all the hubs in the headend.

### Related Topics

- View recommendations for BFS QAMs
- View BFS QAM settings
- Add a BFS QAM
- Modify a BFS QAM
- Delete a BFS QAM

## BFS and Distinguished QAM Modulator Recommendations

We recommend the following regarding BFS and Distinguished QAM modulators:

- Because all DHCTs on a headend need both BFS and SI data, set up your BFS QAM modulator to also be the Distinguished QAM modulator. However, if you are using an MQAM modulator to carry BFS data, you will need to set up another QAM modulator as the Distinguished QAM modulator to carry SI data. Only a QAM modulator can become a Distinguished QAM modulator.
- Make sure the BFS/Distinguished QAM modulator is not assigned to a specific hub, but that it sends BFS and SI data to all hubs in the headend.
- When you activate the BFS/Distinguished QAM modulator, make sure you select the **Allow SI** option to allow the modulator to process SI data, as well as other types of data.
- Make sure you define only one Distinguished QAM modulator per headend.

**Important:** If more than one Distinguished QAM candidate exists in a headend, the DNCS automatically selects one of those QAM modulators to be the Distinguished QAM. Depending on the other data you need to transmit through that QAM modulator, this may or may not be desirable.

### Related Topics

- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters
- Setting Up BFS QAM Modulator Connections
- Activating a BFS QAM Modulator

## BFS QAM Settings

Use the Set Up QAM page to manage the BFS QAM modulators in your network. The following tabs in this window provide settings for the BFS QAM:

- Basic Parameters Settings
- Connection Settings
- Advanced Parameters settings - The system automatically sets up advanced parameters. As a result, you do not need to complete any fields on the Advanced Parameters tab.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

### Basic Parameter Settings - BFS QAM Modulator

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪If the BFS QAM Modulator connects to a BFS BIG, click the **SWIF** option to select the type of card sending BFS data from the BFS BIG to this QAM modulator.<br>▪If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator<br>Select the type of modulation this QAM modulator uses. For example, if this modulator |

| | |
|---|---|
| uses | uses 256 QAM, you would select **256 QAM**. |
| **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

## Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

### Connections Settings - BFS QAM Modulator

Use the following fields when you manage the connections for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives from the BFS QAM resides. |
| Device Type | Determines the device type that feeds this QAM:<br>▪If a BFS BIG feeds the BFS QAM, select **BIG**.<br>▪If an ASI card on the DNCS feeds this BFS QAM, select **ASI**. Select this option if you are using the QAM modulator with an RCS.<br>The option you select determines which parameters display for setup, as described below. |
| Device Name | The name of the device. Valid for either BFS BIG or ASI QAMs. |
| Card Type | The type of card in the BFS BIG.<br>Select **MSYNC SWIF**. |
| Slot Number | The slot number where the MSYNC control card is installed on the BFS BIG (usually, slot 3).<br>Valid for BFS BIG only. |
| Port Number | The port number for the various cards:<br>▪**For BFS BIG** - control card that is connected to this QAM modulator (usually port 1).<br>▪**For ASI** - Select the port number on the ASI card that is connected to this BFS QAM modulator. |

### Related Topics

- Add a BFS QAM
- Setting Up BFS QAM Modulator Connections in an RCS
- BFS QAM Modulator
- BFS QAM Settings

## Add a BFS QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used for all systems except those that use the RCS option. If your system uses the RCS option, follow a different procedure to set up a BFS QAM modulator for an RCS. A different procedure is required because the RCS option requires system information (SI) to be delivered out-of-band by a QPSK modulator. Other systems typically deliver SI out-of-band and inband by the BFS QAM modulator. See Manage Regional Control System for more information.

### Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the BFS QAM modulator basic parameters.
2. Set up the BFS QAM modulator connection to the BFS BIG or DNCS.
3. Activate the BFS QAM modulator.

### You Need to Know

Before You Begin

Before adding a BFS QAM modulator, make sure that you have first added one of the following elements to the DNCS:

- Systems without Direct ASI: First add a BFS BIG to the DNCS.
- Systems with Direct ASI: First add an MPEG BFS source to the DNCS.

**Important:** Before you begin, you must have your network map.

You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- If connecting to a BFS BIG, obtain the following information:
  - Output transport stream ID used by the BFS BIG
  - Slot number where the MSYNC control card is installed on the corresponding BFS BIG (usually, slot 3)
  - Port number on the MSYNC control card or SWIF transmit card that is connected to this QAM modulator (usually, port 1)
- If connecting directly to the ASI card on the DNCS, the output transport stream ID used by the DNCS

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

## Add a BFS QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used for all systems except those that use the RCS option. If your system uses the RCS option, follow a different procedure to set up a BFS QAM modulator for an RCS. A different procedure is required because the RCS option requires system information (SI) to be delivered out-of-band by a QPSK modulator. Other systems typically deliver SI out-of-band and inband by the BFS QAM modulator. See Manage Regional Control System for more information.

### Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the BFS QAM modulator basic parameters.
2. Set up the BFS QAM modulator connection to the BFS BIG or DNCS.
3. Activate the BFS QAM modulator.

### You Need to Know

Before You Begin

Before adding a BFS QAM modulator, make sure that you have first added one of the following elements to the DNCS:

- Systems without Direct ASI: First add a BFS BIG to the DNCS.
- Systems with Direct ASI: First add an MPEG BFS source to the DNCS.

**Important:** Before you begin, you must have your network map.

You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- If connecting to a BFS BIG, obtain the following information:
  - Output transport stream ID used by the BFS BIG
  - Slot number where the MSYNC control card is installed on the corresponding BFS BIG (usually, slot 3)
  - Port number on the MSYNC control card or SWIF transmit card that is connected to this QAM modulator (usually, port 1)
- If connecting directly to the ASI card on the DNCS, the output transport stream ID used by the DNCS

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Setting Up BFS QAM Modulator Basic Parameters

The first step in adding a BFS QAM modulator is to set up the BFS QAM modulator basic parameters. Complete these steps to set up the basic parameters for a BFS QAM modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > QAM**. The Set Up QAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameter Settings - BFS QAM Modulator.

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪ Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪ Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪ If the BFS QAM Modulator connects to a BFS BIG, click the |

| | | |
|---|---|---|
| | **SWIF** option to select the type of card sending BFS data from the BFS BIG to this QAM modulator.<br>▪ If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. | |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. | |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| | **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| | **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| | **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| | **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| | **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

### Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

6.Click **Apply**. The system saves the QAM modulator information you have entered thus far into the DNCS database and enables the Port To Hubs button.

7. Click **Port to Hubs**. The RF Output Port window opens. The Basic Parameters area of this window shows the data that you entered for key RF output fields. The Associated Hubs area shows the hubs that are available to receive content data from this QAM modulator.

8. Make sure the **Selected Hubs** field shows no hub names so that this QAM modulator sends BFS and SI data (DNCS BFS QAM only) to all hubs in the headend.

**Note:** To remove a hub name from the Selected Hubs field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field.

9. Click **Save**. The system saves this information into the DNCS database and closes the RF Output Port window.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

10. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to select one of the following options:

- Set up the connections between the BFS QAM modulator and the BFS BIG (for a DNCS BFS QAM installation)
- Set up the connections for a BFS QAM in an RCS (for an RNCS/LIONN BFS QAM installation)

### Setting Up BFS QAM Modulator Connections

After you set up the basic parameters for a BFS QAM modulator, complete these steps to set up the connections between the BFS QAM modulator and the BFS BIG or the ASI card on the DNCS.

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this QAM modulator.
2. If not already selected, click to select the **Input Port** option in the **QAM Name** area.
3. Complete the fields on the screen as described in Connections Settings - BFS QAM Modulator.

Use the following fields when you manage the connections for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives from the BFS QAM resides. |
| Device Type | Determines the device type that feeds this QAM:<br>▪ If a BFS BIG feeds the BFS QAM, select **BIG**.<br>▪ If an ASI card on the DNCS feeds this BFS QAM, select **ASI**. Select this option if you are using the QAM modulator with an RCS.<br>The option you select determines which parameters display for setup, as described below. |
| Device Name | The name of the device. Valid for either BFS BIG or ASI QAMs. |
| Card Type | The type of card in the BFS BIG.<br>Select **MSYNC SWIF**. |
| Slot Number | The slot number where the MSYNC control card is installed on the BFS BIG (usually, slot 3).<br>Valid for BFS BIG only. |
| Port Number | The port number for the various cards:<br>▪ **For BFS BIG** - control card that is connected to this QAM modulator (usually port 1).<br>▪ **For ASI** - Select the port number on the ASI card that is connected to this BFS QAM modulator. |

#### Related Topics

- Add a BFS QAM
- Setting Up BFS QAM Modulator Connections in an RCS
- BFS QAM Modulator
- BFS QAM Settings

4. Click **Apply**. The system saves this information into the DNCS database.
5. Your next step is to activate the BFS QAM modulator.

### Activating a BFS QAM Modulator

After you set up the connections between the BFS QAM modulator and the device that feeds it, complete these steps to activate the BFS QAM modulator.

**Note:** You can activate a QAM modulator only after all parameters for the QAM modulator have been saved to the DNCS database, and only after the QAM modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
2. At the **Administrative State** field, click the **Online** option.
3. If this BFS QAM modulator will also function as a Distinguished QAM modulator, verify that **Allow SI** is set to **Yes**. If it is not, click and select **Yes**.
4. Click **Save**. The system saves the QAM modulator information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new QAM modulator.
5. Add the new BFS QAM modulator to your network map.
6. Do you need to add another BFS QAM modulator?
   - If **yes**, go back to Setting Up BFS QAM Modulator Basic Parameters.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console. Go to Verifying Your VASP Configuration.

## Modify a BFS QAM Modulator

**Important:** Do not attempt to modify or delete a BFS QAM modulator without assistance from Cisco Services. Certain BFS modifications may degrade system performance. For this reason, always consult Cisco Services before making changes to a BFS QAM modulator.

## Change the BFS QAM Output Frequency

To modify a BFS QAM on your system, complete this procedure during a maintenance window.

**Note**: This procedure is required for each BFS QAM that you want to change.

1. At the BFS QAM front panel, press **Options**, go to **Output Frequency**, and record this frequency in the event you need to restore the original output (channel center) frequency.
2. Press **Options** again, scroll to **Sessions Count**, and record the number of sessions. You will need this number later to verify the restoration of sessions.
3. Press **Options** again, scroll to **Program Count**, and record the number of programs (encrypted sessions). You will need this number later to verify the restoration of programs.
4. At the DNCS administrative console, click the **DNCS** tab.
5. Click the **Network Element Provisioning** tab.
6. Click **QAM**. The **QAM List** window opens.
7. Double-click the QAM you want to modify. The **Set Up QAM** window opens.
8. Select the **Channel Center Frequency** field and type in a unique frequency from the list of recommended modulator frequencies.

   Use the center frequencies shown in the following table to send data from your QAM modulators to the DHCTs on your system. Notice that these frequencies are separated by increments of 6 MHz.

   **Note:** If you are experiencing signal interference, try offsetting your modulator frequencies by 250 kHz from the frequencies shown in the table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 153 | 159 | 165 | 171 | 177 | 183 | 189 | 195 | 201 | 207 |
| 213 | 219 | 225 | 231 | 237 | 243 | 249 | 255 | 261 | 267 |
| 273 | 279 | 285 | 291 | 297 | 303 | 309 | 315 | 321 | 327 |
| 333 | 339 | 345 | 351 | 357 | 363 | 369 | 375 | 381 | 387 |
| 393 | 399 | 405 | 411 | 417 | 423 | 429 | 435 | 441 | 447 |
| 453 | 459 | 465 | 471 | 477 | 483 | 489 | 495 | 501 | 507 |
| 513 | 519 | 525 | 531 | 537 | 543 | 549 | 555 | 561 | 567 |
| 573 | 579 | 585 | 591 | 597 | 603 | 609 | 615 | 621 | 627 |
| 633 | 639 | 645 | 651 | 657 | 663 | 669 | 675 | 681 | 687 |
| 693 | 699 | 705 | 711 | 717 | 723 | 729 | 735 | 741 | 747 |

9. Click **Apply**.
10. Click **Save**. This saves your changes and opens the **QAM List** window.

**Note:** If you experience signal interference, try offsetting your BFS QAM output frequency by 250 KHz from the frequency you chose.

11. Repeat this procedure for the any other BFS QAMs on your system that you need to change.
12. Next you need to reboot the BFS QAM and verify the session and program counts.

### Reboot the BFS QAM and Verify Counts

1. At the **QAM List** window, select the BFS QAM that you changed.
2. To reset this BFS QAM, click **File > Reset**. Resetting the QAM applies the changes you made to the BFS QAM, which then begins transmitting on the unique frequency you entered previously.
3. At the BFS QAM front panel, verify that the session and program counts match the values you recorded earlier (see Change the BFS QAM Output Frequency).

**Note:** If the counts at the BFS QAM front panel do not match the recorded values, stop and contact Cisco Services.

4. At the DNCS, navigate to the **Session Summary** page and tear down the sessions on the BFS QAM.
5. In an **xterm** window, type **clearDbSessions -c** and press **Enter**.
6. Repeat step 3.
7. Repeat this procedure for all of the other BFS QAMs on your system that you changed.
8. Test PPV, xOD, and third party applications and confirm normal set-top behavior before proceeding.

### Related Topics

- BFS QAM Settings
- Add a BFS QAM
- Delete a BFS QAM Modulator

## Delete a BFS QAM Modulator

**Important:** Do not attempt to modify or delete a BFS QAM modulator without assistance from Cisco Services. Certain BFS modifications may degrade system performance. For this reason, always consult Cisco Services before making changes to a BFS QAM modulator.

# VASPs

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

**Important:** This procedure can be used for all systems except those using the RCS option. If your system uses the RCS option, follow a different method to verify the VASP configuration in an RCS. A different method is required because remote sites of an RCS require additional VASP entries.

After you add a BFS QAM modulator, verify that your Value Added Service Provider (VASP) entries are correct. Or, if you are adding a third-party application that needs to negotiate resources with the DNCS, add a VASP entry to the DNCS. Adding a VASP entry in this situation enables the DNCS to communicate with the device that provides third-party application data.

VASP is a generic term for the device that provides a service or functionality to elements on a Digital Broadband Delivery Service (DBDS). For example, if you are offering interactive services such as VOD, you must have one VASP entry for each VOD server installed in your network. Without a VASP entry defined on the DNCS, the DNCS would not be able to process signals to and from the VOD server.

A network may include multiple VASP entries, each providing a unique set of services. However, the following VASP entries are required for any DNCS to successfully provide services to subscribers. These entries are created automatically by the system when your DBDS was initially installed:

- Broadcast File System Used by the BFS when starting its sessions
- CFSession UI Used by the user interface (UI) in the session setup request
- GEARServer Used for EAS activity
- HCTM Server Used for DHCT management
- Message Server Used by the system when sending pass-thru messages (this VASP never starts sessions)
- MMM Server Used for EAS activity
- OSM Server Used for DHCT operating system (OS) sessions

Occasionally, one or more of these entries may be missing or not in service. Therefore, it is a good idea to verify your VASP configuration whenever you make changes to your network.

**Important:** Depending on the services your network offers, there may be more VASP entries listed in the DNCS. However, the seven entries listed above **must** be present **and** in service for the DBDS to function properly. In addition, if you are offering VOD, you must add one VASP entry for each VOD server installed in your network. Without a VASP entry, a DNCS is unable to process signals to and from the VOD server.

## What do you want to do?

- Verify your VASP configuration
- View VASP settings
- Add a VASP entry
- Activate a VASP entry
- Modify a VASP entry
- Delete a VASP entry

## Verifying Your VASP Configuration

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Verify that the following VASP entries appear in the VASP List window and that they show a status of **In Service**.

| VASP Entry Name | IP Address | Status |
|---|---|---|
| Broadcast File System | 10.253.0.1 | In Service |
| CF Session UI | 10.253.0.1 | In Service |
| GEARServer | 10.253.0.1 | In Service |
| HCTM Server | 10.253.0.1 | In Service |
| Message Server | 10.253.0.1 | In Service |
| MMM Server | 10.253.0.1 | In Service |
| OSM Server | 10.253.0.1 | In Service |

5. **Note:** All of the VASP entries in the preceding table connect to the same IP address. These are the system default values. Your IP address entries may be different based on your system configuration. Check your network map to verify the IP addresses for your VASP entries.

6. Do all seven VASP entries appear in the VASP List window as shown in step 4, **and** do they all show a status of **In Service**?
   - If **yes**, go to step 6.
   - If **no**, go to step 7.
7. Do you need to add any VASP entries, such as for a VOD server?
   - If **yes**, go to Adding a VASP Entry.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.
8. Are any of these seven VASP entries missing from the VASP List window?
   - If **yes**, go to Adding a VASP Entry.
   - If **no**, go to step 8.
9. Do any of these seven VASP entries have a status other than **In Service**?
   - If **yes**, go to Activating a VASP Entry.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.

# VASP Settings

Use the Set Up VASP page to manage the VASP entries in your network.

## VASP Entry Fields

Use the following fields when you manage VASP entries in the DNCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.<br>**Example:** You might give a VASP entry associated with a VOD service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with a VOD service. |
| Name | The name of this VASP entry. You can use up to 80 alphanumeric characters.<br>Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br>**Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated. Select **In Service** to activate this VASP. |

## Related Topics

- Verifying Your VASP Configuration
- Add a VASP Entry
- Activating a VASP Entry
- Modifying a VASP Entry
- Deleting a VASP Entry

### VASP Entry Fields

Use the following fields when you manage VASP entries in the DNCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br><br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.<br><br>**Example:** You might give a VASP entry associated with a VOD service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with a VOD service. |
| Name | The name of this VASP entry. You can use up to 80 alphanumeric characters.<br><br>Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br><br>**Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br><br>Be careful to properly place the dots (.) between numbers.<br><br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated. Select **In Service** to activate this VASP. |

## Add a VASP Entry

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > File > New**

Complete these steps if you need to add a VASP entry to a DBDS that does not use RCS. For more descriptive information about VASP entries, refer to Verifying Your VASP Configuration.

**Note:** Systems using RCS follow a different method to add a VASP entry to the RCS.

**Important:** If you are offering VOD services, you must add one VASP entry for each VOD server installed in your network. Without a VASP entry, the DNCS will not be able to process signals to and from the server.

### You Need to Know

Before You Begin

Before you begin, you must have the IP address of the server associated with the VASP entry you are adding (from your system administrator).

### Adding a VASP Entry

1. On the VASP List window, click **File > New**. The Set Up VASP window opens.
2. Complete the fields on the screen as described in VASP Entry Fields.

Use the following fields when you manage VASP entries in the DNCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.<br>**Example:** You might give a VASP entry associated with a VOD service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with a VOD service. |
| Name | The name of this VASP entry. You can use up to 80 alphanumeric characters.<br>Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br>**Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing |

| | |
|---|---|
| | the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated. Select **In Service** to activate this VASP. |

3. Click **Save**. The system saves the VASP entry information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.
4. Add the new VASP entry information to your network map.
5. Do you need to add another VASP entry?
   - If **yes**, repeat steps this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.

## Add a VASP Entry

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > File > New**

Complete these steps if you need to add a VASP entry to a DBDS that does not use RCS. For more descriptive information about VASP entries, refer to Verifying Your VASP Configuration.

**Note:** Systems using RCS follow a different method to add a VASP entry to the RCS.

**Important:** If you are offering VOD services, you must add one VASP entry for each VOD server installed in your network. Without a VASP entry, the DNCS will not be able to process signals to and from the server.

### You Need to Know

Before You Begin

Before you begin, you must have the IP address of the server associated with the VASP entry you are adding (from your system administrator).

### Adding a VASP Entry

1. On the VASP List window, click **File > New**. The Set Up VASP window opens.
2. Complete the fields on the screen as described in VASP Entry Fields.

Use the following fields when you manage VASP entries in the DNCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.<br>**Example:** You might give a VASP entry associated with a VOD service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with a VOD service. |
| Name | The name of this VASP entry. You can use up to 80 alphanumeric characters.<br>Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br>**Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing |

| | |
|---|---|
| | the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated. Select **In Service** to activate this VASP. |

3. Click **Save**. The system saves the VASP entry information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.
4. Add the new VASP entry information to your network map.
5. Do you need to add another VASP entry?
   - If **yes**, repeat steps this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.

## Activating a VASP Entry

Occasionally, a VASP entry is taken out of service, such as during maintenance or when you change VOD server brands (for example, replacing an nCube VOD server with a Concurrent VOD server). Use this procedure to place a VASP entry back into service that had been previously taken out of service.

1. On the VASP List window, click to select the VASP you need to place in service.
2. Click **File > Open**. The Set Up VASP window for that VASP opens.
3. Click the **In Service** option.
4. Click **Save**. The system places the VASP into service. The Set Up VASP window closes and the VASP List window updates to show the changed status for this VASP.
5. Do you need to activate another VASP?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.

## Modify a VASP Entry

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Open**

After a VASP entry has been saved in the DNCS, you can modify only the name of the VASP entry and its status of In Service or Out of Service. To change any other parameters, you must delete the VASP entry, and then re-add it to the DNCS, using the new information.

### Modifying a VASP Entry

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Click once on the row containing the VASP entry you want to modify.
5. Click **File > Open**. The Set Up VASP window opens for the VASP entry you selected.
6. To change the name of this VASP entry, click in the **Name** field and change the name as desired. You can use up to 80 alphanumeric characters.

   **Note:** We recommend that you establish a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.

   **Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43.

7. To change the status of this VASP entry from **In Service** to **Out of Service**, or vice versa, click the desired option so that it is selected (**yellow**).
8. When you finish making changes, click **Save**. The system saves the new VASP information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP information.
9. Update your network map to reflect these changes.
10. Do you need to modify another VASP entry?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.

### Related Topics

- Verifying Your VASP Configuration
- VASP Settings
- Add a VASP Entry
- Activating a VASP Entry
- Deleting a VASP Entry

### Modifying a VASP Entry

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Click once on the row containing the VASP entry you want to modify.
5. Click **File > Open**. The Set Up VASP window opens for the VASP entry you selected.
6. To change the name of this VASP entry, click in the **Name** field and change the name as desired. You can use up to 80 alphanumeric characters.

   **Note:** We recommend that you establish a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.

   **Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43.

7. To change the status of this VASP entry from **In Service** to **Out of Service**, or vice versa, click the desired option so that it is selected (**yellow**).
8. When you finish making changes, click **Save**. The system saves the new VASP information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP information.
9. Update your network map to reflect these changes.
10. Do you need to modify another VASP entry?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.

# Delete a VASP Entry

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Delete**

Use this procedure to delete a VASP entry from the DNCS.

### Deleting a VASP Entry

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Click once on the row containing the VASP entry you want to delete.
5. Click **File > Delete.** A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the VASP entry from the DNCS database and from the VASP List window.
7. Delete the VASP entry from your network map.
8. Do you need to delete another VASP entry?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.

### Related Topics

- Verifying Your VASP Configuration
- VASP Settings
- Add a VASP Entry
- Activating a VASP Entry
- Modifying a VASP Entry

### Deleting a VASP Entry

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Click once on the row containing the VASP entry you want to delete.
5. Click **File > Delete.** A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the VASP entry from the DNCS database and from the VASP List window.
7. Delete the VASP entry from your network map.
8. Do you need to delete another VASP entry?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.

# BFS BIG

If your DNCS has no ASI card, the first step in setting up the elements that process system data for your network is to add a BFS BIG. A BFS BIG (sometimes called a data BIG) takes the data it receives from the DNCS and generates an MPEG transport stream that the BFS BIG then sends to the BFS QAM modulator.

In addition to providing BFS data to DHCTs, your system must also deliver SI data to DHCTs. Systems that do not use the RCS option deliver SI both inband (by a QAM modulator) and out-of-band (by a QPSK modulator). To deliver SI data to all DHCTs, you must establish (distinguish) one QAM modulator per headend to carry inband SI data to all the DHCTs on that headend. This QAM modulator is called the Distinguished QAM. Any QAM modulator that is online (active) and not assigned to a specific hub is a candidate for a Distinguished QAM modulator. We recommend that you set up your BFS QAM modulator to also be the Distinguished QAM. However, if you are using an MQAM modulator to carry BFS data, you will need to distinguish a QAM modulator to carry SI data. Only a QAM modulator can become a Distinguished QAM modulator.

**Important:** If your DNCS has an ASI card, do not add a BFS BIG to the DNCS. Instead, add an MPEG BFS source for the ASI card, and then connect the ASI card directly to the BFS QAM modulator.

**Note:** The data traveling through the BFS BIG to the BFS QAM modulator is for system information and configuration purposes only and does not contain audio and video program data. However, you can configure a BIG to also process audio and video data by installing a single-wire interface (SWIF) Receive card. The BIG comes with a SWIF Transmit card already installed.

### Related Topics

- Review settings for the BFS BIG
- Add a BFS BIG
- Modify a BFS BIG
- Delete a BFS BIG

## BFS BIG Settings

Use the Set Up BIG page to manage the BFS BIGs in your network. Three tabs in this window provide settings for the BFS BIG:

- Basic Parameters fields
- Card fields

### Basic Parameter Settings - BFS BIG

Use the following fields when you manage the basic parameters for a BFS BIG.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS BIG resides. |
| BIG Name | The name you will use to identify this BFS BIG.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map (for example, **HE1_BFSBIG**). |
| Administrative State | Determines the availability of the BFS BIG.<br>Set the BFS BIG to one of the following states:<br>▪**Online** - The BFS BIG receives, processes, and transmits data<br>▪**Offline** - The BFS BIG does not receive, process, or transmit data |
| Slot Number | The slot number where the MSYNC control card is physically installed in this BFS BIG.<br>We recommend that the MSYNC control card be installed in slot 3. Make your selection based on where your MSYNC control card is actually installed. |
| IP Address | The IP address for the MSYNC control card installed in this BFS BIG.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the Ethernet port being used on the MSYNC control card installed in the BFS BIG.<br>There are two MAC addresses for the MSYNC control card - one for each Ethernet port. Make sure you type the MAC address for the Ethernet port being used to receive data from the DNCS. |
| Subnet Mask | The subnet mask where the MSYNC control card resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, check with your network administrator for the proper mask. |
| Output Mode | The type of output the BFS BIG uses.<br>Select either the **SWIF** or **ASI** option.<br>Base your selection on which type of output interface connection is on the back of the MSYNC control card that is installed in this BFS BIG. |
| Output Transport Stream ID | A unique number to identify the transport stream going from the output interface connection on the MSYNC control card.<br>You can use up to 5 numeric characters.<br>**Example:** If this BFS BIG is associated with Headend 1, and data is going out through the MSYNC control card on port 3, you might type **131** for the transport stream ID. You can use up to 5 numeric characters.<br>**Notes:**<br>Be sure to use a number that is consistent with the numbering scheme used |

on your network map.

If the corresponding BFS QAM modulator is not connected to a SWIF transmit card, you will need the Output Transport Stream ID when you set up the modulator.

If necessary, change the PID (program ID) assignments to each stream by clicking PAT Configuration. These assignments are typically made when your system is upgraded and should not be altered unless you are adding a third-party application. For assistance supporting third-party applications, refer to Supporting a Third-Party Application.

### BFS BIG Card Settings

Use the following fields when you manage a BFS BIG card in the DNCS.

| Field | Description |
|---|---|
| Card Type | The type of card you are adding. |
| Slot Number | The slot number of the card you are adding.<br>Verify that the slot number is correct. If not, click **Slot Number**, and then select the correct slot from the list that appears.<br>**Important:** You must base your slot number selection on where cards are actually installed in the BIG. However, We recommend the following slot number assignments for each card type:<br>▪SWIF Receive Card Slot 6<br>▪OC3 ATM Card Slot 5<br>▪SWIF Transmit Card Slot 4 |
| Port | The receive and transmit ports for the SWIF cards:<br>▪**SWIF Receive card** - Type a unique number to identify the transport stream coming into the SWIF Receive card through that port.<br>▪**SWIF Transmit card** - Type a unique number to identify the transport stream going from the SWIF Transmit card through that port.<br>You can use up to 5 numeric characters in either case.<br>You do not need to define every port only the ports that actually send or receive data. Be sure to use a number that is consistent with the numbering scheme used on your network map. |

## Add a BFS BIG

Before adding a BFS QAM modulator, make sure that you have first added one of the following elements to the DNCS:

- **Systems without Direct ASI:** First add a BFS BIG to the DNCS. Each headend in your network must have a BFS QAM modulator associated with a BFS BIG. In addition, each headend in your network must also have a Distinguished QAM modulator. Otherwise, some DHCTs in your network will not receive BFS and SI data for that headend.
- **Systems with Direct ASI:** First add an MPEG BFS source to the DNCS. Each headend in your network must have a BFS QAM modulator associated with an ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

**Adding a BFS BIG**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > BIG > File > New**

Be sure to allow yourself adequate time to complete this procedure. To add a BFS BIG to the DNCS, you must complete the following tasks in order. For step-by-step instructions for a particular task, click on that task.

1. Set up the BFS BIG parameters.
2. Set up the cards installed in the BFS BIG.
3. Set up the connections from the BFS BIG to various devices.
4. Disconnect any devices previously connected to the BFS BIG that are no longer appropriate.

**Note:** For assistance disconnecting devices from the BFS BIG, consult Cisco Services.

## Add a BFS BIG

Before adding a BFS QAM modulator, make sure that you have first added one of the following elements to the DNCS:

- **Systems without Direct ASI:** First add a BFS BIG to the DNCS. Each headend in your network must have a BFS QAM modulator associated with a BFS BIG. In addition, each headend in your network must also have a Distinguished QAM modulator. Otherwise, some DHCTs in your network will not receive BFS and SI data for that headend.
- **Systems with Direct ASI:** First add an MPEG BFS source to the DNCS. Each headend in your network must have a BFS QAM modulator associated with an ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

**Adding a BFS BIG**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > BIG > File > New**

Be sure to allow yourself adequate time to complete this procedure. To add a BFS BIG to the DNCS, you must complete the following tasks in order. For step-by-step instructions for a particular task, click on that task.

1. Set up the BFS BIG parameters.
2. Set up the cards installed in the BFS BIG.
3. Set up the connections from the BFS BIG to various devices.
4. Disconnect any devices previously connected to the BFS BIG that are no longer appropriate.

**Note:** For assistance disconnecting devices from the BFS BIG, consult Cisco Services.

### Setting Up BFS BIG Parameters

The first step in adding a BFS BIG to the DNCS is setting up the parameters for the BFS BIG.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **BIG**. The BIG List window opens.
4. Click **File > New**. The Set Up BIG window opens with the BIG tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameter Settings - BFS BIG.

Use the following fields when you manage the basic parameters for a BFS BIG.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS BIG resides. |
| BIG Name | The name you will use to identify this BFS BIG.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map (for example, **HE1_BFSBIG**). |
| Administrative State | Determines the availability of the BFS BIG.<br>Set the BFS BIG to one of the following states:<br>▪ **Online** - The BFS BIG receives, processes, and transmits data<br>▪ **Offline** - The BFS BIG does not receive, process, or transmit data |
| Slot Number | The slot number where the MSYNC control card is physically installed in this BFS BIG.<br>We recommend that the MSYNC control card be installed in slot 3. Make your selection based on where your MSYNC control card is actually installed. |
| IP Address | The IP address for the MSYNC control card installed in this BFS BIG.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the Ethernet port being used on the MSYNC control card installed in the BFS BIG.<br>There are two MAC addresses for the MSYNC control card - one for each Ethernet port. Make sure you type the MAC address for the Ethernet port being used to receive data from the DNCS. |
| Subnet Mask | The subnet mask where the MSYNC control card resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, check with your network administrator for the proper mask. |
| Output Mode | The type of output the BFS BIG uses.<br>Select either the **SWIF** or **ASI** option.<br>Base your selection on which type of output interface connection is on the back of the MSYNC control card that is installed in this BFS BIG. |

| | |
|---|---|
| Output Transport Stream ID | A unique number to identify the transport stream going from the output interface connection on the MSYNC control card.<br><br>You can use up to 5 numeric characters.<br><br>**Example:** If this BFS BIG is associated with Headend 1, and data is going out through the MSYNC control card on port 3, you might type **131** for the transport stream ID. You can use up to 5 numeric characters.<br><br>**Notes:**<br><br>Be sure to use a number that is consistent with the numbering scheme used on your network map.<br><br>If the corresponding BFS QAM modulator is not connected to a SWIF transmit card, you will need the Output Transport Stream ID when you set up the modulator.<br><br>If necessary, change the PID (program ID) assignments to each stream by clicking PAT Configuration. These assignments are typically made when your system is upgraded and should not be altered unless you are adding a third-party application. For assistance supporting third-party applications, refer to Supporting a Third-Party Application. |

6. Click **Apply**. The system saves the BFS BIG information you have entered into the DNCS database.
7. Your next step is to set up the cards installed in the BFS BIG. Go to Setting Up BFS BIG Cards.

### Setting Up BFS BIG Cards

After you set up the BFS BIG parameters, the MSYNC control card is set up in the DNCS database. Complete these steps to set up any OC3 ATM or SWIF cards that are also installed in the BFS BIG.

1. On the Set Up BIG window, click the **Cards** tab. The Cards window opens with an illustration of the BFS BIG with the MSYNC control card in the slot you selected on the BIG tab (usually, slot 3).

   **Note:** The slots are numbered 1 through 6 from the bottom to the top of the BIG chassis.

2. Point to the empty slot on the graphic that corresponds to the slot where the card you want to set up is physically installed in the BIG chassis.
3. Click the right mouse button and select **New** from the menu. The Card Type window opens.
4. Click **Card Type** and select the type of card you are adding.
5. Click **OK**. The Set Up XXX Card window opens (XXX = the card type you selected).
6. Complete the fields on the screen as described in BFS BIG Card Settings.

   Use the following fields when you manage a BFS BIG card in the DNCS.

| Field | Description |
|---|---|
| Card Type | The type of card you are adding. |
| Slot Number | The slot number of the card you are adding.<br>Verify that the slot number is correct. If not, click **Slot Number**, and then select the correct slot from the list that appears.<br>**Important:** You must base your slot number selection on where cards are actually installed in the BIG. However, We recommend the following slot number assignments for each card type:<br>▪ SWIF Receive Card Slot 6<br>▪ OC3 ATM Card Slot 5<br>▪ SWIF Transmit Card Slot 4 |
| Port | The receive and transmit ports for the SWIF cards:<br>▪ **SWIF Receive card** - Type a unique number to identify the transport stream coming into the SWIF Receive card through that port.<br>▪ **SWIF Transmit card** - Type a unique number to identify the transport stream going from the SWIF Transmit card through that port.<br>You can use up to 5 numeric characters in either case.<br>You do not need to define every port only the ports that actually send or receive data. Be sure to use a number that is consistent with the numbering scheme used on your network map. |

7. Click **Save**. The system saves the card information in the DNCS database and closes the Set Up XXX Card window. The Set Up BIG window updates to include the new card.
8. Do you need to add information about another card type installed in this BFS BIG?
   - If **yes**, repeat this procedure.
   - If **no**, click **Apply**. The system saves the BFS BIG information you have entered thus far into the DNCS database. Go to Setting Up BFS BIG Connections.

### Setting Up BFS BIG Connections

After you set up the cards that are installed in the BFS BIG, complete these steps to set up the connections between the BFS BIG and other devices.

1. On the Set Up BIG window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this BIG.
2. In the table under the **BIG Name** field locate the card you set up on the Cards tab. Note that the Ports column represents the available output ports on that card as boxes.
3. Click on the box for the output port on the card through which the BIG is connected. A check mark appears in the box, and the box changes to **yellow**.
4. In the **Connect To** area, click the arrow next to each option to define the input port on the device connected to the BIG through the card you selected.

   **Note:** These options will vary depending on the type of card you selected.

5. Click **Apply**. The port box you checked in the table under BIG Name changes to **green** to show that the port is connected. In addition, the device to which that port is connected appears in the illustration.
6. Do you need to establish connectivity for another card installed in this BIG?
   - If **yes**, repeat this procedure from step 2.
   - If **no**, go to step 7.
7. Are there devices currently connected to this BIG that are no longer appropriate?
   - If **yes**, go to Disconnecting Devices from a BFS BIG.
   - If **no**, click **Save**. The system saves the BIG information in the DNCS database and closes the Set Up BIG window. The BIG List window updates to include the new BIG.
8. Add this BFS BIG to your network map.
9. Click **File > Close** to close the BIG List window and return to the DNCS Administrative Console.
10. Your next step is to add the BFS QAM modulator that is connected to this BFS BIG. Go to Add a BFS QAM.

## Modify a BIG

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > BIG > [BIG Name] > File > Open**

After a BIG has been saved in the DNCS, you can modify any of its parameters, except for the headend to which it is assigned.

### Modifying a BIG

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **BIG**. The BIG List window opens.
4. Click once on the row containing the BIG you want to modify.
5. Click **File > Open**. The Set Up BIG window opens for the BIG you selected.
6. Make changes to the fields as described in Basic Parameters - BFS BIG and BFS BIG Card Fields.

Use the following fields when you manage a BFS BIG card in the DNCS.

| Field | Description |
|---|---|
| Card Type | The type of card you are adding. |
| Slot Number | The slot number of the card you are adding.<br>Verify that the slot number is correct. If not, click **Slot Number**, and then select the correct slot from the list that appears.<br>**Important:** You must base your slot number selection on where cards are actually installed in the BIG. However, We recommend the following slot number assignments for each card type:<br>▪ SWIF Receive Card Slot 6<br>▪ OC3 ATM Card Slot 5<br>▪ SWIF Transmit Card Slot 4 |
| Port | The receive and transmit ports for the SWIF cards:<br>▪ **SWIF Receive card** - Type a unique number to identify the transport stream coming into the SWIF Receive card through that port.<br>▪ **SWIF Transmit card** - Type a unique number to identify the transport stream going from the SWIF Transmit card through that port.<br>You can use up to 5 numeric characters in either case.<br>You do not need to define every port only the ports that actually send or receive data. Be sure to use a number that is consistent with the numbering scheme used on your network map. |
| Use the following fields when you manage the basic parameter | **Description** |

s for a
BFS BIG.

| Field | |
|---|---|
| Headend Name | The headend in which this BFS BIG resides. |
| BIG Name | The name you will use to identify this BFS BIG.<br><br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map (for example, **HE1_BFSBIG**). |
| Administrative State | Determines the availability of the BFS BIG.<br><br>Set the BFS BIG to one of the following states:<br><br>▪ **Online** - The BFS BIG receives, processes, and transmits data<br>▪ **Offline** - The BFS BIG does not receive, process, or transmit data |
| Slot Number | The slot number where the MSYNC control card is physically installed in this BFS BIG.<br><br>We recommend that the MSYNC control card be installed in slot 3. Make your selection based on where your MSYNC control card is actually installed. |
| IP Address | The IP address for the MSYNC control card installed in this BFS BIG.<br><br>Be careful to properly place the dots (.) between numbers.<br><br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the Ethernet port being used on the MSYNC control card installed in the BFS BIG.<br><br>There are two MAC addresses for the MSYNC control card - one for each Ethernet port. Make sure you type the MAC address for the Ethernet port being used to receive data from the DNCS. |
| Subnet Mask | The subnet mask where the MSYNC control card resides.<br><br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, check with your network administrator for the proper mask. |
| Output Mode | The type of output the BFS BIG uses.<br><br>Select either the **SWIF** or **ASI** option.<br><br>Base your selection on which type of output interface connection is on the back of the MSYNC control card that is installed in this BFS BIG. |
| Output Transport Stream ID | A unique number to identify the transport stream going from the output interface connection on the MSYNC control card.<br><br>You can use up to 5 numeric characters.<br><br>**Example:** If this BFS BIG is associated with Headend 1, and data is going out through the MSYNC control card on port 3, you might type **131** for the transport stream ID. You can use up to 5 numeric characters.<br><br>**Notes:**<br><br>Be sure to use a number that is consistent with the numbering scheme used on your network map. |

If the corresponding BFS QAM modulator is not connected to a SWIF transmit card, you will need the Output Transport Stream ID when you set up the modulator.

If necessary, change the PID (program ID) assignments to each stream by clicking PAT Configuration. These assignments are typically made when your system is upgraded and should not be altered unless you are adding a third-party application. For assistance supporting third-party applications, refer to Supporting a Third-Party Application.

**Note:** If you would like to save your changes to the database without closing the window, you can click **Apply** at any time.

7. When you finish making changes, click **Save**. The system saves the new BIG information in the DNCS database and closes the Set Up BIG window. The BIG List window updates to include the new BIG information.

8. Update your network map to reflect these changes.

9. Do you need to modify another BIG?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **File > Close** to close the BIG List window and return to the DNCS Administrative Console.

## Modify a BIG

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > BIG > [BIG Name] > File > Open**

After a BIG has been saved in the DNCS, you can modify any of its parameters, except for the headend to which it is assigned.

### Modifying a BIG

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **BIG**. The BIG List window opens.
4. Click once on the row containing the BIG you want to modify.
5. Click **File > Open**. The Set Up BIG window opens for the BIG you selected.
6. Make changes to the fields as described in Basic Parameters - BFS BIG and BFS BIG Card Fields.

Use the following fields when you manage a BFS BIG card in the DNCS.

| Field | Description |
|---|---|
| Card Type | The type of card you are adding. |
| Slot Number | The slot number of the card you are adding.<br>Verify that the slot number is correct. If not, click **Slot Number**, and then select the correct slot from the list that appears.<br>**Important:** You must base your slot number selection on where cards are actually installed in the BIG. However, We recommend the following slot number assignments for each card type:<br>▪ SWIF Receive Card Slot 6<br>▪ OC3 ATM Card Slot 5<br>▪ SWIF Transmit Card Slot 4 |
| Port | The receive and transmit ports for the SWIF cards:<br>▪ **SWIF Receive card** - Type a unique number to identify the transport stream coming into the SWIF Receive card through that port.<br>▪ **SWIF Transmit card** - Type a unique number to identify the transport stream going from the SWIF Transmit card through that port.<br>You can use up to 5 numeric characters in either case.<br>You do not need to define every port only the ports that actually send or receive data. Be sure to use a number that is consistent with the numbering scheme used on your network map. |
| Use the following fields when you manage the basic parameter | **Description** |

s for a
BFS BIG.

| Field | |
|---|---|
| Headend Name | The headend in which this BFS BIG resides. |
| BIG Name | The name you will use to identify this BFS BIG.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map (for example, **HE1_BFSBIG**). |
| Administrative State | Determines the availability of the BFS BIG.<br>Set the BFS BIG to one of the following states:<br>▪ **Online** - The BFS BIG receives, processes, and transmits data<br>▪ **Offline** - The BFS BIG does not receive, process, or transmit data |
| Slot Number | The slot number where the MSYNC control card is physically installed in this BFS BIG.<br>We recommend that the MSYNC control card be installed in slot 3. Make your selection based on where your MSYNC control card is actually installed. |
| IP Address | The IP address for the MSYNC control card installed in this BFS BIG.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the Ethernet port being used on the MSYNC control card installed in the BFS BIG.<br>There are two MAC addresses for the MSYNC control card - one for each Ethernet port. Make sure you type the MAC address for the Ethernet port being used to receive data from the DNCS. |
| Subnet Mask | The subnet mask where the MSYNC control card resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, check with your network administrator for the proper mask. |
| Output Mode | The type of output the BFS BIG uses.<br>Select either the **SWIF** or **ASI** option.<br>Base your selection on which type of output interface connection is on the back of the MSYNC control card that is installed in this BFS BIG. |
| Output Transport Stream ID | A unique number to identify the transport stream going from the output interface connection on the MSYNC control card.<br>You can use up to 5 numeric characters.<br>**Example:** If this BFS BIG is associated with Headend 1, and data is going out through the MSYNC control card on port 3, you might type **131** for the transport stream ID. You can use up to 5 numeric characters.<br>**Notes:**<br>Be sure to use a number that is consistent with the numbering scheme used on your network map. |

If the corresponding BFS QAM modulator is not connected to a SWIF transmit card, you will need the Output Transport Stream ID when you set up the modulator.

If necessary, change the PID (program ID) assignments to each stream by clicking PAT Configuration. These assignments are typically made when your system is upgraded and should not be altered unless you are adding a third-party application. For assistance supporting third-party applications, refer to Supporting a Third-Party Application.

**Note:** If you would like to save your changes to the database without closing the window, you can click **Apply** at any time.

7. When you finish making changes, click **Save**. The system saves the new BIG information in the DNCS database and closes the Set Up BIG window. The BIG List window updates to include the new BIG information.

8. Update your network map to reflect these changes.

9. Do you need to modify another BIG?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **File > Close** to close the BIG List window and return to the DNCS Administrative Console.

## Delete a BIG

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > BIG > [BIG Name] > File > Delete**

**Note:** If there are any QAM or MQAM modulators connected to a BIG when you delete it, the system automatically deactivates them by placing them off-line. However, the QAM or MQAM modulator information stays in the DNCS database.

### Deleting a BIG

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **BIG**. The BIG List window opens.
4. Click once on the row containing the BIG you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the BIG information from the DNCS database and from the BIG List window. If there were any QAM or MQAM modulators connected to this BIG, the system automatically deactivates them by placing them off-line. However, the QAM or MQAM modulator information remains in the DNCS database.
7. Delete the BIG from your network map.
8. Do you need to delete another BIG?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the BIG List window and return to the DNCS Administrative Console.

## Delete a BIG

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > BIG > [BIG Name] > File > Delete**

**Note:** If there are any QAM or MQAM modulators connected to a BIG when you delete it, the system automatically deactivates them by placing them off-line. However, the QAM or MQAM modulator information stays in the DNCS database.

### Deleting a BIG

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **BIG**. The BIG List window opens.
4. Click once on the row containing the BIG you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the BIG information from the DNCS database and from the BIG List window. If there were any QAM or MQAM modulators connected to this BIG, the system automatically deactivates them by placing them off-line. However, the QAM or MQAM modulator information remains in the DNCS database.
7. Delete the BIG from your network map.
8. Do you need to delete another BIG?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the BIG List window and return to the DNCS Administrative Console.

### Disconnecting Devices from a BFS BIG

After you physically disconnect a device from a BFS BIG, complete these steps to record that change in the DNCS database.

1. On the Connectivity tab of the Set Up BIG window, in the table under the **BIG Name** field, locate the card connected to the device that you need to disconnect.
2. Click on the box for the output port of the card that connects the BIG to the device you are disconnecting. A check mark appears in the box, and the box changes to **yellow**.
3. In the **Connect To** area, click the **Device Type** arrow, and then select **none** from the menu.
4. Click **Apply**. The system removes that connection information from the DNCS database. In addition, the device to which that port was connected disappears from the illustration.
5. Do you need to disconnect another device from this BIG?
   - If **yes**, repeat this procedure.
   - If **no**, click **Save**. The system saves the BIG information in the DNCS database and closes the Set Up BIG window. The BIG List window updates to include the new BIG.
6. Record these changes on your network map.
7. Click **File > Close** to close the BIG List window and return to the DNCS Administrative Console.
8. Is this a new BFS BIG?
   - If **yes**, go to Add a BFS QAM.
   - If **no**, continue with any other changes that you need to make to your network.

# ATM PVC Maps

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > ATM PVC > File > New**

After you are certain that your VASP configuration is correct and if your network uses a BFS BIG, you are ready to add an ATM PVC map. ATM PVCs carry VASP data from the machine where the data resides, through the ATM switch, and to the BFS BIG. The BFS BIG terminates the PVC, processes the data, and sends it to the BFS QAM for delivery to DHCTs.

**Important:** Systems that use the Direct ASI option do not need ATM PVC maps. ATM PVC maps are used only in systems that use a BFS BIG.

## What do you want to do?

- Review ATM PVC settings
- Add an ATM PVC map
- Modify an ATM PVC map
- Delete an ATM PVC map

## ATM PVC Settings

Use the Set Up ATM PVC Map page to manage the ATM PVC maps in your network.

Use the following fields when you manage an ATM PVC map in the DNCS.

| Field | Description |
|---|---|
| Description | A description for this ATM PVC map.<br><br>**Example:** ChicagoPVC.<br><br>You can use up to 20 alphanumeric characters. |
| VASP Name | The name of the VASP type.<br><br>Select **Broadcast File System** to configure the map to support each of the VASPs associated with the BFS BIG. |
| VASP VPI | The virtual path indicator for the VASP.<br><br>Type **0** (numeral zero). |
| VASP Port Number | The port number of the VASP.<br><br>Type **1** (numeral one). |
| BIG Name | The BIG associated with this ATM PVC map. |
| ATM Card Slot Number | The slot number where the ATM card is installed in the BIG. |
| ATM Card VPI | The virtual path indicator for the ATM card.<br><br>Type **1** to identify the data path. |
| Bandwidth | The bandwidth of the map.<br><br>Type **30**. |

## Add an ATM PVC Map

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **ATM PVC**. The ATM PVC Map List window opens.
4. Click **File > New**. The Set Up ATM PVC Map window opens.
5. Complete the fields on the screen as described in ATM PVC Map Fields .

Use the following fields when you manage an ATM PVC map in the DNCS.

| Field | Description |
|---|---|
| Description | A description for this ATM PVC map.<br><br>**Example:** ChicagoPVC.<br><br>You can use up to 20 alphanumeric characters. |
| VASP Name | The name of the VASP type.<br><br>Select **Broadcast File System** to configure the map to support each of the VASPs associated with the BFS BIG. |
| VASP VPI | The virtual path indicator for the VASP.<br><br>Type **0** (numeral zero). |
| VASP Port Number | The port number of the VASP.<br><br>Type **1** (numeral one). |
| BIG Name | The BIG associated with this ATM PVC map. |
| ATM Card Slot Number | The slot number where the ATM card is installed in the BIG. |
| ATM Card VPI | The virtual path indicator for the ATM card.<br><br>Type **1** to identify the data path. |
| Bandwidth | The bandwidth of the map.<br><br>Type **30**. |

6. Click **Save**. The system saves the ATM PVC map information in the DNCS database and closes the Set Up ATM PVC Map window. The ATM PVC Map List window updates to include the new ATM PVC map.
7. Add the new ATM PVC map to your network map.
8. Click **File > Close** to close the Set Up ATM PVC Map window and return to the DNCS Administrative Console.

9. Are you setting up your network for the first time?

- If **yes**, go to Setting Up Two-Way Communication.
- If **no**, continue making any other changes that you need to make to your network. When finished, update your network map with the changes.

## Modify an ATM PVC Map

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > ATM PVC > [ATM PVC Map Name] > File > Open**

After an ATM PVC map has been saved in the DNCS, you can modify any of its parameters.

### Modifying an ATM PVC Map

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **ATM PVC**. The ATM PVC Map List window opens.
4. Click once on the row containing the ATM PVC map you want to modify.
5. Click **File > Open**. The Set Up ATM PVC Map window opens for the ATM PVC map you selected.
6. Make changes to the fields as described in ATM PVC Map Fields .

Use the following fields when you manage an ATM PVC map in the DNCS.

| Field | Description |
|---|---|
| Description | A description for this ATM PVC map.<br><br>**Example:** ChicagoPVC.<br><br>You can use up to 20 alphanumeric characters. |
| VASP Name | The name of the VASP type.<br><br>Select **Broadcast File System** to configure the map to support each of the VASPs associated with the BFS BIG. |
| VASP VPI | The virtual path indicator for the VASP.<br><br>Type **0** (numeral zero). |
| VASP Port Number | The port number of the VASP.<br><br>Type **1** (numeral one). |
| BIG Name | The BIG associated with this ATM PVC map. |
| ATM Card Slot Number | The slot number where the ATM card is installed in the BIG. |
| ATM Card VPI | The virtual path indicator for the ATM card.<br><br>Type **1** to identify the data path. |
| Bandwidth | The bandwidth of the map. |

Type **30**.

7. When you finish making changes, click **Save**. The system saves the new ATM PVC map information in the DNCS database and closes the Set Up ATM PVC map window. The ATM PVC Map List window updates to include the new ATM PVC map information.

8. Update your network map to reflect these changes.

9. Do you need to modify another ATM PVC map?

   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the ATM PVC Map List window and return to the DNCS Administrative Console.

## Modify an ATM PVC Map

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > ATM PVC > [ATM PVC Map Name] > File > Open**

After an ATM PVC map has been saved in the DNCS, you can modify any of its parameters.

### Modifying an ATM PVC Map

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **ATM PVC**. The ATM PVC Map List window opens.
4. Click once on the row containing the ATM PVC map you want to modify.
5. Click **File > Open**. The Set Up ATM PVC Map window opens for the ATM PVC map you selected.
6. Make changes to the fields as described in ATM PVC Map Fields .

Use the following fields when you manage an ATM PVC map in the DNCS.

| Field | Description |
|---|---|
| Description | A description for this ATM PVC map.<br><br>**Example:** ChicagoPVC.<br><br>You can use up to 20 alphanumeric characters. |
| VASP Name | The name of the VASP type.<br><br>Select **Broadcast File System** to configure the map to support each of the VASPs associated with the BFS BIG. |
| VASP VPI | The virtual path indicator for the VASP.<br><br>Type **0** (numeral zero). |
| VASP Port Number | The port number of the VASP.<br><br>Type **1** (numeral one). |
| BIG Name | The BIG associated with this ATM PVC map. |
| ATM Card Slot Number | The slot number where the ATM card is installed in the BIG. |
| ATM Card VPI | The virtual path indicator for the ATM card.<br><br>Type **1** to identify the data path. |
| Bandwidth | The bandwidth of the map. |

Type **30**.

7. When you finish making changes, click **Save**. The system saves the new ATM PVC map information in the DNCS database and closes the Set Up ATM PVC map window. The ATM PVC Map List window updates to include the new ATM PVC map information.

8. Update your network map to reflect these changes.

9. Do you need to modify another ATM PVC map?

   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the ATM PVC Map List window and return to the DNCS Administrative Console.

## Delete an ATM PVC Map

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > ATM PVC > [ATM PVC Map Name] > File > Delete**

Use this procedure to delete an ATM PVC map from the DNCS.

### Deleting an ATM PVC Map

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **ATM PVC**. The ATM PVC Map List window opens.
4. Click once on the row containing the ATM PVC map you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the ATM PVC map from the DNCS database and from the ATM PVC Map List window.
7. Delete the ATM PVC map from your network map.
8. Do you need to delete another ATM PVC map?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the ATM PVC Map List window and return to the DNCS Administrative Console.

## Delete an ATM PVC Map

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > ATM PVC > [ATM PVC Map Name] > File > Delete**

Use this procedure to delete an ATM PVC map from the DNCS.

### Deleting an ATM PVC Map

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **ATM PVC**. The ATM PVC Map List window opens.
4. Click once on the row containing the ATM PVC map you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the ATM PVC map from the DNCS database and from the ATM PVC Map List window.
7. Delete the ATM PVC map from your network map.
8. Do you need to delete another ATM PVC map?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the ATM PVC Map List window and return to the DNCS Administrative Console.

# MPEG Content Source

The first step in setting up elements that process program or service data is to add an MPEG content source. The DBDS receives content (program and service information) through devices such as the following:

- IRTs
- MDRs
- RTEs
- IRDs
- Multiplexers
- VOD servers

These devices are called MPEG sources, because they receive content from satellites and convert it into MPEG transport streams.

## What do you want to do?

- Review MPEG content source settings
- Add an MPEG content source
- Modify an MPEG content source
- Delete an MPEG content source

## MPEG Content Source Settings

Use the Set Up MPEG Source page to manage the MPEG sources in your network. Three tabs in this window provide settings for the MPEG source:

- Basic Parameters fields

Use the following fields when you manage the basic parameters for an MPEG source.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this source. |
| MPEG Source Name | The name of this source.<br>**Example:** HE1_IRT1.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Device Type | The device type associated with this MPEG source. If the source will provide VOD data, select the **Service Group Object** option. |
| IP Address | The IP address for this MPEG source.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the MPEG source. |

- Connections fields

Use the following fields when you manage the connections for an MPEG content source.

| Field | Description |
|---|---|
| Port Number | The number that identifies the output port on this MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator. Start with the first available port number. We recommend starting with 0 (zero). |
| Transport Stream ID | The number that identifies the transport stream going from this MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator.<br>For VOD, this number must correspond with the ASI input (usually on your network map) on the associated QAM, MQAM, GQAM, or GoQAM modulator.<br>**Important:** If you are using our Overlay solution, make certain to enter a TSID that<br>is within the range reserved for our devices. This range is listed to the right of the TSID field for easy reference. |
| Transport Protocol | The type of output card that is installed in this MPEG source.<br>Click the **Transport Protocol** arrow and select the type of output card that is installed in this MPEG source: ASI, DHEI, SWIF, or Ethernet.<br>**Notes:** |

| | |
|---|---|
| | ▪ If the MPEG source is a VOD server, select **ASI**.<br>▪ If you select Ethernet, complete the **Physical Address**, **IP Address**, and the **Subnet Mask** fields. |
| Physical Address | The MAC address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| IP Address | The IP address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| Subnet Mask | The subnet mask of the output card that is installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |

### Basic Parameters - MPEG Content Source

Use the following fields when you manage the basic parameters for an MPEG source.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this source. |
| MPEG Source Name | The name of this source.<br>**Example:** HE1_IRT1.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Device Type | The device type associated with this MPEG source. If the source will provide VOD data, select the **Service Group Object** option. |
| IP Address | The IP address for this MPEG source.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the MPEG source. |

### Connections - MPEG Content Source

Use the following fields when you manage the connections for an MPEG content source.

| Field | Description |
|---|---|
| Port Number | The number that identifies the output port on this MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator. Start with the first available port number. We recommend starting with 0 (zero). |
| Transport Stream ID | The number that identifies the transport stream going from this MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator.<br>For VOD, this number must correspond with the ASI input (usually on your network map) on the associated QAM, MQAM, GQAM, or GoQAM modulator.<br>**Important:** If you are using our Overlay solution, make certain to enter a TSID that<br>is within the range reserved for our devices. This range is listed to the right of the TSID field for easy reference. |
| Transport Protocol | The type of output card that is installed in this MPEG source.<br>Click the **Transport Protocol** arrow and select the type of output card that is installed in this MPEG source: ASI, DHEI, SWIF, or Ethernet.<br>**Notes:**<br>▪If the MPEG source is a VOD server, select **ASI**.<br>▪If you select Ethernet, complete the **Physical Address**, **IP Address**, and the **Subnet Mask** fields. |
| Physical Address | The MAC address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| IP Address | The IP address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| Subnet Mask | The subnet mask of the output card that is installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |

## Add an MPEG Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > File > New**

**Note:** This procedure can be used for all system configurations.

Adding an MPEG content source requires the following steps:

- Setting up the MPEG content source basic parameters
- Setting up the MPEG content source connections

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- Name of the headend containing the MPEG source
- Name used to identify the MPEG source
- Type of MPEG source (for example, IRT, MDR, VOD server, and so forth)
- IP address for the MPEG source
- Type of output card installed in the MPEG source (ASI, DHEI, or SWIF)
- Number identifying the output port on the MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator
- Number identifying the transport stream going from the MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Setting Up MPEG Source Basic Parameters

The first step in adding an MPEG content source is to complete these steps to set up the basic parameters.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click **File > New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameters - MPEG Content Source.

Use the following fields when you manage the basic parameters for an MPEG source.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this source. |
| MPEG Source Name | The name of this source.<br>**Example:** HE1_IRT1.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Device Type | The device type associated with this MPEG source. If the source will provide VOD data, select the **Service Group Object** option. |
| IP Address | The IP address for this MPEG source.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the MPEG source. |

6. Click **Apply**. The system saves the basic parameters for this MPEG source in the DNCS database. The previously disabled Connectivity tab becomes available.
7. Your next step is to set up the connection from the MPEG source to the content QAM, MQAM, GQAM, or GoQAM modulator. Go to Setting Up MPEG Source Connections.

### Setting Up MPEG Source Connections

After you set up the basic parameters for an MPEG content source, complete these steps to set up set up the connections from the MPEG source to its associated content QAM, MQAM, GQAM, or GoQAM modulator.

1. On the Set Up MPEG source window, click the **Connectivity** tab. The Connectivity window opens with an illustration of any devices already connected to this MPEG source. (If no devices are yet connected, the illustration field will be empty.)
2. Click **Create Port**. The Port Number Prompt window opens.
3. Complete the fields on the screen as described in Connections - MPEG Content Source.

Use the following fields when you manage the connections for an MPEG content source.

| Field | Description |
|---|---|
| Port Number | The number that identifies the output port on this MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator. Start with the first available port number. We recommend starting with 0 (zero). |
| Transport Stream ID | The number that identifies the transport stream going from this MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator.<br>For VOD, this number must correspond with the ASI input (usually on your network map) on the associated QAM, MQAM, GQAM, or GoQAM modulator.<br>**Important:** If you are using our Overlay solution, make certain to enter a TSID that<br>is within the range reserved for our devices. This range is listed to the right of the TSID field for easy reference. |
| Transport Protocol | The type of output card that is installed in this MPEG source.<br>Click the **Transport Protocol** arrow and select the type of output card that is installed in this MPEG source: ASI, DHEI, SWIF, or Ethernet.<br>**Notes:**<br>▪ If the MPEG source is a VOD server, select **ASI**.<br>▪ If you select Ethernet, complete the **Physical Address**, **IP Address**, and the **Subnet Mask** fields. |
| Physical Address | The MAC address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| IP Address | The IP address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| Subnet Mask | The subnet mask of the output card that is installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |

4. Click **OK**. The system saves this information in the DNCS database and closes the Port Number Prompt window. The Connectivity tab updates with the new port and transport stream information. The Modify Port and Delete Port options become available.

**Note:** When you set up the associated content QAM, MQAM, GQAM, or GoQAM modulator, the system will automatically complete the Connect To fields on this window.

5. Click **Apply**. The system saves the MPEG source information in the DNCS database and updates the Connectivity illustration to include the new port information.

6. Is the MPEG source connected to another ASI input port on a content MQAM, GQAM, or GoQAM modulator?

- If **yes**, repeat this procedure from step 2.
- If **no**, go to step 9.

7. Is the MPEG source connected to a set of content QAM modulators that are connected to each other (daisy-chained)?

- If **yes**, repeat this procedure from step 2 for each QAM modulator in the chain.

  **Note:** While each QAM modulator will use a different port number on the MPEG source, all of the modulators must have the same transport stream ID. In addition, if you click **Apply**, the Connectivity illustration will show the MPEG source connected multiple times to one modulator.

- If **no**, go to step 10.

8. Click **Save**. The system saves the MPEG source information in the DNCS database and closes the Set Up MPEG Source window. The MPEG Source List window updates to include the new MPEG source.

9. Add the new MPEG source to your network map.

10. Do you need to add another MPEG Source?

- If **yes**, go back to Setting Up MPEG Source Basic Parameters.
- If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console.

11. Your next step is to add the content QAM, MQAM, or GQAM modulator that will be receiving data from this MPEG content source. Go to the following procedure, according to the device that will receive data from this MPEG source:

- Adding a Content QAM Modulator
- Adding a Content MQAM Modulator
- Adding a Content GQAM Modulator
- Adding a Content RF GoQAM Modulator
- Adding a Content IF GoQAM Modulator

## Modify an MPEG Source

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > [MPEG Source Name] > File > Open**

**Note:** This procedure can be used for any system configuration.

After an MPEG source has been saved in the DNCS, you can modify any of its parameters, except for the headend associated with it and the device type.

**Important:** Contact Cisco Services for assistance in modifying an MPEG BFS source.

### Modifying an MPEG Source

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click once on the row containing the MPEG source you want to modify.
5. Click **File > Open**. The Set Up MPEG Source window for the MPEG source you selected opens.
6. Make changes to the fields as described in Basic Parameters - MPEG Content Source and in Connections - MPEG Content Source.

Use the following fields when you manage the connections for an MPEG content source.

| Field | Description |
|---|---|
| Port Number | The number that identifies the output port on this MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator. Start with the first available port number. We recommend starting with 0 (zero). |
| Transport Stream ID | The number that identifies the transport stream going from this MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator.<br>For VOD, this number must correspond with the ASI input (usually on your network map) on the associated QAM, MQAM, GQAM, or GoQAM modulator.<br>**Important:** If you are using our Overlay solution, make certain to enter a TSID that<br>is within the range reserved for our devices. This range is listed to the right of the TSID field for easy reference. |
| Transport Protocol | The type of output card that is installed in this MPEG source.<br>Click the **Transport Protocol** arrow and select the type of output card that is installed in this MPEG source: ASI, DHEI, SWIF, or Ethernet.<br>**Notes:**<br>▪ If the MPEG source is a VOD server, select **ASI**.<br>▪ If you select Ethernet, complete the **Physical Address**, **IP Address**, and the **Subnet Mask** fields. |
| Physical Address | The MAC address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| IP Address | The IP address of the output card installed in this MPEG source. |

| | |
|---|---|
| | Only displays if you select **Ethernet** as the Transport Protocol. |
| Subnet Mask | The subnet mask of the output card that is installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |

Use the following fields when you manage the basic parameters for an MPEG source.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this source. |
| MPEG Source Name | The name of this source.<br>**Example:** HE1_IRT1.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Device Type | The device type associated with this MPEG source. If the source will provide VOD data, select the **Service Group Object** option. |
| IP Address | The IP address for this MPEG source.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the MPEG source. |

**Note:** If you would like to save your changes to the database without closing the window, you can click **Apply** at any time.

7. When you finish making changes, click **Save**. The system saves the new MPEG source information in the DNCS database and closes the Set Up MPEG Source window. The MPEG Source List window updates to include the new MPEG source information.

8. Update your network map to reflect these changes.

9. Do you need to modify another MPEG source?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console.

## Modify an MPEG Source

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > [MPEG Source Name] > File > Open**

**Note:** This procedure can be used for any system configuration.

After an MPEG source has been saved in the DNCS, you can modify any of its parameters, except for the headend associated with it and the device type.

**Important:** Contact Cisco Services for assistance in modifying an MPEG BFS source.

### Modifying an MPEG Source

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click once on the row containing the MPEG source you want to modify.
5. Click **File > Open**. The Set Up MPEG Source window for the MPEG source you selected opens.
6. Make changes to the fields as described in Basic Parameters - MPEG Content Source and in Connections - MPEG Content Source.

Use the following fields when you manage the connections for an MPEG content source.

| Field | Description |
|---|---|
| Port Number | The number that identifies the output port on this MPEG source that is physically connected to the input port on the associated content QAM, MQAM, GQAM, or GoQAM modulator. Start with the first available port number. We recommend starting with 0 (zero). |
| Transport Stream ID | The number that identifies the transport stream going from this MPEG source to the associated content QAM, MQAM, GQAM, or GoQAM modulator.<br>For VOD, this number must correspond with the ASI input (usually on your network map) on the associated QAM, MQAM, GQAM, or GoQAM modulator.<br>**Important:** If you are using our Overlay solution, make certain to enter a TSID that<br>is within the range reserved for our devices. This range is listed to the right of the TSID field for easy reference. |
| Transport Protocol | The type of output card that is installed in this MPEG source.<br>Click the **Transport Protocol** arrow and select the type of output card that is installed in this MPEG source: ASI, DHEI, SWIF, or Ethernet.<br>**Notes:**<br>▪ If the MPEG source is a VOD server, select **ASI**.<br>▪ If you select Ethernet, complete the **Physical Address**, **IP Address**, and the **Subnet Mask** fields. |
| Physical Address | The MAC address of the output card installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |
| IP Address | The IP address of the output card installed in this MPEG source. |

| | |
|---|---|
| | Only displays if you select **Ethernet** as the Transport Protocol. |
| Subnet Mask | The subnet mask of the output card that is installed in this MPEG source.<br>Only displays if you select **Ethernet** as the Transport Protocol. |

Use the following fields when you manage the basic parameters for an MPEG source.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this source. |
| MPEG Source Name | The name of this source.<br>**Example:** HE1_IRT1.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Device Type | The device type associated with this MPEG source. If the source will provide VOD data, select the **Service Group Object** option. |
| IP Address | The IP address for this MPEG source.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the MPEG source. |

**Note:** If you would like to save your changes to the database without closing the window, you can click **Apply** at any time.

7. When you finish making changes, click **Save**. The system saves the new MPEG source information in the DNCS database and closes the Set Up MPEG Source window. The MPEG Source List window updates to include the new MPEG source information.

8. Update your network map to reflect these changes.

9. Do you need to modify another MPEG source?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console.

## Delete an MPEG Source

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > [MPEG Source Name] > File > Delete**

**Note:** This procedure can be used for all system configurations.

Use this procedure to delete an MPEG content source from the DNCS.

### Deleting an MPEG Source

1. Disconnect any elements associated with this source.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **MPEG Source**. The MPEG Source List window opens.
5. Click once on the row containing the MPEG source you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the MPEG source information from the DNCS database and from the MPEG Source List window.
8. Delete the MPEG source from your network map.
9. Do you need to delete another MPEG source?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console.

## Delete an MPEG Source

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > [MPEG Source Name] > File > Delete**

**Note:** This procedure can be used for all system configurations.

Use this procedure to delete an MPEG content source from the DNCS.

### Deleting an MPEG Source

1. Disconnect any elements associated with this source.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **MPEG Source**. The MPEG Source List window opens.
5. Click once on the row containing the MPEG source you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the MPEG source information from the DNCS database and from the MPEG Source List window.
8. Delete the MPEG source from your network map.
9. Do you need to delete another MPEG source?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console.

# QAM Modulator for Content

A QAM modulator that receives the data that provides DHCTs with content is referred to as a content QAM modulator. The content QAM modulator encrypts the data, if needed, and modulates it onto an RF carrier for distribution to DHCTs. You may hear the content QAM modulator referred to as a service QAM modulator because it provides the data that subscribers recognize as services.

Content QAM modulators carry data to all DHCTs in a hub and can receive data via DHEI, ASI, or SWIF inputs. SWIF inputs originate from a BIG using our SWIF card.

## What do you want to do?

- Review content QAM settings
- Add a content QAM
- Modify a content QAM
- Delete a content QAM
- Activate a content QAM
- Reset a content QAM
- Tear down sessions on a content QAM
- View recommended frequencies
- Locate the QAM MAC address

## QAM Modulator Settings

Use the Set Up QAM Modulator page on the DNCS Administrative Console to manage the QAM devices in your network. Two tabs in this window provide settings for the QAM:

- Basic Parameters - Content QAM: Use the settings on the Basic Parameters tab to configure the QAM.
- Connectivity Parameters - Content QAM: Use the settings on the Connectivity tab to configure the connections between the modulator and its associated MPEG source

**Note:** Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### Basic Parameters - Content QAM

Use the following fields when you manage the basic parameters for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content QAM |
| QAM Name | The name of this QAM<br>You can use up to 20 alphanumeric characters. Be sure to use a name that allows you to easily identify the modulator and where it resides. For example, a name of VODhub1Q43 could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for the QAM<br>For assistance locating the MAC address, see Locate the MAC Address of a QAM. |
| IP Address | The IP address for this QAM<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this QAM modulator resides<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Administrative State | Defines whether or not this modulator is enabled or not.<br>▪When **Online** is selected, the modulator is enabled.<br>▪When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator |

| | |
|---|---|
| | to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br>▪When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. |
| Input Port | The type of interface that will receive data from the QAM<br>**Important:** If the QAM modulator will process VOD data, select ASI for the input port. |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses. For example,if the modulator uses 256 QAM, select **256 QAM**.<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream going from this modulator<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to set-tops<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. For assistance, see Recommended Modulator Frequencies. |
| | **Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier<br>Enable this option to produce an unmodulated RF carrier, which is is useful when performing testing. |
| | **Mute RF Output** - Determines whether the QAM's RF output port is muted<br>Enable this option to turn off the RF output for a port. Turning off the RF output port is helpful when installing the modulator. |

**Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM

Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)

Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.

For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected.

**Interleaver Depth** - Determines the depth of interleaving for the QAM

This setting appears only when the Overlay feature is enabled.

**Port to Hubs** - Allows you to see the hubs available to this QAM

**Important:** Click **Apply** to turn on the Hubs button. Then, click the Hubs button to view the hubs that are available to receive content data from this QAM.

**Associate Hubs Area**

In the Available Hubs list, select the hub name and then click **Add**. The hub name moves into the Selected Hubs list. Repeat this step for each hub that will receive data from this modulator.

**Important:** If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs list. Note that this modulator is now a Distinguished QAM candidate.

### Connectivity Parameters - Content QAM

Use the following fields when you manage the connections for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the QAM resides |
| Device Type | The type of MPEG source device being used to send data to this QAM, for example IRT, MDR and Service Group Object |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

### Recommended Modulator Frequencies

Use the center frequencies shown in the following table to send data from your QAM modulators to the DHCTs on your system. Notice that these frequencies are separated by increments of 6 MHz.

**Note:** If you are experiencing signal interference, try offsetting your modulator frequencies by 250 kHz from the frequencies shown in the table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 153 | 159 | 165 | 171 | 177 | 183 | 189 | 195 | 201 | 207 |
| 213 | 219 | 225 | 231 | 237 | 243 | 249 | 255 | 261 | 267 |
| 273 | 279 | 285 | 291 | 297 | 303 | 309 | 315 | 321 | 327 |
| 333 | 339 | 345 | 351 | 357 | 363 | 369 | 375 | 381 | 387 |
| 393 | 399 | 405 | 411 | 417 | 423 | 429 | 435 | 441 | 447 |
| 453 | 459 | 465 | 471 | 477 | 483 | 489 | 495 | 501 | 507 |
| 513 | 519 | 525 | 531 | 537 | 543 | 549 | 555 | 561 | 567 |
| 573 | 579 | 585 | 591 | 597 | 603 | 609 | 615 | 621 | 627 |
| 633 | 639 | 645 | 651 | 657 | 663 | 669 | 675 | 681 | 687 |
| 693 | 699 | 705 | 711 | 717 | 723 | 729 | 735 | 741 | 747 |

### RF Output Port Parameters - Content QAM

Use the following fields when you manage the RF output port parameters for a content QAM modulator.

| Field | Description |
|---|---|
| **Basic Parameters** | |
| These fields cannot be modified from the RF Output Port window. To change these fields, click **Cancel** to close the RF Output Port window and then change these fields from the Basic Parameters tab. For more information about these settings, go to Basic Parameters - Content QAM. | |
| **Associate Hubs** | |
| Available Hubs | Lists the hubs that are available to receive program/service data from this QAM modulator.<br>**Add a hub to this list:** Select the hub and click **Add**. |
| Selected Hubs | Lists the hubs that receive program/service data from this QAM modulator.<br>If this QAM modulator is sending data to all hubs in the headend, verify that no hubs appear in the Selected Hubs field. Note that this modulator is now a Distinguished QAM candidate.<br>**Remove a hub from this list:** Select the hub and click **Remove**. |

## Information to Add a Content QAM

Before you add a content QAM modulator to the DNCS, gather the following data so that you can enter it into the appropriate fields.

- Name of the headend containing the QAM modulator
- Name used to identify the QAM modulator
- IP address for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- Subnet mask for the QAM modulator (from your system administrator)
- Type of input interface that will be receiving data from the associated MPEG source (ASI, DHEI, or SWIF)

  **Note:** If the QAM modulator will be processing VOD data, the modulator must have an ASI input interface.

- Number identifying the transport stream going from the QAM modulator out to the hubs on your system
- Type of modulation the QAM modulator uses
- Frequency of the channel being used to send data from the QAM modulator to the hubs on your system
- Names of the hubs you want to receive data from this QAM modulator
- Number identifying the input port on this QAM modulator that is physically connected to the associated MPEG source
- Name of the headend containing the associated MPEG source
- Type of MPEG source device being used to send data to this QAM modulator (for example, IRT, MDR, VOD server, and so forth)
- Name of the associated MPEG source
- Number identifying the output port of the associated MPEG source that is physically connected to the input port on this QAM modulator

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

## Locate the MAC Address of a QAM

You can look at the sticker on the side of the QAM, MQAM, SCS MQAM, GQAM, or GoQAM to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

## Add a Content QAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > QAM**

### Complete Basic Parameters

**Note**: For a list of information needed to add the modulator to the DNCS, go to Information to Add a Content QAM.

The first step in adding a content QAM modulator is to complete these steps to set up the basic parameters for the modulator.

**Tips:**

- Until you click **Apply**, the Hubs button remains dimmed.
- Until you click **Apply**, the Administrative State is defined as Offline. Do not select the Online option until you have configured the QAM settings in the Basic Parameters tab and the Connectivity tab.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File> New > QAM**. The Set Up QAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameters - Content QAM, and then click **Apply**. The Hubs button and the Administrative State become selectable.

Use the following fields when you manage the basic parameters for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content QAM |
| QAM Name | The name of this QAM<br>You can use up to 20 alphanumeric characters. Be sure to use a name that allows you to easily identify the modulator and where it resides. For example, a name of VODhub1Q43 could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for the QAM<br>For assistance locating the MAC address, see Locate the MAC Address of a QAM. |
| IP Address | The IP address for this QAM<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this QAM modulator resides<br>If your system uses a standard network configuration, |

| | |
|---|---|
| | type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br><br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br><br>Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br><br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway<br><br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Administrative State | Defines whether or not this modulator is enabled or not.<br><br>▪ When **Online** is selected, the modulator is enabled.<br>▪ When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br><br>▪ When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪ When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. |
| Input Port | The type of interface that will receive data from the QAM<br><br>**Important:** If the QAM modulator will process VOD data, select ASI for the input port. |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses. For example,if the modulator uses 256 QAM, select **256 QAM**.<br><br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator: |

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.
- Modulators using 256-QAM support a total bandwidth of 38.811 Mbps.

**Transport Stream ID** - Identifies the transport stream going from this modulator

You can use up to 5 numeric characters.

**Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to set-tops

We recommend that you enter a value in 6 MHz increments from 91 to 867. For assistance, see Recommended Modulator Frequencies.

**Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier

Enable this option to produce an unmodulated RF carrier, which is is useful when performing testing.

**Mute RF Output** - Determines whether the QAM's RF output port is muted

Enable this option to turn off the RF output for a port. Turning off the RF output port is helpful when installing the modulator.

**Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM

Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)

Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.

For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected.

**Interleaver Depth** - Determines the depth of interleaving for the QAM

This setting appears only when the Overlay feature is enabled.

**Port to Hubs** - Allows you to see the hubs available to this QAM

**Important:** Click **Apply** to turn on the Hubs button. Then, click the Hubs button to view the hubs that are available to receive content data from this QAM.

**Associate Hubs Area**

In the Available Hubs list, select the hub name and then click **Add**. The hub name moves into the Selected Hubs list. Repeat this step for each hub that will receive data from this modulator.

**Important:** If this QAM modulator will send data to all

| | |
|---|---|
| | hubs in the headend, make sure no hubs appear in the Selected Hubs list. Note that this modulator is now a Distinguished QAM candidate. |

6. Click **Hubs**. The RF Output Port window opens.

7. Define the hubs that will receive program/service data from this QAM modulator by completing the fields as described in RF Output Port Parameters - Content QAM.

Use the following fields when you manage the RF output port parameters for a content QAM modulator.

| Field | Description |
|---|---|
| **Basic Parameters** | |
| These fields cannot be modified from the RF Output Port window. To change these fields, click **Cancel** to close the RF Output Port window and then change these fields from the Basic Parameters tab. For more information about these settings, go to Basic Parameters - Content QAM. | |
| **Associate Hubs** | |
| Available Hubs | Lists the hubs that are available to receive program/service data from this QAM modulator.<br>**Add a hub to this list:** Select the hub and click **Add**. |
| Selected Hubs | Lists the hubs that receive program/service data from this QAM modulator.<br>If this QAM modulator is sending data to all hubs in the headend, verify that no hubs appear in the Selected Hubs field. Note that this modulator is now a Distinguished QAM candidate.<br>**Remove a hub from this list:** Select the hub and click **Remove**. |

8. On the RF Output Port window, click **Save**. The RF Output Port window closes and the Set Up QAM window is now visible.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

**Next:** Add Connectivity Parameters

### Complete Basic Parameters

**Note**: For a list of information needed to add the modulator to the DNCS, go to Information to Add a Content QAM .

The first step in adding a content QAM modulator is to complete these steps to set up the basic parameters for the modulator.

**Tips:**

- Until you click **Apply**, the Hubs button remains dimmed.
- Until you click **Apply**, the Administrative State is defined as Offline. Do not select the Online option until you have configured the QAM settings in the Basic Parameters tab and the Connectivity tab.

### Add Connectivity Parameters

After you have completed the fields in the Basic Parameters tab, follow these instructions to complete the fields in the Connectivity tab and set up the connections between the modulator and the MPEG source that feeds the modulator.

**Previous:** Set up the Complete Basic Parameters

After you have completed the fields in the Basic Parameters tab, follow these instructions to complete the fields in the Connectivity tab and set up the connections between the modulator and the MPEG source that feeds the modulator.

**Previous:** Set up the Complete Basic Parameters

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with a graphical representation of the devices already connected to this QAM modulator.
2. Select the **Input Port** option.
3. Complete the fields on the screen as described in ▸ Connectivity Parameters - Content QAM.

Use the following fields when you manage the connections for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the QAM resides |
| Device Type | The type of MPEG source device being used to send data to this QAM, for example IRT, MDR and Service Group Object |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

4. Click **Apply**. The system saves this information in the DNCS database and updates the illustration so that it shows the information you entered.
5. Select the **Output Port** option.
6. Complete the fields on the screen as described in ▸ Connectivity Parameters - Content QAM.

Use the following fields when you manage the connections for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the QAM resides |
| Device Type | The type of MPEG source device being used to send data to this QAM, for example IRT, MDR and Service Group Object |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

7. Click **Apply**. The system saves this information in the DNCS database and updates the illustration so that it shows the information you entered.

8. Next you need to Activate a QAM Modulator.

### Activate a QAM Modulator

**Important:** You can activate a QAM modulator only after all parameters for the modulator have been saved to the DNCS database, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. If you have not already done so, add the content QAM modulator or add the BFS QAM modulator to the DNCS.
2. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
3. At the Administrative State field, click the **Online** option.
4. If this QAM modulator will function as a distinguished QAM modulator, verify that **Allow SI** is set to **Yes**. If it is not, click the option button and select **Yes**.
5. Click **Save**. The system saves the QAM modulator information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new QAM modulator.
6. Add the new content QAM modulator to your network map.
7. Click **File > Close** to close the QAM List window and return to the DNCS.

### Related Topics

- Set Up Your Network

## Modify a Content QAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM/MQAM Name] > File > Open**

**Important:** Do not attempt to modify a BFS QAM. Contact Cisco Services for assistance in changing a BFS QAM.

Complete these steps to modify a content QAM, MQAM, or GQAM.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the QAM you want to modify.
5. Click **File > Open**. The Set Up QAM window opens.
6. To change the basic parameters, refer to Basic Parameters - Content QAM.

Use the following fields when you manage the basic parameters for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content QAM |
| QAM Name | The name of this QAM<br>You can use up to 20 alphanumeric characters. Be sure to use a name that allows you to easily identify the modulator and where it resides. For example, a name of VODhub1Q43 could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for the QAM<br>For assistance locating the MAC address, see Locate the MAC Address of a QAM. |
| IP Address | The IP address for this QAM<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this QAM modulator resides<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>Modulators using **64-QAM** support a total bandwidth of |

| | |
|---|---|
| | 26.971 Mbps.<br><br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway<br><br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Administrative State | Defines whether or not this modulator is enabled or not.<br><br>▪ When **Online** is selected, the modulator is enabled.<br>▪ When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br><br>▪ When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪ When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. |
| Input Port | The type of interface that will receive data from the QAM<br><br>**Important:** If the QAM modulator will process VOD data, select ASI for the input port. |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses. For example,if the modulator uses 256 QAM, select **256 QAM**.<br><br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br><br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream going from this modulator<br><br>You can use up to 5 numeric characters. |

**Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to set-tops

We recommend that you enter a value in 6 MHz increments from 91 to 867. For assistance, see Recommended Modulator Frequencies.

**Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier

Enable this option to produce an unmodulated RF carrier, which is is useful when performing testing.

**Mute RF Output** - Determines whether the QAM's RF output port is muted

Enable this option to turn off the RF output for a port. Turning off the RF output port is helpful when installing the modulator.

**Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM

Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)

Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.

For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected.

**Interleaver Depth** - Determines the depth of interleaving for the QAM

This setting appears only when the Overlay feature is enabled.

**Port to Hubs** - Allows you to see the hubs available to this QAM

**Important:** Click **Apply** to turn on the Hubs button. Then, click the Hubs button to view the hubs that are available to receive content data from this QAM.

**Associate Hubs Area**

In the Available Hubs list, select the hub name and then click **Add**. The hub name moves into the Selected Hubs list. Repeat this step for each hub that will receive data from this modulator.

**Important:** If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs list. Note that this modulator is now a Distinguished QAM candidate.

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

7. To change the connectivity parameters, refer to Connectivity Parameters - Content QAM.

Use the following fields when you manage the connections for a content QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the QAM resides |
| Device Type | The type of MPEG source device being used to send data to this QAM, for example IRT, MDR and Service Group Object |
| Device Name | The name of the source device |
| The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.<br><br>**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator. | |

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

8. When you finish making changes, click **Save**. The system saves the new QAM information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new modulator information.

9. Update your network map to reflect these changes.

## Related Topics

- Set Up Your Network
- Recommended Modulator Frequencies
- Locate the MAC Address of a QAM

## Reset a Content QAM

**Quick Path: DNCS > Network Element Provisioning > QAM > [Select QAM] > File > Reset**

Resetting a QAM, MQAM, GQAM, or GoQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

**Important:** You can reset only our modulators from the DNCS. Generic QAM modulators cannot be reset from the DNCS. To reset a generic QAM modulator, refer to the documentation provided by the manufacturer of the modulator.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Select the QAM, MQAM, GQAM, or GoQAM modulator that you want to reboot.

**Notes:**

- Each MQAM modulator is listed four times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GQAM modulator is listed 16 times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GoQAM (RF or IF) is listed twice (once for each of the modulator's RF output channels), but select only the first occurrence.

5. Click **File > Reset**. The confirmation window appears with the question, "Are you sure you want to reset QAM modulator 'name of modulator'?"
6. Click **Yes**. The QAM List window displays the following message, "The reset request has been received by QAM modulator 'name of modulator'."

## Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display Sessions > [Select Session] > Tear Down**

**Important:** Unless you have been instructed by Cisco Services, only tear down sessions on content QAM modulators. Do not tear down sessions on BFS QAM modulators.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to Use the Filter to Display Sessions.
2. When the list of sessions displays, use one of the following methods to select the sessions you would like to tear down:
   - To tear down specific sessions, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete.
   - To tear down all sessions, click **Select All Displayed Sessions**.

   **Note:** If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.
3. Click **Tear Down**. The system tears down the sessions you selected and updates the status of all sessions.
4. Click **File > Close** to close the Session Data window.
5. Depending on your reason for tearing down the session, you may decide to complete one of the following tasks:
   - If you tore down the session in order to delete a QAM modulator, you can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind. For assistance, see Delete a Content QAM Modulator.
   - If you deleted the session in order to correct an unlisted, active session, restart the session. For assistance, see Restart a Session.

### Related Topics

- Why Tear Down Sessions?

### Why Tear Down Sessions?

This section describes how to tear down sessions for either of the following reasons:

- You need to delete a QAM modulator that carries content.

  **Note:** Before deleting a QAM modulator that carries content, first tear down sessions associated with the modulator. Deleting a modulator without first tearing down its related sessions can degrade system performance. Performance can degrade because the DNCS uses its resources to attempt to associate sessions with a modulator that no longer exists. These sessions are called orphaned sessions.

- You need to tear down and restart an unlisted, active session in order to correct it.

## Delete a Content QAM, MQAM, or GQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [Select modulator] > File > Delete**

**Important:** Do not attempt to delete a BFS modulator. Contact us for assistance in deleting a BFS modulator.

Complete these steps to delete a QAM, MQAM, or GQAM modulator that carries content.

1. First tear down all sessions that are running on the modulator you want to delete.

   **Note:** Before you delete a modulator, first tear down all of the sessions associated with the modulator. If you delete a modulator without first tearing down its related sessions, system performance may be degraded. Performance degrades because the DNCS uses its resources attempting to associate sessions with a modulator that no longer exists.

2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List window opens.
5. Click once on the row containing the QAM that you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the selected modulator information from the DNCS database and from the QAM List window.
8. Delete the selected modulator from your network map.
9. Do you need to delete another QAM modulator.
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

# MQAM Modulator for Content

A content MQAM modulator receives data that provides set-tops with content. Like the QAM modulator, the MQAM modulator it takes the data it receives and, if necessary, it encrypts the data before modulating it onto an RF carrier for distribution to all DHCTs in a hub.

However, one MQAM modulator can perform the work of four QAM modulators. This is possible because the MQAM modulator can receive content from up to two MPEG sources and send the modified data out to the hubs on up to four transport streams. (The QAM modulator receives content from only one MPEG source and can send the modified data out on only one transport stream.)

## What do you want to do?

- Review content MQAM settings
- Add a content MQAM
- Modify a content MQAM
- Delete a content MQAM
- Activate a content MQAM
- Reset a content MQAM
- Tear down sessions on a content MQAM
- View recommended frequencies
- Locate the MQAM MAC address

## MQAM Modulator Settings

Use the Set Up MQAM Modulator page on the DNCS Administrative Console to manage the MQAM devices in your network. Two tabs in this window provide settings for the MQAM:

- Basic Parameters settings: Use the settings on the Basic Parameters tab to configure the MQAM.
- Connectivity settings: Use the settings on the Connectivity tab to configure the connections between the modulator and its associated MPEG source.

**Note:** Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### Basic Parameters - Content MQAM

Use the following fields when you manage the basic parameters for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.<br>**Example:** A name of **VODhub1Q43** could represent a modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for this content modulator. |
| IP Address | The IP address for this content modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | The IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Administrative State | Defines whether or not this modulator is enabled or not.<br>▪When **Online** is selected, the modulator is enabled.<br>▪When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br>▪When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or |

| | | |
|---|---|---|
| | a BFS QAM modulator. Do not select this option for a content QAM modulator. | |
| Input Port | The type of interface that will receive data from the modulator.<br><br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses.<br><br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br><br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br><br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br><br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br><br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br><br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| | **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br><br>This is useful when performing testing. |
| | **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br><br>This is helpful when installing the modulator. |
| | **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br><br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br><br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |

| | |
|---|---|
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>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 that will receive data from this modulator.<br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |

### Connections - Content MQAM Modulator

Use the following fields when you manage the connections for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | Type of MPEG source device being used to send data to this modulator.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

### Basic Parameters - Content MQAM

Use the following fields when you manage the basic parameters for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.<br>**Example:** A name of **VODhub1Q43** could represent a modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for this content modulator. |
| IP Address | The IP address for this content modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | The IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Administrative State | Defines whether or not this modulator is enabled or not.<br>▪When **Online** is selected, the modulator is enabled.<br>▪When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br>▪When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪When this option is not selected, this modulator cannot process SI. |

| | | |
|---|---|---|
| | **Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. | |
| Input Port | The type of interface that will receive data from the modulator.<br><br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses.<br><br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br><br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br><br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br><br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br><br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br><br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| | **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br><br>This is useful when performing testing. |
| | **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br><br>This is helpful when installing the modulator. |
| | **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br><br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br><br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |

| | |
|---|---|
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>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 that will receive data from this modulator.<br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |

### Connections - Content MQAM Modulator

Use the following fields when you manage the connections for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | Type of MPEG source device being used to send data to this modulator.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

### Recommended Modulator Frequencies

Use the center frequencies shown in the following table to send data from your QAM modulators to the DHCTs on your system. Notice that these frequencies are separated by increments of 6 MHz.

**Note:** If you are experiencing signal interference, try offsetting your modulator frequencies by 250 kHz from the frequencies shown in the table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 153 | 159 | 165 | 171 | 177 | 183 | 189 | 195 | 201 | 207 |
| 213 | 219 | 225 | 231 | 237 | 243 | 249 | 255 | 261 | 267 |
| 273 | 279 | 285 | 291 | 297 | 303 | 309 | 315 | 321 | 327 |
| 333 | 339 | 345 | 351 | 357 | 363 | 369 | 375 | 381 | 387 |
| 393 | 399 | 405 | 411 | 417 | 423 | 429 | 435 | 441 | 447 |
| 453 | 459 | 465 | 471 | 477 | 483 | 489 | 495 | 501 | 507 |
| 513 | 519 | 525 | 531 | 537 | 543 | 549 | 555 | 561 | 567 |
| 573 | 579 | 585 | 591 | 597 | 603 | 609 | 615 | 621 | 627 |
| 633 | 639 | 645 | 651 | 657 | 663 | 669 | 675 | 681 | 687 |
| 693 | 699 | 705 | 711 | 717 | 723 | 729 | 735 | 741 | 747 |

## Information to Add a Content MQAM

Before you add a content MQAM modulator to the DNCS, gather the following data so that you can enter it into the appropriate fields.

- Name of the headend containing the modulator
- Name used to identify the modulator
- IP address for the modulator (from your system administrator)
- MAC address for the modulator (for assistance, go to locating the MAC address)
- Subnet mask for the modulator (from your system administrator)
- If applicable, the default gateway that the modulator uses
- Number identifying the transport streams going from the modulator out to the hubs on your system
- Type of modulation the modulator uses
- Frequency of the channel being used to send data from the modulator to the hubs on your system
- Names of the hubs you want to receive data from this modulator
- Number identifying the input port on this modulator that is physically connected to the associated MPEG source
- Name of the headend containing the associated MPEG source
- Type of MPEG source device being used to send data to this modulator (for example, IRT, MDR, VOD server, and so forth)
- Name of the associated MPEG source
- Number identifying the output port of the associated MPEG source that is physically connected to the input port on this QAM modulator

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

## Locate the MAC Address of a QAM

You can look at the sticker on the side of the QAM, MQAM, SCS MQAM, GQAM, or GoQAM to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

## Add a Content MQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > MQAM**

### Complete Basic Parameters

**Note:** For a list of information needed to add the modulator to the DNCS, go to Information to Add a Content MQAM.

The first step in adding a content MQAM modulator is to complete these steps to set up the basic parameters for the modulator.

**Tip:** Until you click **Apply**, the Administrative State is defined as Offline. Do not select the Online option until you have configured the MQAM settings in the Basic Parameters tab and the Connectivity tab.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File> New > MQAM**. The Set Up MQAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameters - Content MQAM, and then click **Apply**. The Administrative State becomes selectable.

Use the following fields when you manage the basic parameters for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.<br>**Example:** A name of **VODhub1Q43** could represent a modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for this content modulator. |
| IP Address | The IP address for this content modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator: |

| | | |
|---|---|---|
| | Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. | |
| Default Gateway | The IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. | |
| Administrative State | Defines whether or not this modulator is enabled or not.<br>▪ When **Online** is selected, the modulator is enabled.<br>▪ When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. | |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br>▪ When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪ When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br>We recommend that you enter a value in 6 |

| | |
|---|---|
| | MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>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 that will receive data from this modulator.<br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |

6. Next you need to Add Connectivity Parameters to the MQAM.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### Complete Basic Parameters

**Note:** For a list of information needed to add the modulator to the DNCS, go to Information to Add a Content MQAM.

The first step in adding a content MQAM modulator is to complete these steps to set up the basic parameters for the modulator.

**Tip:** Until you click **Apply**, the Administrative State is defined as Offline. Do not select the Online option until you have configured the MQAM settings in the Basic Parameters tab and the Connectivity tab.

### Add Connectivity Parameters

After you have completed the fields in the Basic Parameters tab, follow these instructions to complete the fields in the Connectivity tab and set up the connections between the modulator and the MPEG source that feeds the modulator.

**Previous:** Set up the Complete Basic Parameters

1. On the Set Up MQAM window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this MQAM modulator.
2. If not already selected, click to select the **Input 1 Port** option.
3. Complete the fields on the screen as described in Connections - Content MQAM Modulator.

Use the following fields when you manage the connections for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | Type of MPEG source device being used to send data to this modulator.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

4. Click **Apply**. The system saves this information into the DNCS database and updates the illustration so that it shows the information you entered.
5. Is an MPEG source sending data to Input Port 2 on this modulator?
   - If **yes**, click the **Input 2 Port** option. Repeat this procedure from step 3 to define and save the connectivity parameters for the second input port on the modulator.
   - If **no**, you are finished with this procedure.
6. Next you need to Activate a Content MQAM.

### Activate a Content MQAM

**Important:** You can activate an MQAM modulator only after all parameters for the modulator have been saved to the DNCS database, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. If you have not already done so, add the content MQAM to the DNCS.
2. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
3. At the Administrative State field, click the **Online** option.
4. Click **Save**. The system saves the MQAM modulator information in the DNCS database and closes the Set Up MQAM window. The QAM List window updates to include the new MQAM modulator.

   **Note:** The new MQAM modulator is listed four times to show its four output streams.

5. Add the new content MQAM modulator to your network map.
6. Click **File > Close** to close QAM List window and return to the DNCS.

### Related Topics

- Set Up Your Network

# Modify a Content MQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM/MQAM Name] > File > Open**

**Important:** Do not attempt to modify a BFS QAM. Contact Cisco Services for assistance in changing a BFS QAM.

Complete these steps to modify a content QAM, MQAM, or GQAM.

### Modify a Content MQAM

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the MQAM you want to modify.
5. Click **File > Open**. The Set Up MQAM window opens.
6. To change the basic parameters, refer to Basic Parameters - Content MQAM.

Use the following fields when you manage the basic parameters for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.<br>**Example:** A name of **VODhub1Q43** could represent a modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for this content modulator. |
| IP Address | The IP address for this content modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | The IP address of your default gateway. |

| | | |
|---|---|---|
| | Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. | |
| Administrative State | Defines whether or not this modulator is enabled or not.<br>▪ When **Online** is selected, the modulator is enabled.<br>▪ When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. | |
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br>▪ When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪ When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| | **Continuous Wave Mode** - | Enable this option to produce an |

| | |
|---|---|
| Determines whether the modulator produces an unmodulated RF carrier | unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>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 that will receive data from this modulator.<br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |

**Note:** If you would like to save your changes to the database without closing this window, you can click Apply at any time.

7.To change the connectivity parameters, refer to ▸ Connections - Content MQAM Modulator.

Use the following fields when you manage the connections for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | Type of MPEG source device being used to send data to this modulator.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

8. When you finish making changes, click **Save**. The system saves the new QAM information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new modulator information.

9. Update your network map to reflect these changes.

10. Do you need to modify another MQAM?

- If **yes**, repeat this procedure from step 4.
- If no, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

## Related Topics

- Set Up Your Network
- Recommended Modulator Frequencies
- Locate the MAC Address of a QAM

### Modify a Content MQAM

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the MQAM you want to modify.
5. Click **File > Open**. The Set Up MQAM window opens.
6. To change the basic parameters, refer to Basic Parameters - Content MQAM.

Use the following fields when you manage the basic parameters for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 20 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.<br>**Example:** A name of **VODhub1Q43** could represent a modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| MAC Address | The MAC address for this content modulator. |
| IP Address | The IP address for this content modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Subnet Mask | The subnet mask where this modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Modulation Type | The type of modulation this modulator uses. For example, if this is a 256 QAM modulator that uses ITU B modulation, you would select ITU J.83 Annex B (6 MHz).<br>The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>Modulators using **64-QAM** support a total bandwidth of 26.971 Mbps.<br>Modulators using **256-QAM** support a total bandwidth of 38.811 Mbps. |
| Default Gateway | The IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Administrative State | Defines whether or not this modulator is enabled or not.<br>▪ When **Online** is selected, the modulator is enabled.<br>▪ When **Offline** is selected, the modulator is disabled.<br>**Important:** If you are adding a QAM modulator to the DNCS, do not place the modulator online until you have set up the connections between the modulator and the MPEG source that feeds the modulator. For assistance, go to Add Connectivity Parameters. |

| | | |
|---|---|---|
| Allow SI | Defines whether or not this modulator will process system information (SI) and send the SI to all hubs in the headend. Use the following guidance to set this option:<br>▪ When this option is selected, the modulator can process SI and send the SI to all hubs in the headend.<br>▪ When this option is not selected, this modulator cannot process SI.<br>**Important:** Select this option only for a distinguished QAM modulator or a BFS QAM modulator. Do not select this option for a content QAM modulator. | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz)** - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| | **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| | **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| | **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.) |

| | |
|---|---|
| | Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br><br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br><br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br><br>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 that will receive data from this modulator.<br><br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |

**Note:** If you would like to save your changes to the database without closing this window, you can click Apply at any time.

7. To change the connectivity parameters, refer to ▸ Connections - Content MQAM Modulator.

Use the following fields when you manage the connections for a content MQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | Type of MPEG source device being used to send data to this modulator.<br><br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

8. When you finish making changes, click **Save**. The system saves the new QAM information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new modulator information.

9. Update your network map to reflect these changes.

10. Do you need to modify another MQAM?

- If **yes**, repeat this procedure from step 4.
- If no, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

## Reset a Content MQAM

**Quick Path: DNCS > Network Element Provisioning > QAM > [Select QAM] > File > Reset**

Resetting a QAM, MQAM, GQAM, or GoQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

**Important:** You can reset only our modulators from the DNCS. Generic QAM modulators cannot be reset from the DNCS. To reset a generic QAM modulator, refer to the documentation provided by the manufacturer of the modulator.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Select the QAM, MQAM, GQAM, or GoQAM modulator that you want to reboot.

**Notes:**

- Each MQAM modulator is listed four times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GQAM modulator is listed 16 times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GoQAM (RF or IF) is listed twice (once for each of the modulator's RF output channels), but select only the first occurrence.

5. Click **File > Reset**. The confirmation window appears with the question, "Are you sure you want to reset QAM modulator 'name of modulator'?"
6. Click **Yes**. The QAM List window displays the following message, "The reset request has been received by QAM modulator 'name of modulator'."

## Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display Sessions > [Select Session] > Tear Down**

**Important:** Unless you have been instructed by Cisco Services, only tear down sessions on content QAM modulators. Do not tear down sessions on BFS QAM modulators.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to Use the Filter to Display Sessions.
2. When the list of sessions displays, use one of the following methods to select the sessions you would like to tear down:
   - To tear down specific sessions, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete.
   - To tear down all sessions, click **Select All Displayed Sessions**.

   **Note:** If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.
3. Click **Tear Down**. The system tears down the sessions you selected and updates the status of all sessions.
4. Click **File > Close** to close the Session Data window.
5. Depending on your reason for tearing down the session, you may decide to complete one of the following tasks:
   - If you tore down the session in order to delete a QAM modulator, you can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind. For assistance, see Delete a Content QAM Modulator.
   - If you deleted the session in order to correct an unlisted, active session, restart the session. For assistance, see Restart a Session.

**Related Topics**

- Why Tear Down Sessions?

### Why Tear Down Sessions?

This section describes how to tear down sessions for either of the following reasons:

- You need to delete a QAM modulator that carries content.

  **Note:** Before deleting a QAM modulator that carries content, first tear down sessions associated with the modulator. Deleting a modulator without first tearing down its related sessions can degrade system performance. Performance can degrade because the DNCS uses its resources to attempt to associate sessions with a modulator that no longer exists. These sessions are called orphaned sessions.

- You need to tear down and restart an unlisted, active session in order to correct it.

## Delete a Content QAM, MQAM, or GQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [Select modulator] > File > Delete**

**Important:** Do not attempt to delete a BFS modulator. Contact us for assistance in deleting a BFS modulator.

Complete these steps to delete a QAM, MQAM, or GQAM modulator that carries content.

1. First tear down all sessions that are running on the modulator you want to delete.

   **Note:** Before you delete a modulator, first tear down all of the sessions associated with the modulator. If you delete a modulator without first tearing down its related sessions, system performance may be degraded. Performance degrades because the DNCS uses its resources attempting to associate sessions with a modulator that no longer exists.

2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List window opens.
5. Click once on the row containing the QAM that you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the selected modulator information from the DNCS database and from the QAM List window.
8. Delete the selected modulator from your network map.
9. Do you need to delete another QAM modulator.
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

# GQAM Modulator for Content

The content GQAM modulator performs the same tasks that a QAM or an MQAM modulator performs: it takes the data it receives and, if necessary, it encrypts the data before modulating it onto an RF carrier for distribution to all DHCTs in a hub. Unlike the content QAM modulator, which can receive data from only one ASI MPEG source, a content GQAM modulator can receive content from up to four ASI MPEG sources. A content GQAM modulator can also send the modified data out to the hubs on up to 16 transport streams in contrast to the QAM modulator, which can send data out on only one transport stream. In other words, you can use one GQAM modulator to perform the work of 16 QAM modulators.

The content GQAM can also receive data on a Gigabit Ethernet (GbE) input. Typically, GbE input is used to receive data that provides VOD service.

## What do you want to do?

- Review settings for content GQAM modulators
- View recommended frequencies for GQAM modulators
- Add a content GQAM modulator
- Locate the MAC address of a content GQAM modulator
- Reset a content GQAM modulator
- Set up multicast sessions on a content GQAM modulator
- Set Up Stat Mux Dejitter Groups
- Set up a Transport Stream Route (TSR) on the GQAM modulator
- Set up GQAM redundancy
- Modify a content GQAM modulator
- Tear down sessions on a content GQAM modulator
- Delete a content GQAM modulator

## Content GQAM Modulator Settings

Use the Set Up GQAM Modulator page on the DNCS Administrative Console to manage the GQAM devices in your network. Two tabs in this window provide settings for the GQAM:

- Basic Parameters settings: Use the settings on the Basic Parameters tab to configure the GQAM.
- Connectivity settings: Use the settings on the Connectivity tab to configure the connections between the modulator and its associated MPEG source

**Note:** Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### Basic Parameters - Content GQAM Modulator

Use the following fields when you manage the basic parameters for a content GQAM modulator.

| Field | Description | |
|---|---|---|
| Headend Name | The headend associated with this content QAM. | |
| GQAM Name | The name of this QAM.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the QAM modulator and where it resides.<br>**Example:** A name of **VODhub1Q43** could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. | |
| IP Address | The IP address for this content QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. | |
| Physical Address | The MAC address for this content QAM. | |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. | |
| Default Gateway | The IP address of your default gateway (if used).<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. | |
| Dual GbE Port | Click to enable dual GbE port support (GQAM software release 4.0 or later required). | |
| | **IP Address** - For the primary GbE port | Enter the IP address of the primary GbE port. |
| | **Subnet Mask** - For the primary GbE port | Enter the subnet mask of the primary GbE port. |
| | **Physical Address** - For the primary GbE port | Enter the MAC address of the primary GbE port. |
| | **Second IP Address** - For the secondary GbE port | Enter the IP address of the secondary (backup) GbE port. |
| | **Second Subnet Mask** - For the secondary GbE port | Enter the subnet mask of the secondary (backup) GbE port. |
| | **Second Physical Address** - For the secondary GbE port | Enter the MAC address of the secondary (backup) GbE port. |
| | **Los Timer** - Loss of signal timer (milliseconds) | Enter the length of time (in milliseconds) you want the GQAM modulator to wait before switching from the active GbE port to the inactive GbE port when the modulator |

| | | |
|---|---|---|
| | | detects a loss of signal on the active GbE input port. |
| Switch Mode | Determines how the GQAM switches from the primary (active) GbE port to the secondary (inactive) GbE port. Select one of the following options:<br>▪**Auto** - The GQAM modulator switches from the active GbE input port to the inactive GbE input port whenever the modulator detects a loss of signal on the active port that meets or exceeds the setting for the Los timer.<br>▪**Manual** - Forces the GQAM modulator to use a specific GbE port. Typically, this setting is used for maintenance or troubleshooting.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking **Status**. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Initial Port | Determines which port (First or Second) the GQAM uses during boot up. Select the port that the modulator uses during boot up.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking Status. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Input Port | The type of interface that will receive data from the QAM.<br>If the QAM modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see |

| | |
|---|---|
| | a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM.<br>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 that will receive data from this modulator.<br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |
| **Application Support** - Defines the application that each RF output carrier provides | Click the arrow of each RF carrier and select the application that each RF output carrier provides:<br>▪**Shared** - Select this option when the RF carrier is used for VOD, SDV, and Broadcast sessions.<br>▪**VOD Only** -Select this option when the RF carrier is used only for VOD sessions.<br>▪**SDV Only** - Select this option when the RF carrier is used only for SDV sessions.<br>▪**Broadcast Only** -Select this option when the RF carrier is used only for broadcast sessions. |

### Connections - Content GQAM Modulator

Use the following fields when you manage the connections for a content GQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the GQAM resides. |
| Device Type | The type of MPEG source device being used to send data to this GQAM.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device. |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

### Recommended Modulator Frequencies

Use the center frequencies shown in the following table to send data from your QAM modulators to the DHCTs on your system. Notice that these frequencies are separated by increments of 6 MHz.

**Note:** If you are experiencing signal interference, try offsetting your modulator frequencies by 250 kHz from the frequencies shown in the table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 153 | 159 | 165 | 171 | 177 | 183 | 189 | 195 | 201 | 207 |
| 213 | 219 | 225 | 231 | 237 | 243 | 249 | 255 | 261 | 267 |
| 273 | 279 | 285 | 291 | 297 | 303 | 309 | 315 | 321 | 327 |
| 333 | 339 | 345 | 351 | 357 | 363 | 369 | 375 | 381 | 387 |
| 393 | 399 | 405 | 411 | 417 | 423 | 429 | 435 | 441 | 447 |
| 453 | 459 | 465 | 471 | 477 | 483 | 489 | 495 | 501 | 507 |
| 513 | 519 | 525 | 531 | 537 | 543 | 549 | 555 | 561 | 567 |
| 573 | 579 | 585 | 591 | 597 | 603 | 609 | 615 | 621 | 627 |
| 633 | 639 | 645 | 651 | 657 | 663 | 669 | 675 | 681 | 687 |
| 693 | 699 | 705 | 711 | 717 | 723 | 729 | 735 | 741 | 747 |

## Add a Content GQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > GQAM**

This topic describes how to use the Set Up GQAM window to add a GQAM modulator with any of the following input port configurations to the DNCS:

- A GQAM modulator with four ASI input ports and one GbE input port
- A GQAM modulator with four ASI input ports and dual GbE input ports

If you are using a GQAM modulator to send content to DHCTs and you have already added an MPEG source to the DNCS database, you are ready to add the GQAM modulator to the DNCS database.

### You Need to Know

### Before You Begin

Before you begin, you must have your network map. You must also have the following information. (Note that different information is required depending on the input that the modulator accepts.)

- Name of the headend containing the modulator
- Name used to identify the modulator
- Type of modulation the modulator uses
- If applicable, the default gateway that the modulator uses
- Number identifying the transport stream going from the modulator out to the hubs on your system
- Frequency of the channel being used to send data from the modulator to the hubs on your system
- Names of the hubs you want to receive data from this modulator
- Name of the headend containing the associated MPEG source
- Type of MPEG source device being used to send data to this modulator (for example, IRT, MDR, VOD server, and so forth)
- Name of the associated MPEG source
- If the modulator accepts ASI input, obtain the following information:
  - IP address for the ASI port (from your system administrator)
  - MAC address for the ASI port (click for information on locating the MAC address)
  - Subnet mask for the ASI port (from your system administrator)
- If the modulator accepts GbE input, obtain the following information:
  - The IP address for the GbE port (and for the secondary GbE port, if used)
  - The subnet mask for the GbE port (and for the secondary GbE port, if used)
  - The MAC address of the GbE port (and for the secondary GbE port, if used)

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Related Topics

- Setting Up Basic Parameters
- Setting Up Content GQAM Modulator Connections
- Activating a Content GQAM Modulator
- Locate the MAC Address of a QAM

### Setting Up Content GQAM Modulator Basic Parameters

The first step in adding a content GQAM modulator is to complete these steps to set up the basic parameters for the modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **GQAM**. The GQAM List window opens.
4. Click **File > New > GQAM**. The Set Up GQAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameters - Content GQAM Modulator.

Use the following fields when you manage the basic parameters for a content GQAM modulator.

| Field | Description | |
|---|---|---|
| Headend Name | The headend associated with this content QAM. | |
| GQAM Name | The name of this QAM.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the QAM modulator and where it resides.<br>**Example:** A name of **VODhub1Q43** could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. | |
| IP Address | The IP address for this content QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. | |
| Physical Address | The MAC address for this content QAM. | |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. | |
| Default Gateway | The IP address of your default gateway (if used).<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. | |
| Dual GbE Port | Click to enable dual GbE port support (GQAM software release 4.0 or later required). | |
| | **IP Address** - For the primary GbE port | Enter the IP address of the primary GbE port. |
| | **Subnet Mask** - For the primary GbE port | Enter the subnet mask of the primary GbE port. |
| | **Physical Address** - For the primary GbE port | Enter the MAC address of the primary GbE port. |

| | | |
|---|---|---|
| | **Second IP Address** - For the secondary GbE port | Enter the IP address of the secondary (backup) GbE port. |
| | **Second Subnet Mask** - For the secondary GbE port | Enter the subnet mask of the secondary (backup) GbE port. |
| | **Second Physical Address** - For the secondary GbE port | Enter the MAC address of the secondary (backup) GbE port. |
| | **Los Timer** - Loss of signal timer (milliseconds) | Enter the length of time (in milliseconds) you want the GQAM modulator to wait before switching from the active GbE port to the inactive GbE port when the modulator detects a loss of signal on the active GbE input port. |
| Switch Mode | Determines how the GQAM switches from the primary (active) GbE port to the secondary (inactive) GbE port. Select one of the following options:<br>▪ **Auto** - The GQAM modulator switches from the active GbE input port to the inactive GbE input port whenever the modulator detects a loss of signal on the active port that meets or exceeds the setting for the Los timer.<br>▪ **Manual** - Forces the GQAM modulator to use a specific GbE port. Typically, this setting is used for maintenance or troubleshooting.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking **Status**. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Initial Port | Determines which port (First or Second) the GQAM uses during boot up. Select the port that the modulator uses during boot up.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking Status. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Input Port | The type of interface that will receive data from the QAM.<br>If the QAM modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br>**Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps. |

| | |
|---|---|
| | ▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br><br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br><br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br><br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br><br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br><br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br><br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br><br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM.<br><br>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 that will receive data from this modulator.<br><br>If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |
| **Application Support** - Defines the application that each RF output carrier provides | Click the arrow of each RF carrier and select the application that each RF output carrier provides: |

| | |
|---|---|
| | ▪ **Shared** - Select this option when the RF carrier is used for VOD, SDV, and Broadcast sessions.<br>▪ **VOD Only** -Select this option when the RF carrier is used only for VOD sessions.<br>▪ **SDV Only** - Select this option when the RF carrier is used only for SDV sessions.<br>▪ **Broadcast Only** -Select this option when the RF carrier is used only for broadcast sessions. |

**Important:** Unless you are setting up multicast sessions or setting up stat mux dejitter groups (SMDGs) on this modulator, you should not need to use the Advanced Parameters tab because the system automatically selects the appropriate configuration file for you. This file tells the modulator which version of GQAM software to use. Unless you are setting up multicast sessions or SMDGs, do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance.

6. Click **Apply**. The system saves the change you have made to the Basic Parameters tab.

7. Your next step is to set up the connections between the content GQAM modulator and its associated MPEG source. Go to Setting Up Content GQAM Modulator Connections.

### Setting Up Content GQAM Modulator Connections

After you set up the basic parameters for the content GQAM modulator, complete these steps to set up the connections between the modulator and its associated MPEG source.

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with a graphical representation of the devices already connected to this modulator.
2. If not already selected, click to select the **Input Port** option.
3. Complete the fields on the screen as described in Connections - Content GQAM Modulator.

Use the following fields when you manage the connections for a content GQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the GQAM resides. |
| Device Type | The type of MPEG source device being used to send data to this GQAM.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device. |
| The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.<br>**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator. | |

4. Click **Apply**. The system saves this information in the DNCS database and updates the illustration so that it shows the information you entered.
5. Your next step is to activate the modulator by placing it online. Go to Activating a Content GQAM Modulator.

### Activate a Content GQAM

After you set up the connections between a content GQAM modulator and its associated MPEG source, complete these steps to activate the modulator by placing it online.

**Important:** You can activate a GQAM modulator only after all parameters for the modulator have been saved to the DNCS database, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. If you have not already done so, add the content GQAM to the DNCS.
2. On the Set Up GQAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
3. At the Administrative State field, click the **Online** option.
4. Click **Save**. The system saves the modulator information in the DNCS database and closes the Set Up GQAM window. The GQAM List window updates to include the new modulator.

   Note: The new GQAM modulator is listed 16 times to show its 16 output streams.

5. Add the new content GQAM modulator to your network map.
6. Click **File > Close** to close the QAM List and return to the DNCS.

### Related Topics

- Set Up Your Network

## Locate the MAC Address of a QAM

You can look at the sticker on the side of the QAM, MQAM, SCS MQAM, GQAM, or GoQAM to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

## Reset a Content GQAM

**Quick Path: DNCS > Network Element Provisioning > QAM > [Select QAM] > File > Reset**

Resetting a QAM, MQAM, GQAM, or GoQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

**Important:** You can reset only our modulators from the DNCS. Generic QAM modulators cannot be reset from the DNCS. To reset a generic QAM modulator, refer to the documentation provided by the manufacturer of the modulator.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Select the QAM, MQAM, GQAM, or GoQAM modulator that you want to reboot.

**Notes:**

- Each MQAM modulator is listed four times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GQAM modulator is listed 16 times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GoQAM (RF or IF) is listed twice (once for each of the modulator's RF output channels), but select only the first occurrence.

5. Click **File > Reset**. The confirmation window appears with the question, "Are you sure you want to reset QAM modulator 'name of modulator'?"
6. Click **Yes**. The QAM List window displays the following message, "The reset request has been received by QAM modulator 'name of modulator'."

## Modify a Content GQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM/MQAM Name] > File > Open**

After a GQAM modulator is saved in the DNCS database, you can modify any of its parameters except for the headend to which it is assigned.

### Modifying a Content GQAM Modulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the GQAM modulator you want to modify.
5. Click **File > Open**. The Set Up GQAM window opens as appropriate.
6. To change the basic parameters, refer to Basic Parameters - Content GQAM Modulator.

Use the following fields when you manage the basic parameters for a content GQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content QAM. |
| GQAM Name | The name of this QAM.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the QAM modulator and where it resides.<br>**Example:** A name of **VODhub1Q43** could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| IP Address | The IP address for this content QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for this content QAM. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Default Gateway | The IP address of your default gateway (if used).<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Dual GbE Port | Click to enable dual GbE port support (GQAM software release 4.0 or later required). |
| **IP Address** - For the primary GbE port | Enter the IP address of the primary GbE port. |

| | | |
|---|---|---|
| | **Subnet Mask** - For the primary GbE port | Enter the subnet mask of the primary GbE port. |
| | **Physical Address** - For the primary GbE port | Enter the MAC address of the primary GbE port. |
| | **Second IP Address** - For the secondary GbE port | Enter the IP address of the secondary (backup) GbE port. |
| | **Second Subnet Mask** - For the secondary GbE port | Enter the subnet mask of the secondary (backup) GbE port. |
| | **Second Physical Address** - For the secondary GbE port | Enter the MAC address of the secondary (backup) GbE port. |
| | **Los Timer** - Loss of signal timer (milliseconds) | Enter the length of time (in milliseconds) you want the GQAM modulator to wait before switching from the active GbE port to the inactive GbE port when the modulator detects a loss of signal on the active GbE input port. |
| Switch Mode | Determines how the GQAM switches from the primary (active) GbE port to the secondary (inactive) GbE port. Select one of the following options:<br>▪ **Auto** - The GQAM modulator switches from the active GbE input port to the inactive GbE input port whenever the modulator detects a loss of signal on the active port that meets or exceeds the setting for the Los timer.<br>▪ **Manual** - Forces the GQAM modulator to use a specific GbE port. Typically, this setting is used for maintenance or troubleshooting.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking **Status**. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Initial Port | Determines which port (First or Second) the GQAM uses during boot up. Select the port that the modulator uses during boot up.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking Status. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Input Port | The type of interface that will receive data from the QAM.<br>If the QAM modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**.<br>**Note:** The type of modulation affects the |

| | |
|---|---|
| | total bandwidth available for setting up sessions on the modulator:<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM.<br>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 that will receive data from this modulator. |

| | |
|---|---|
| | If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |
| **Application Support** - Defines the application that each RF output carrier provides | Click the arrow of each RF carrier and select the application that each RF output carrier provides:<br>▪ **Shared** - Select this option when the RF carrier is used for VOD, SDV, and Broadcast sessions.<br>▪ **VOD Only** -Select this option when the RF carrier is used only for VOD sessions.<br>▪ **SDV Only** - Select this option when the RF carrier is used only for SDV sessions.<br>▪ **Broadcast Only** -Select this option when the RF carrier is used only for broadcast sessions. |

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

7.To change the connectivity parameters, refer to Connections - Content GQAM Modulator.

Use the following fields when you manage the connections for a content GQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the GQAM resides. |
| Device Type | The type of MPEG source device being used to send data to this GQAM.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device. |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

8.When you finish making changes, click **Save**. The system saves the new QAM information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new modulator information.

9.Update your network map to reflect these changes.

10.Do you need to modify another QAM?

- If **yes**, repeat this procedure from step 4.
- If no, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

## Modify a Content GQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM/MQAM Name] > File > Open**

After a GQAM modulator is saved in the DNCS database, you can modify any of its parameters except for the headend to which it is assigned.

### Modifying a Content GQAM Modulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the GQAM modulator you want to modify.
5. Click **File > Open**. The Set Up GQAM window opens as appropriate.
6. To change the basic parameters, refer to Basic Parameters - Content GQAM Modulator.

Use the following fields when you manage the basic parameters for a content GQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this content QAM. |
| GQAM Name | The name of this QAM.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the QAM modulator and where it resides.<br>**Example:** A name of **VODhub1Q43** could represent a QAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| IP Address | The IP address for this content QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for this content QAM. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0**. Otherwise, type the subnet mask as assigned by your system administrator. |
| Default Gateway | The IP address of your default gateway (if used).<br>Using a default gateway speeds up the reconnection process that occurs after a QAM is rebooted. |
| Dual GbE Port | Click to enable dual GbE port support (GQAM software release 4.0 or later required). |
| **IP Address** - For the primary | Enter the IP address of the primary GbE port. |

| | | |
|---|---|---|
| | GbE port | |
| | **Subnet Mask** - For the primary GbE port | Enter the subnet mask of the primary GbE port. |
| | **Physical Address** - For the primary GbE port | Enter the MAC address of the primary GbE port. |
| | **Second IP Address** - For the secondary GbE port | Enter the IP address of the secondary (backup) GbE port. |
| | **Second Subnet Mask** - For the secondary GbE port | Enter the subnet mask of the secondary (backup) GbE port. |
| | **Second Physical Address** - For the secondary GbE port | Enter the MAC address of the secondary (backup) GbE port. |
| | **Los Timer** - Loss of signal timer (milliseconds) | Enter the length of time (in milliseconds) you want the GQAM modulator to wait before switching from the active GbE port to the inactive GbE port when the modulator detects a loss of signal on the active GbE input port. |
| Switch Mode | Determines how the GQAM switches from the primary (active) GbE port to the secondary (inactive) GbE port. Select one of the following options:<br>▪ **Auto** - The GQAM modulator switches from the active GbE input port to the inactive GbE input port whenever the modulator detects a loss of signal on the active port that meets or exceeds the setting for the Los timer.<br>▪ **Manual** - Forces the GQAM modulator to use a specific GbE port. Typically, this setting is used for maintenance or troubleshooting.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking **Status**. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Initial Port | Determines which port (First or Second) the GQAM uses during boot up. Select the port that the modulator uses during boot up.<br>Available only when you use a dual-GbE port GQAM (GQAM software version 4.0 or higher required).<br>**Note:** You can verify which GbE input port is active by clicking Status. When you click Status, the DNCS displays the GbE input port that is active along with the current date and time. Port 5 indicates the primary GbE port is active. Port 6 indicates the secondary (backup) GbE port is active. | |
| Input Port | The type of interface that will receive data from the QAM.<br>If the QAM modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256 QAM**. |

| | |
|---|---|
| | **Note:** The type of modulation affects the total bandwidth available for setting up sessions on the modulator:<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps. |
| **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.<br>For systems offering VOD service, enabling this option may be helpful when reallocating service group resources or in the rare event that the video server is out of service. When enabled, the DNCS rejects VOD resource requests associated with the port selected. |
| **Interleaver Depth** - Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM.<br>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 that will receive data from this modulator. |

| | |
|---|---|
| | If this QAM modulator will send data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field. |
| **Application Support** - Defines the application that each RF output carrier provides | Click the arrow of each RF carrier and select the application that each RF output carrier provides:<br>▪ **Shared** - Select this option when the RF carrier is used for VOD, SDV, and Broadcast sessions.<br>▪ **VOD Only** -Select this option when the RF carrier is used only for VOD sessions.<br>▪ **SDV Only** - Select this option when the RF carrier is used only for SDV sessions.<br>▪ **Broadcast Only** -Select this option when the RF carrier is used only for broadcast sessions. |

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

7.To change the connectivity parameters, refer to ▸ Connections - Content GQAM Modulator.

Use the following fields when you manage the connections for a content GQAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the GQAM resides. |
| Device Type | The type of MPEG source device being used to send data to this GQAM.<br>**Example:** IRT, MDR and Service Group Object. |
| Device Name | The name of the source device. |
| The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.<br>**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator. | |

**Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

8.When you finish making changes, click **Save**. The system saves the new QAM information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new modulator information.

9.Update your network map to reflect these changes.

10.Do you need to modify another QAM?

- If **yes**, repeat this procedure from step 4.
- If no, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

## Delete a Content QAM, MQAM, or GQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [Select modulator] > File > Delete**

**Important:** Do not attempt to delete a BFS modulator. Contact us for assistance in deleting a BFS modulator.

Complete these steps to delete a QAM, MQAM, or GQAM modulator that carries content.

1. First tear down all sessions that are running on the modulator you want to delete.

   **Note:** Before you delete a modulator, first tear down all of the sessions associated with the modulator. If you delete a modulator without first tearing down its related sessions, system performance may be degraded. Performance degrades because the DNCS uses its resources attempting to associate sessions with a modulator that no longer exists.

2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List window opens.
5. Click once on the row containing the QAM that you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the selected modulator information from the DNCS database and from the QAM List window.
8. Delete the selected modulator from your network map.
9. Do you need to delete another QAM modulator.
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

## Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display Sessions > [Select Session] > Tear Down**

**Important:** Unless you have been instructed by Cisco Services, only tear down sessions on content QAM modulators. Do not tear down sessions on BFS QAM modulators.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to Use the Filter to Display Sessions.
2. When the list of sessions displays, use one of the following methods to select the sessions you would like to tear down:
   - To tear down specific sessions, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete.
   - To tear down all sessions, click **Select All Displayed Sessions**.

   **Note:** If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.
3. Click **Tear Down**. The system tears down the sessions you selected and updates the status of all sessions.
4. Click **File > Close** to close the Session Data window.
5. Depending on your reason for tearing down the session, you may decide to complete one of the following tasks:
   - If you tore down the session in order to delete a QAM modulator, you can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind. For assistance, see Delete a Content QAM Modulator.
   - If you deleted the session in order to correct an unlisted, active session, restart the session. For assistance, see Restart a Session.

**Related Topics**

- Why Tear Down Sessions?

### Why Tear Down Sessions?

This section describes how to tear down sessions for either of the following reasons:

- You need to delete a QAM modulator that carries content.

  **Note:** Before deleting a QAM modulator that carries content, first tear down sessions associated with the modulator. Deleting a modulator without first tearing down its related sessions can degrade system performance. Performance can degrade because the DNCS uses its resources to attempt to associate sessions with a modulator that no longer exists. These sessions are called orphaned sessions.

- You need to tear down and restart an unlisted, active session in order to correct it.

## Multicast Sessions

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > GQAM > Advanced Parameters tab > Multicast Sessions: Set up**

This section describes how to use the Multicast Digital Session Definition window to set up multicast sessions on a GQAM modulator and on any stat mux dejitter groups (SMDGs) that have been set up for a GQAM modulator:

- **GQAM modulator** - If you are using a GQAM modulator to send multicast sessions to the network and you already added a GQAM modulator to the DNCS and created a source for the session, you can follow the procedure in this topic to set up multicast sessions on the GQAM modulator.
- **GQAM SMDGs** - If you are using a GQAM modulator that receives input from a statistical multiplexor (stat mux) to send multicast sessions to the network and you already added SMDGs to the DNCS and created a source for the session, you can follow the procedure in this topic to set up multicast sessions on the GQAM SMDGs. You can set up a maximum of 60 sessions on an SMDG.

  **Important:** SMDG sessions must use the same input port and output port that the SMDG uses. Otherwise, the session may fail.

### Related Topics

- Multicast Session Settings - GQAM Modulator
- Information Needed for Multicast Sessions
- Set Up Multicast Sessions on a GQAM

### Multicast Session Settings - GQAM Modulator

Use the following fields when you manage multicast sessions on a GQAM modulator.

| Field | Description |
|---|---|
| Source ID | Source that the session will use. |
| Session ID | Left Session ID field.<br>Enter 12 zeros (**00:00:00:00:00:00**). |
| | Right Session ID field.<br>The Source ID you used when you added the source to the DNCS. |
| Bandwidth | The maximum amount of bandwidth (in Mbps) that the system should allow for this device.<br>This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>▪Standard MPEG video streams use **2** or **3** Mbps.<br>▪HDTV streams use **13** Mbps.<br>▪Audio streams use **0.2** Mbps.<br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| Output Carrier | The output destination of the source. |
| Program Number | The MPEG program number being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Source IP Address 1 | The IP address of the first device. |
| Source IP Address 2 | The IP address of the second device (if used). |
| Source IP Address 3 | The IP address of the third device (if used). |
| Input Destination Multicast IP Address | The multicast IP address on the GQAM modulator where sources are input. |
| UDP Port | The port number on the modulator where the sources are input.<br>**Important:** If you are using GQAMs, and the multicast session is being set up as an SMDG session, the session's input port must match the input port of the SMDG. Otherwise, the session may fail. |

Related Topics

- Information Needed for Multicast Sessions
- Set Up Multicast Sessions on a GQAM
- Stat Mux Dejitter Groups

### Information Needed for Multicast Sessions

You need the following information to set up a multicast session on the GQAM modulator:

- Source ID as you defined it when you added the content source to the DNCS
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the content from the source (refer to your network map)
- MPEG program number (from your content service provider)
- IP addresses of source devices (up to 3 different source devices can be used)
- Input destination multicast ID address on the GQAM modulator
- Destination UDP port on the GQAM modulator

**Important:** To support multicast sessions, GQAM software version 4.0 or later must be installed on the GQAM modulator.

### Related Topics

- Multicast Session Settings
- Set Up Multicast Sessions on a GQAM

### Set Up Multicast Sessions on a GQAM

**Important:** To support multicast sessions, GQAM software version 4.0 or later must be installed on the GQAM modulator.

# Stat Mux Dejitter Groups (SMDGs)

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

**Quick Path from GQAM: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Stat Mux Dejitter Groups: Set up**

This topic describes how to use the Stat Mux Dejitter Groups window to set up stat mux dejitter groups (SMDGs) on GQAM modulators that receive multiplexed sources.

Setting up SMDGs enables a GQAM modulator to appropriately process multiplexed sources. Failing to set up SMDGs on GQAM modulators that receive multiplexed sources may result in tiling of the video on set-tops. SMDGs identify each GQAM input and output that will carry the multiplex and they also allow the modulator to appropriately process the multiplexed sources.

**Related Topics**

- Set up stat mux dejitter groups
- Set up multicast sessions on GQAM SMDGs
- View stat mux dejitter group settings

### Stat Mux Dejitter Group Settings

Use the following fields when you manage SMDGs.

| Field | Description |
|---|---|
| ID | An identifier to indicate the SMDG. This must be a numerical value from 1 to 65535. |
| QAM Name | The QAM that carries this SMDG. |
| Bandwidth | The bandwidth that the modulator uses:<br>▪QAM-64<br>▪QAM-256 |
| Input Port | The input port that this SMDG uses. |
| Destination IP Address | The IP address of the receiving device, based on the following criteria:<br>▪If a GbE port receives the source, enter the IP multicast address for the GQAM modulator.<br>▪If an ASI port receives the source, do not enter data in this field.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Destination UDP Port | The UDP port of the receiving device, based on the following criteria:<br>▪If a GbE port receives the source, enter the UDP port on the GQAM modulator that receives the multiplexed source.<br>▪If an ASI port receives the source, do not enter data in this field. |
| Output Port | The output port that this SMDG uses. |

Related Topics

- Information Needed to Set up Stat Mux Dejitter Groups
- Set Up Stat Mux Dejitter Groups

## Set Up Stat Mux Dejitter Groups Overview

You can set up a maximum of 16 SMDGs on a GQAM modulator  one SMDG for each RF output port on the GQAM modulator. Each SMDG can accommodate a maximum of 60 sessions.

If you are using a GQAM modulator that receives sources from a statistical multiplexor (stat mux) and you have already added the GQAM modulator to the DNCS, you can set up SMDGs on the modulator. SMDGs identify each GQAM input and output that will carry the multiplex and they also allow the modulator to appropriately process the multiplexed sources. After setting up SMDGs on the GQAM modulator, you can set up sessions for groups to carry.

**Important:** Setting up an SMDG enables the GQAM modulator to appropriately process multiplexed sources. Failing to set up SMDGs on GQAM modulators that receive multiplexed sources may result in tiling of the video on DHCTs.

### Related Topics

- Information Needed to Set Up Stat Mux Dejitter Groups
- Set Up Stat Mux Dejitter Groups
- Stat Mux Dejitter Groups Settings

### Information Needed to Set Up Stat Mux Dejitter Groups

Before you begin, make certain that you have the following software installed on your system:

- GQAM software release 4.0 or later
- DNCS SR 2.7/3.7/4.2 SP2 or later

You will also need the following information:

- Your network map
- The input ports that receive the multiplexed source (ASI inputs, Ethernet inputs, or both)
- If a GbE port is used for multicasting, the destination multicast IP address (IP multicast address) for the GQAM modulator
- If a GbE port is used for unicasting, the destination UDP port number on the GQAM modulator that receives the source
- GQAM output port number that modulates the source onto the network

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Related Topics

- Set Up Stat Mux Dejitter Groups
- Stat Mux Dejitter Group Settings

### Setting Up Stat Mux Dejitter Groups

Complete these instructions to set up SMDGs by mapping the input port that receives the multiplexed source to the output port that modulates the source onto the network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **GQAM**. The GQAM List window opens.
4. Select the GQAM modulator on which you want to set up an SMDG. Then select **File > Open**. The Set Up GQAM window opens with the Basic Parameters tab in the forefront.
5. Click the **Advanced Parameters** tab.
6. Click the **Set Up** button for Stat Mux Dejitter Groups. The Stat Mux Dejitter Groups window opens for the selected GQAM modulator.
7. Click **Add**. Empty fields appear at the top of the window.
8. Complete the fields on the screen as described in Stat Mux Dejitter Group Settings.

Use the following fields when you manage SMDGs.

| Field | Description |
|---|---|
| ID | An identifier to indicate the SMDG. This must be a numerical value from 1 to 65535. |
| QAM Name | The QAM that carries this SMDG. |
| Bandwidth | The bandwidth that the modulator uses:<br>▪ QAM-64<br>▪ QAM-256 |
| Input Port | The input port that this SMDG uses. |
| Destination IP Address | The IP address of the receiving device, based on the following criteria:<br>▪ If a GbE port receives the source, enter the IP multicast address for the GQAM modulator.<br>▪ If an ASI port receives the source, do not enter data in this field.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Destination UDP Port | The UDP port of the receiving device, based on the following criteria:<br>▪ If a GbE port receives the source, enter the UDP port on the GQAM modulator that receives the multiplexed source.<br>▪ If an ASI port receives the source, do not enter data in this field. |
| Output Port | The output port that this SMDG uses. |

Related Topics

- Information Needed to Set up Stat Mux Dejitter Groups
- Set Up Stat Mux Dejitter Groups

9. Click **Save**. Parameters for the SMDG are listed in the Stat Mux Dejitter Group window.

10. Do you need to add another SMDG to this GQAM modulator?

- If **yes**, repeat this procedure from step 7.
- If **no**, go to step 11.

11. Do you need to add SMDGs to another GQAM modulator?

- If **yes**, repeat this procedure from step 4.
- If **no**, you have successfully added SMDGs to the GQAM modulators that receive multiplexed sources and are ready to set up sessions for these SMDGs. For assistance setting up multicast sessions, see Set Up Multicast Sessions on a GQAM. For assistance setting up CF sessions, see Define a Digital Source and Session.

## Related Topics

- Content GQAM Modulator Settings
- Reset a Content GQAM
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

## Transport Stream Route (TSR)

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up**

The FCC requires Program and System Information Protocol (PSIP) support for off-air content. A transport stream route (TSR) is required to support PSIP on a GQAM. This feature provides the following enhancements:

- Enables a passthrough mode on a GQAM for PSIP support
- Allows GQAMs to be used for tru2way™ (formerly OCAP™) common download
- Allows system operators to select and encrypt a single multi-program transport stream (MPTS)
- Allows GQAMs to be used with a Network Overlay Bulk Encryptor (NOBE) at Overlay sites
- Allows for re-purpose and re-use of GoQAMs

**Important:** System Release (SR) 4.3 is required to configure this feature on the GQAM.

## What do you want to do?

- Learn about Transport Stream Route Settings
- Set Up a Transport Stream Route
- Modify a Transport Stream Route
- Delete a Transport Stream Route

### Transport Stream Route Settings

Use the following fields when you manage TSRs.

| Field | Description |
|---|---|
| Route ID | A unique number that identifies this TSR.<br>**Valid values:** Any 2-byte integer in the range of 1 to 65535. |
| Starting ECM Pid | Provides the starting PID value for the ECM PIDs for the TSR. This field, along with the Number of ECM Pids field, defines the range of PIDs for the TSR.<br>PIDs from this range are used for inserting PowerKEY ECMs when encrypted sessions exist 'on top of' the TSR. |
| Number of ECM Pids | Provides the number of PIDs available for ECM PID allocation for the TSR. This field, along with the Starting ECM Pid field, defines the range of PIDs for the TSR. |
| Input | |
| Qam Input Port | Select the input port of the source to the GQAM.<br>**Valid values:**<br>▪**0 - 3**: ASI ports 0 to 3, respectively<br>▪**4:** GigE port<br>**Note:** If the GQAM is a dual-GigE port GQAM, selecting port 4 selects the logical GigE port, which could physically be either port 4 or port 5. |
| Stream Delivery Type | Select one of the following options:<br>▪Unicast<br>▪Multicast IP Only<br>▪Multicast IP + UDP Port<br>▪Virtual IP + UDP Port |
| Source IP Address | The IP address of the source device. |
| Source IP Address 2 | The IP address of the second source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪Multicast IP Only<br>▪Multicast IP + UDP Port<br>▪Virtual IP + UDP Port |
| Source IP Address 3 | The IP address of the third source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪Multicast IP Only<br>▪Multicast IP + UDP Port |

| | |
|---|---|
| | ▪Virtual IP + UDP Port |
| Destination IP Address | The GbE IP address of the destination device or the multicast group destination (GDA) to which the content will flow.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪Multicast IP Only<br>▪Multicast IP + UDP Port<br>▪Virtual IP + UDP Port |
| UDP Port | The UDP port of the destination device to which the content will flow.<br>Active only if you select either one of the following options in Stream Delivery Type:<br>▪Multicast IP + UDP Port<br>▪Virtual IP + UDP Port |
| Output | |
| Qam Output Port | Select the output port (1 to 16) on the GQAM used for this stream. |

**Related Topics**

- Set Up a Transport Stream Route
- Modify a Transport Stream Route
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

### Set Up a Transport Stream Route

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up > Add**

### Setting Up a Transport Stream Route

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List opens.
4. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
5. Click the **Advanced Parameters** tab.
6. Click **Transport Stream Route: Set up**. The Transport Stream Route List for [GQAM name] window opens.
7. Click **Add**. The Transport Stream Route window opens.
8. Complete the fields on the screen as described in Transport Stream Route Settings.

Use the following fields when you manage TSRs.

| Field | Description |
|---|---|
| Route ID | A unique number that identifies this TSR.<br>**Valid values:** Any 2-byte integer in the range of 1 to 65535. |
| Starting ECM Pid | Provides the starting PID value for the ECM PIDs for the TSR. This field, along with the Number of ECM Pids field, defines the range of PIDs for the TSR.<br>PIDs from this range are used for inserting PowerKEY ECMs when encrypted sessions exist 'on top of' the TSR. |
| Number of ECM Pids | Provides the number of PIDs available for ECM PID allocation for the TSR. This field, along with the Starting ECM Pid field, defines the range of PIDs for the TSR. |
| Input | |
| Qam Input Port | Select the input port of the source to the GQAM.<br>**Valid values:**<br>▪ **0 - 3**: ASI ports 0 to 3, respectively<br>▪ **4:** GigE port<br>**Note:** If the GQAM is a dual-GigE port GQAM, selecting port 4 selects the logical GigE port, which could physically be either port 4 or port 5. |
| Stream Delivery Type | Select one of the following options:<br>▪ Unicast<br>▪ Multicast IP Only |

| | |
|---|---|
| | ▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address | The IP address of the source device. |
| Source IP Address 2 | The IP address of the second source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address 3 | The IP address of the third source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Destination IP Address | The GbE IP address of the destination device or the multicast group destination (GDA) to which the content will flow.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| UDP Port | The UDP port of the destination device to which the content will flow.<br>Active only if you select either one of the following options in Stream Delivery Type:<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Output | |
| Qam Output Port | Select the output port (1 to 16) on the GQAM used for this stream. |

9. Click **Save**. The system saves the TSR and applies it to the ECM PIDs you entered. The Transport Stream Route List updates to include the new TSR information.

10. Do you need to create another TSR on this GQAM modulator?

- If **yes**, repeat this procedure from step 7 for each additional TSR that this GQAM modulator will carry.
- If **no**, click **Exit** to close the Transport Stream Route List window.

## Related Topics

- Modify a Transport Stream Route
- Delete a Transport Stream Route
- Transport Stream Route (TSR)
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

### Set Up a Transport Stream Route

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up > Add**

### Setting Up a Transport Stream Route

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List opens.
4. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
5. Click the **Advanced Parameters** tab.
6. Click **Transport Stream Route: Set up**. The Transport Stream Route List for [GQAM name] window opens.
7. Click **Add**. The Transport Stream Route window opens.
8. Complete the fields on the screen as described in Transport Stream Route Settings.

Use the following fields when you manage TSRs.

| Field | Description |
|---|---|
| Route ID | A unique number that identifies this TSR.<br>**Valid values:** Any 2-byte integer in the range of 1 to 65535. |
| Starting ECM Pid | Provides the starting PID value for the ECM PIDs for the TSR. This field, along with the Number of ECM Pids field, defines the range of PIDs for the TSR.<br>PIDs from this range are used for inserting PowerKEY ECMs when encrypted sessions exist 'on top of' the TSR. |
| Number of ECM Pids | Provides the number of PIDs available for ECM PID allocation for the TSR. This field, along with the Starting ECM Pid field, defines the range of PIDs for the TSR. |
| Input | |
| Qam Input Port | Select the input port of the source to the GQAM.<br>**Valid values:**<br>▪ **0 - 3**: ASI ports 0 to 3, respectively<br>▪ **4:** GigE port<br>**Note:** If the GQAM is a dual-GigE port GQAM, selecting port 4 selects the logical GigE port, which could physically be either port 4 or port 5. |
| Stream Delivery Type | Select one of the following options:<br>▪ Unicast |

| | |
|---|---|
| | ▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address | The IP address of the source device. |
| Source IP Address 2 | The IP address of the second source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address 3 | The IP address of the third source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Destination IP Address | The GbE IP address of the destination device or the multicast group destination (GDA) to which the content will flow.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| UDP Port | The UDP port of the destination device to which the content will flow.<br>Active only if you select either one of the following options in Stream Delivery Type:<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Output | |
| Qam Output Port | Select the output port (1 to 16) on the GQAM used for this stream. |

9. Click **Save**. The system saves the TSR and applies it to the ECM PIDs you entered. The Transport Stream Route List updates to include the new TSR information.

10. Do you need to create another TSR on this GQAM modulator?

- If **yes**, repeat this procedure from step 7 for each additional TSR that this GQAM modulator will carry.
- If **no**, click **Exit** to close the Transport Stream Route List window.

## Related Topics

- Modify a Transport Stream Route
- Delete a Transport Stream Route
- Transport Stream Route (TSR)
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

### Modify a Transport Stream Route

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up > [select TSR] > Open**

### Modifying a Transport Stream Route

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List opens.
4. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
5. Click the **Advanced Parameters** tab.
6. Click **Transport Stream Route: Set up**. The Transport Stream Route List for [GQAM name] window opens.
7. Select the TSR you want to modify.
8. Click **Open**. The Transport Stream Route window opens.
9. Modify the fields as described in Transport Stream Route Settings.

Use the following fields when you manage TSRs.

| Field | Description |
|---|---|
| Route ID | A unique number that identifies this TSR.<br>**Valid values:** Any 2-byte integer in the range of 1 to 65535. |
| Starting ECM Pid | Provides the starting PID value for the ECM PIDs for the TSR. This field, along with the Number of ECM Pids field, defines the range of PIDs for the TSR.<br>PIDs from this range are used for inserting PowerKEY ECMs when encrypted sessions exist 'on top of' the TSR. |
| Number of ECM Pids | Provides the number of PIDs available for ECM PID allocation for the TSR. This field, along with the Starting ECM Pid field, defines the range of PIDs for the TSR. |
| Input | |
| Qam Input Port | Select the input port of the source to the GQAM.<br>**Valid values:**<br>▪ **0 - 3**: ASI ports 0 to 3, respectively<br>▪ **4:** GigE port<br>**Note:** If the GQAM is a dual-GigE port GQAM, selecting port 4 selects the logical GigE port, which could physically be either port 4 or port 5. |
| Stream Delivery Type | Select one of the following options: |

| | |
|---|---|
| | ▪ Unicast<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address | The IP address of the source device. |
| Source IP Address 2 | The IP address of the second source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address 3 | The IP address of the third source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Destination IP Address | The GbE IP address of the destination device or the multicast group destination (GDA) to which the content will flow.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| UDP Port | The UDP port of the destination device to which the content will flow.<br>Active only if you select either one of the following options in Stream Delivery Type:<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Output | |
| Qam Output Port | Select the output port (1 to 16) on the GQAM used for this stream. |

10. Click **Save**. The system saves the TSR changes and applies them to the ECM PIDs you entered.
11. Do you need to modify another TSR on this GQAM modulator?
    - If **yes**, repeat this procedure from step 7.
    - If **no**, click **Exit** to close the Transport Stream Route List window.

## Related Topics

- Delete a Transport Stream Route
- Transport Stream Route (TSR)
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

### Modify a Transport Stream Route

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up > [select TSR] > Open**

### Modifying a Transport Stream Route

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List opens.
4. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
5. Click the **Advanced Parameters** tab.
6. Click **Transport Stream Route: Set up**. The Transport Stream Route List for [GQAM name] window opens.
7. Select the TSR you want to modify.
8. Click **Open**. The Transport Stream Route window opens.
9. Modify the fields as described in Transport Stream Route Settings.

Use the following fields when you manage TSRs.

| Field | Description |
|---|---|
| Route ID | A unique number that identifies this TSR.<br>**Valid values:** Any 2-byte integer in the range of 1 to 65535. |
| Starting ECM Pid | Provides the starting PID value for the ECM PIDs for the TSR. This field, along with the Number of ECM Pids field, defines the range of PIDs for the TSR.<br>PIDs from this range are used for inserting PowerKEY ECMs when encrypted sessions exist 'on top of' the TSR. |
| Number of ECM Pids | Provides the number of PIDs available for ECM PID allocation for the TSR. This field, along with the Starting ECM Pid field, defines the range of PIDs for the TSR. |
| Input | |
| Qam Input Port | Select the input port of the source to the GQAM.<br>**Valid values:**<br>▪ **0 - 3**: ASI ports 0 to 3, respectively<br>▪ **4:** GigE port<br>**Note:** If the GQAM is a dual-GigE port GQAM, selecting port 4 selects the logical GigE port, which could physically be either port 4 or port 5. |
| Stream Delivery Type | |

| | |
|---|---|
| | Select one of the following options:<br>▪ Unicast<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address | The IP address of the source device. |
| Source IP Address 2 | The IP address of the second source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Source IP Address 3 | The IP address of the third source device.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Destination IP Address | The GbE IP address of the destination device or the multicast group destination (GDA) to which the content will flow.<br>Active only if you select Ethernet 1 or 2 in Qam Input Port and one of the following options in Stream Delivery Type:<br>▪ Multicast IP Only<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| UDP Port | The UDP port of the destination device to which the content will flow.<br>Active only if you select either one of the following options in Stream Delivery Type:<br>▪ Multicast IP + UDP Port<br>▪ Virtual IP + UDP Port |
| Output | |
| Qam Output Port | Select the output port (1 to 16) on the GQAM used for this stream. |

10. Click **Save**. The system saves the TSR changes and applies them to the ECM PIDs you entered.
11. Do you need to modify another TSR on this GQAM modulator?
    - If **yes**, repeat this procedure from step 7.
    - If **no**, click **Exit** to close the Transport Stream Route List window.

**Related Topics**

- Delete a Transport Stream Route
- Transport Stream Route (TSR)
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

### Delete a Transport Stream Route

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up > Select TSR > Delete**

### Deleting a Transport Stream Route

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List opens.
4. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
5. Click the **Advanced Parameters** tab.
6. Click **Transport Stream Route: Set up**. The Transport Stream Route List for [GQAM name] window opens.
7. Select the TSR you want to delete.
8. Click **Delete**. A confirmation window opens.
9. Click **OK**. The system removes the TSR from the list and from the PID range.
10. Do you need to delete another TSR on this GQAM modulator?
    - If **yes**, repeat this procedure from step 7.
    - If **no**, click **Exit** to close the Transport Stream Route List window.

### Related Topics

- Transport Stream Route (TSR)
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

### Delete a Transport Stream Route

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Transport Stream Route: Set up > Select TSR > Delete**

### Deleting a Transport Stream Route

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List opens.
4. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
5. Click the **Advanced Parameters** tab.
6. Click **Transport Stream Route: Set up**. The Transport Stream Route List for [GQAM name] window opens.
7. Select the TSR you want to delete.
8. Click **Delete**. A confirmation window opens.
9. Click **OK**. The system removes the TSR from the list and from the PID range.
10. Do you need to delete another TSR on this GQAM modulator?
    - If **yes**, repeat this procedure from step 7.
    - If **no**, click **Exit** to close the Transport Stream Route List window.

### Related Topics

- Transport Stream Route (TSR)
- Modify a Content GQAM Modulator
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

# Generic QAM Model List Window

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM Models**

Using the Generic QAM Model List window to add a generic QAM model to the DNCS is the first step in adding generic QAM modulators to the DNCS. When you add a generic QAM model to the DNCS, you define specifications that are unique to a particular model of QAM modulator. After a generic QAM model exists in this window, you can use the model to add an individual generic QAM modulator to the DNCS; the individual modulator will be added with the specifications of the model you used.

After a generic QAM modulator model is listed in this window, you can modify or delete a model as the needs of your site change.

**Note:** The DNCS refers to table-based modulators, such as our eXtra Dense QAM array (XDQA) and table-based QAM modulators of other manufacturers, as **generic** QAM modulators.

## What do you want to do?

- Review the fields in this window
- Add a generic QAM Model to this window
- Modify a generic QAM model in this window
- Delete a generic QAM model from this window

## Generic QAM Model Settings

Use the Generic QAM Model window on the DNCS Administrative Console to manage the generic QAM models in your network. Two tabs in this window provide settings for the generic QAM model:

- Basic Parameter Settings - Generic QAM Model
- RF Carrier Model Settings - Generic QAM Model

### Basic Parameter Settings - Generic QAM Model

Use the following fields when you manage a generic QAM model in the DNCS.

| Field | Description |
|---|---|
| Model Number | The model number for this generic QAM model.<br>You can use up to 32 alphanumeric characters. |
| Number of GbE Ports | The maximum number of GbE ports provided on this generic QAM model. You can use any number from 0 to 66,365. |
| GbE Port Start Number | The beginning GbE port number for the model. You can use any number from 0 to 66,365. |
| Control IP Address Compatibility | The Internet Protocol (IP) version this model supports:<br>▪IPv4<br>▪IPv6 |
| Multicast Support | The following Internet Group Management Protocol (IGMP) versions that this model supports:<br>▪IGMPv3<br>▪IGMPv2<br>▪IGMPv1 |
| Number of Multicast Sources | The maximum number of multicast sources the that model supports.<br>You can use any number from 0 to 66,365. |
| Dynamic UDP Range | Determines whether the model supports a dynamic range of UDP ports (Yes or No). |
| PID Remapping | Determines whether the model supports packet identifier (PID) remapping (Yes or No). |
| Number of RF ports | The maximum number of RF output ports that the model supports.<br>You can use any number from 0 to 66,365. |
| Number of Carriers Per Ports | The maximum number of carriers per port that the model supports.<br>You can use any number from 0 to 66,365. |
| RF Port Start Number | The beginning RF port number for the model.<br>You can use any number from 0 to 66,365. |
| Encryption Type | The encryption types that the model supports:<br>▪Power Key<br>▪Shared Key<br>▪PassThrough<br>▪Fixed Key |
| Encryption Algorithm | The encryption algorithms that the model supports:<br>▪DES<br>▪3DES Key<br>▪AES Key<br>▪DVB-CSA |

## Information Needed to Add a Generic QAM Model

To add a generic QAM model to the DNCS, you need the following information about the model:

- Model number
- Maximum number of GbE ports
- Starting number of the GbE ports
- Internet Protocol (IP) version that the model supports
- Internet Group Management Protocol (IGMP) version that the model supports
- Maximum number of multicast sources the model supports
- Whether or not the model supports a dynamic range of UDP ports
- Whether or not the model supports packet identifier (PID) remapping
- Maximum number of RF ports
- Maximum number of carriers per RF port
- Starting number of RF ports
- Encryption types supported
- Encryption algorithms supported
- Modulation formats supported
- Whether the following settings are configurable:
    - Output power level
    - Frequency per carrier
    - Control word (CW) mode
    - Output squelch
    - Interleave Depth

**Note:** To obtain this information, consult the documentation provided by the manufacturer of the model.

## Add a Generic QAM Model

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM Models > New**

If you are using a generic QAM modulator to send content to DHCTs, first add the generic QAM model on which the modulator is based to the DNCS. The instructions in this section describe how to create a generic QAM model.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Generic QAM Models**. The Generic QAM Model List window opens.
4. Click **Add**. The Add Generic QAM Model window opens.
5. Complete the fields on the screen as described in Basic Parameter Settings - Generic QAM Model.

Use the following fields when you manage a generic QAM model in the DNCS.

| Field | Description |
|---|---|
| Model Number | The model number for this generic QAM model.<br>You can use up to 32 alphanumeric characters. |
| Number of GbE Ports | The maximum number of GbE ports provided on this generic QAM model. You can use any number from 0 to 66,365. |
| GbE Port Start Number | The beginning GbE port number for the model. You can use any number from 0 to 66,365. |
| Control IP Address Compatibility | The Internet Protocol (IP) version this model supports:<br>▪ IPv4<br>▪ IPv6 |
| Multicast Support | The following Internet Group Management Protocol (IGMP) versions that this model supports:<br>▪ IGMPv3<br>▪ IGMPv2<br>▪ IGMPv1 |
| Number of Multicast Sources | The maximum number of multicast sources the that model supports.<br>You can use any number from 0 to 66,365. |
| Dynamic UDP Range | Determines whether the model supports a dynamic range of UDP ports (Yes or No). |
| PID Remapping | Determines whether the model supports packet identifier (PID) remapping (Yes or No). |
| Number of RF ports | The maximum number of RF output ports that the model supports.<br>You can use any number from 0 to 66,365. |
| Number of Carriers Per Ports | The maximum number of carriers per port that the model supports.<br>You can use any number from 0 to 66,365. |
| RF Port Start Number | The beginning RF port number for the model. |

| | |
|---|---|
| | You can use any number from 0 to 66,365. |
| Encryption Type | The encryption types that the model supports:<br>▪ Power Key<br>▪ Shared Key<br>▪ PassThrough<br>▪ Fixed Key |
| Encryption Algorithm | The encryption algorithms that the model supports:<br>▪ DES<br>▪ 3DES Key<br>▪ AES Key<br>▪ DVB-CSA |

6. Complete the fields on the screen as described in RF Carrier Model Settings - Generic QAM Model.

Use the following fields when you manage generic QAMs in the DNCS.

| Field | Description |
|---|---|
| **QAM Platform Model** | |
| Model Number | The model number for this generic QAM model.<br>You can use up to 32 alphanumeric characters. |
| Number of GbE Ports | The maximum number of GbE ports provided on this generic QAM model.<br>You can use any number from 0 to 66,365. |
| GbE Port Start Number | The beginning GbE port number for the model. You can use any number from 0 to 66,365. |
| Control IP Address Compatibility | The Internet Protocol (IP) version this model supports:<br>▪ IPv4<br>▪ IPv6 |
| Multicast Support | The following Internet Group Management Protocol (IGMP) versions that this model supports:<br>▪ IGMPv3<br>▪ IGMPv2<br>▪ IGMPv1 |
| Number of Multicast Sources | The maximum number of multicast sources the that model supports.<br>You can use any number from 0 to 66,365. |
| Dynamic UDP Range | Determines whether the model supports a dynamic range of UDP ports (Yes or No). |
| PID Remapping | Determines whether the model supports packet identifier (PID) remapping (Yes or No). |
| Number of RF ports | The maximum number of RF output ports that the model supports.<br>You can use any number from 0 to 66,365. |
| Number of Carriers Per Ports | The maximum number of carriers per port that the model supports.<br>You can use any number from 0 to 66,365. |

| | |
|---|---|
| RF Port Start Number | The beginning RF port number for the model.<br>You can use any number from 0 to 66,365. |
| Encryption Type | The encryption types that the model supports:<br>▪ Power Key<br>▪ Shared Key<br>▪ PassThrough<br>▪ Fixed Key |
| Encryption Algorithm | The encryption algorithms that the model supports:<br>▪ DES<br>▪ 3DES Key<br>▪ AES Key<br>▪ DVB-CSA |

**RF Carrier Model**

| | |
|---|---|
| Modulation Format | The modulation formats that the model supports:<br>▪ QAM 64<br>▪ QAM 128<br>▪ QAM 256<br>▪ QAM 1024 |
| Output Power Level | Determines whether the model allows the output power level to be configurable (Yes or No). |
| Frequency Per Carrier | Determines whether the model allows each RF carrier to be configurable (Yes or No). |
| CW Mode | Determines whether the model supports the continuous wave (CW) mode (Yes or No). |
| Output Squelch | Determines whether the model allows the output squelch to be configurable (Yes or No). |
| Interleave Depth | Determines whether the model allows the interleave depth to be configurable (Yes or No). |

7. Click **Save**. The system begins saving the data to the database and, when finished, displays **Done** in the status bar at the bottom of the window.

**Note:** To view the new model in the Generic QAM Model List window, click **Generic QAM Model List** in the path at the top of the window.

8. Do you want to add another generic QAM model to the DNCS?

- If **yes**, click **Generic QAM Model List** in the path at the top of the window and repeat this procedure from step 4.
- If **no**, click **Exit** to close the window.

9. Would you like to add an individual QAM that is based on this generic QAM model to the DNCS?

- If **yes**, go to Add a Generic QAM.
- If **no**, click **Exit** to close the Generic QAM Model List window.

## Modify a Generic QAM Model

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM Models > [Select model] > Open**

You can modify the parameters for a generic QAM model as the needs of your site change. However, you can successfully modify data only for models that are not associated with individual generic QAM modulators.

Follow these instructions to modify data for a generic QAM model.

**Important:** You can only modify generic QAM models that are not used by any generic QAMs.

1. Are individual generic QAM modulators associated with this model?
   - If **yes**, you must first delete all of the individual modulators associated with this model before you can modify the generic QAM model. For assistance deleting individual modulators, see Delete a Generic QAM Model.
   - If **no**, continue with the next step.
2. From the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Generic QAM Models**. The Generic QAM Model List window opens.
5. Select the model whose parameters you want to modify.
6. Click **Edit**. The Open Generic QAM Model window opens for the model you selected.
7. Change the settings on the Open Generic QAM Model window as described in Basic Parameter Settings - Generic QAM Model and RF Carrier Model Settings - Generic QAM Model.

Use the following fields when you manage generic QAMs in the DNCS.

| Field | Description |
|---|---|
| **QAM Platform Model** | |
| Model Number | The model number for this generic QAM model.<br>You can use up to 32 alphanumeric characters. |
| Number of GbE Ports | The maximum number of GbE ports provided on this generic QAM model.<br>You can use any number from 0 to 66,365. |
| GbE Port Start Number | The beginning GbE port number for the model. You can use any number from 0 to 66,365. |
| Control IP Address Compatibility | The Internet Protocol (IP) version this model supports:<br>▪ IPv4<br>▪ IPv6 |
| Multicast Support | The following Internet Group Management Protocol (IGMP) versions that this model supports:<br>▪ IGMPv3<br>▪ IGMPv2<br>▪ IGMPv1 |
| Number of Multicast | The maximum number of multicast sources the that model supports. |

| | |
|---|---|
| Sources | You can use any number from 0 to 66,365. |
| Dynamic UDP Range | Determines whether the model supports a dynamic range of UDP ports (Yes or No). |
| PID Remapping | Determines whether the model supports packet identifier (PID) remapping (Yes or No). |
| Number of RF ports | The maximum number of RF output ports that the model supports.<br>You can use any number from 0 to 66,365. |
| Number of Carriers Per Ports | The maximum number of carriers per port that the model supports.<br>You can use any number from 0 to 66,365. |
| RF Port Start Number | The beginning RF port number for the model.<br>You can use any number from 0 to 66,365. |
| Encryption Type | The encryption types that the model supports:<br>▪Power Key<br>▪Shared Key<br>▪PassThrough<br>▪Fixed Key |
| Encryption Algorithm | The encryption algorithms that the model supports:<br>▪DES<br>▪3DES Key<br>▪AES Key<br>▪DVB-CSA |

## RF Carrier Model

| | |
|---|---|
| Modulation Format | The modulation formats that the model supports:<br>▪QAM 64<br>▪QAM 128<br>▪QAM 256<br>▪QAM 1024 |
| Output Power Level | Determines whether the model allows the output power level to be configurable (Yes or No). |
| Frequency Per Carrier | Determines whether the model allows each RF carrier to be configurable (Yes or No). |
| CW Mode | Determines whether the model supports the continuous wave (CW) mode (Yes or No). |
| Output Squelch | Determines whether the model allows the output squelch to be configurable (Yes or No). |
| Interleave Depth | Determines whether the model allows the interleave depth to be configurable (Yes or No). |

| | |
|---|---|
| Use the following fields when you manage | **Description** |

a generic QAM model in the DNCS.

| Field | |
|---|---|
| Model Number | The model number for this generic QAM model.<br>You can use up to 32 alphanumeric characters. |
| Number of GbE Ports | The maximum number of GbE ports provided on this generic QAM model. You can use any number from 0 to 66,365. |
| GbE Port Start Number | The beginning GbE port number for the model. You can use any number from 0 to 66,365. |
| Control IP Address Compatibility | The Internet Protocol (IP) version this model supports:<br>▪IPv4<br>▪IPv6 |
| Multicast Support | The following Internet Group Management Protocol (IGMP) versions that this model supports:<br>▪IGMPv3<br>▪IGMPv2<br>▪IGMPv1 |
| Number of Multicast Sources | The maximum number of multicast sources the that model supports.<br>You can use any number from 0 to 66,365. |
| Dynamic UDP Range | Determines whether the model supports a dynamic range of UDP ports (Yes or No). |
| PID Remapping | Determines whether the model supports packet identifier (PID) remapping (Yes or No). |
| Number of RF ports | The maximum number of RF output ports that the model supports.<br>You can use any number from 0 to 66,365. |
| Number of Carriers Per Ports | The maximum number of carriers per port that the model supports.<br>You can use any number from 0 to 66,365. |
| RF Port Start Number | The beginning RF port number for the model.<br>You can use any number from 0 to 66,365. |
| Encryption Type | The encryption types that the model supports:<br>▪Power Key<br>▪Shared Key<br>▪PassThrough<br>▪Fixed Key |
| Encryption Algorithm | The encryption algorithms that the model supports:<br>▪DES<br>▪3DES Key<br>▪AES Key<br>▪DVB-CSA |

8. Click **Save**. The system begins saving the data to the database and, when finished, displays **Done** in

the status bar at the bottom of the window.

9. Click **Exit** to close the Generic QAM Model List window.

## Delete a Generic QAM Model

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM Models > [Select model] > Delete**

You can successfully delete only models that are not associated with individual generic QAM modulators.

Follow these instructions to delete a generic QAM model that has no modulators associated with it.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Generic QAM**. The Generic QAM List window opens.
4. Select the model that you want to delete.
5. Click **Delete** at the bottom of the page. The system removes the modulator from the list and deletes the modulator from the DNCS database. When finished, the system displays **Done** in the status bar at the bottom of the window.
6. Click **Exit** to close the Generic QAM Model List window.

# Generic QAMs

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM**

From the Generic QAM List window, you can add QAMs from other manufacturers to the DNCS. The DNCS refers to these QAMs as **generic** QAMs. After generic QAMs are listed in this window, you can modify or delete the generic QAMs as the needs of your site change. From this window, you can also set up multicast sessions on any generic QAM listed in the window.

After you have added a generic QAM to this window, you can manage the generic QAM in the same ways that you manage our QAMs. For example, you can use the **Set Up Digital Source Definition** utility to set up broadcast sessions on the modulator and then view the sessions in the **Session List** window (along with any multicast sessions that you have set up on other generic QAM modulators). You can also add generic QAMs to VOD Service groups by selecting the ports on a generic QAM modulator from the Available Ports list in the **Add Service Group** or **Edit Service Group** window. If you view your network topology graphically, generic QAMs can be displayed this way as well. For example, you can show the generic QAM connected to a specific source by making connections in the **Connectivity** tab of the source's Set Up MPEG Source window.

**Important:** Before you can add a generic QAM to this window, the modulator model must first be defined in the Generic QAM Model List window. For more information, see Generic QAM Model List Window.

## What do you want to do?

- Review the fields in this window
- Add a generic QAM to this window
- Modify a generic QAM in this window
- Delete a generic QAM from this window
- Set up a multicast session on a generic QAM
- Set up a broadcast session on a generic QAM
- Tear down sessions on a generic QAM
- Add a generic QAM to a VOD service group

## Generic QAM Settings

Use the Generic QAM List window on the DNCS Administrative Console to manage the generic QAM devices in your network. Three tabs in this window provide settings for the generic QAM:

- Basic Parameter Settings - Generic QAM
- GbE Input Port Settings - Generic QAM
- RF Carrier Settings - Generic QAM
- Multicast Digital Session Settings - Generic QAM

### Basic Parameter Settings - Generic QAM

Use the following fields when you manage the basic parameters for a generic QAM.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this generic QAM. |
| Model Type | The generic QAM model upon which this modulator is based. |
| Qam Name | The name of this generic QAM.<br>You are limited to 20 alphanumeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1Q43 could represent a QAM modulator whose IP address ends in 43 that process VOD data for hub 1. |
| IP Address | The IP address of this generic QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address for this generic QAM. |
| Subnet Mask | The subnet mask where this generic QAM resides.<br>▪If your system uses a standard network configuration, enter **255.255.255.0.**<br>▪If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>A default gateway speeds up the reconnection process that occurs after modulator is rebooted. |
| Administrative State | Determines the availability of the modulator (**Online** or **Offline**).<br>You can activate a generic QAM modulator only after all parameters for the modulator have been saved, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task. |
| Pid Mapping | The type of PID mapping used by the generic QAM (**Dynamic** or **Static**). |

### GbE Input Port Settings - Generic QAM

Use the following fields when you manage the GbE input ports for a generic QAM.

| Field | Description |
|---|---|
| IP Address | The IP address of the modulator's GbE input port.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address of the modulator's GbE input port. |
| Subnet Mask | The subnet mask of the modulator's GbE input port.<br>If your system uses a standard network configuration, enter **255.255.255.0**.<br>If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Gateway IP | The gateway IP address of the modulator's GbE input port.<br>Be careful to properly place the dots (.) between numbers. |

### RF Carrier Settings - Generic QAM

Use the following fields when you manage the RF carriers for a generic QAM.

| Field | Description |
|---|---|
| Transport Stream ID | A unique number to identify the transport stream going from this generic QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365. |
| Modulation | The type of modulation this generic QAM uses. |
| Frequency | The frequency of the channel you will use to send data from this generic QAM to the hubs in your system |
| Continuous Wave Mode | Determines whether the generic QAM produces an unmodulated RF carrier.<br>Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| Disable | Determines whether you can set up additional sessions on an RF output port on the generic QAM.<br>Enable this option to prevent the DNCS from setting up any additional sessions on this RF carrier. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or, in the rare event, when a port fails. |
| Interleaver Depth | Determines the depth of interleaving for the QAM.<br>Available only if you are using Overlay technology. |

### Multicast Digital Session Settings - Generic QAM

Use the following fields when you manage the multicast sessions for a generic QAM.

| Field | Description |
|---|---|
| Source ID | Source that the session will use. |
| Session ID | Left Session ID field.<br>Enter 12 zeros (**00:00:00:00:00:00**).<br>Right Session ID field.<br>The Source ID you used when you added the source to the DNCS. |
| Bandwidth (Mbps) | The maximum amount of bandwidth (in Mbps) that the system should allow for this device.<br>This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>▪Standard MPEG video streams use 2 or 3 Mbps.<br>▪HDTV streams use 13 Mbps.<br>▪Audio streams use 0.2 Mbps.<br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| Output Carrier | The output destination of the source. |
| Program Number | The MPEG program number being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Source IP Address 1 | The IP address of the first device. |
| Source IP Address 2 | The IP address of the second device (if used). |
| Source IP Address 3 | The IP address of the third device (if used). |
| Input Destination Multicast IP Address | The multicast IP address on the GQAM modulator where sources are input. |
| UDP Port | The port number on the modulator where the sources are input. |

## Add a Generic QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM > New**

This section describes how to add a generic QAM modulator to the Generic QAM Modulator window (and to the DNCS) so that sessions can be set up on the modulator.

**Important:** Unlike our QAMs, generic QAMs do not support DNCS-supplied provisioning. As a result, specifications saved to the DNCS when the generic QAM is added (or **provisioned**) in the DNCS are not provided to the generic QAM when the modulator reboots. Instead, the generic QAM must be provisioned separately, as indicated in the manufacturer's documentation. Typically the generic QAM is provisioned through a craft port.

### Process Overview

To add a generic QAM to the DNCS, complete the following tasks. For step-by-step instructions for a particular task, click on that task.

**Important:** Adding a generic QAM to the DNCS is required in order to set up and manage sessions on the generic QAM, and it is not required to support DNCS-supplied provisioning of the generic QAM.

1. If you have not already done so, add a generic QAM model appropriate to the modulator to the DNCS. For assistance, see Add a Generic QAM Model.
2. Define the basic parameters
3. Define parameters for the GbE input ports
4. Define parameters for the RF carriers
5. Activate the generic QAM

### Related Topics

- Information Needed to add a Generic QAM

## Add a Generic QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM > New**

This section describes how to add a generic QAM modulator to the Generic QAM Modulator window (and to the DNCS) so that sessions can be set up on the modulator.

**Important:** Unlike our QAMs, generic QAMs do not support DNCS-supplied provisioning. As a result, specifications saved to the DNCS when the generic QAM is added (or **provisioned**) in the DNCS are not provided to the generic QAM when the modulator reboots. Instead, the generic QAM must be provisioned separately, as indicated in the manufacturer's documentation. Typically the generic QAM is provisioned through a craft port.

### Process Overview

To add a generic QAM to the DNCS, complete the following tasks. For step-by-step instructions for a particular task, click on that task.

**Important:** Adding a generic QAM to the DNCS is required in order to set up and manage sessions on the generic QAM, and it is not required to support DNCS-supplied provisioning of the generic QAM.

1. If you have not already done so, add a generic QAM model appropriate to the modulator to the DNCS. For assistance, see Add a Generic QAM Model.
2. Define the basic parameters
3. Define parameters for the GbE input ports
4. Define parameters for the RF carriers
5. Activate the generic QAM

### Related Topics

- Information Needed to add a Generic QAM

### Information Needed to Add a Generic QAM

You need the following information to add a generic QAM to the DNCS.

**Note:** Unless noted otherwise, consult the manufacturer of the modulator to obtain this information.

- Name of the headend containing the generic QAM
- The model type on which the generic QAM is based
- Name used to identify the generic QAM
- IP address of the control port on the generic QAM
- MAC address of the control port
- Subnet mask for the control port (from your system administrator)
- If applicable, the default gateway that the generic QAM uses (from your system administrator)
- Type of packet identifier (PID) mapping (With dynamic PID mapping the modulator automatically maps PIDs that pass through the modulator. With static PID mapping, administrators or operators manually map PIDs that pass through the modulator.)

### Related Topics

- Add a Generic QAM

### Define Generic QAM Basic Parameters

Complete these steps to define the basic parameters for a generic QAM and save this information in the DNCS database.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Generic QAM**. The Generic QAM List window opens.
4. Click **Add**. The Add Generic QAM window opens with Basic Parameters settings shown.
5. Complete the fields on the screen as described in Basic Parameter Settings - Generic QAM.

Use the following fields when you manage the basic parameters for a generic QAM.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this generic QAM. |
| Model Type | The generic QAM model upon which this modulator is based. |
| Qam Name | The name of this generic QAM.<br>You are limited to 20 alphanumeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1Q43 could represent a QAM modulator whose IP address ends in 43 that process VOD data for hub 1. |
| IP Address | The IP address of this generic QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address for this generic QAM. |
| Subnet Mask | The subnet mask where this generic QAM resides.<br>▪ If your system uses a standard network configuration, enter **255.255.255.0.**<br>▪ If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>A default gateway speeds up the reconnection process that occurs after modulator is rebooted. |
| Administrative State | Determines the availability of the modulator (**Online** or **Offline**).<br>You can activate a generic QAM modulator only after all parameters for the modulator have been saved, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task. |
| Pid Mapping | The type of PID mapping used by the generic QAM (**Dynamic** or **Static**). |

**Important:** Do not set the Administrative State setting at this time.

6. Click **Save**. The system begins saving the data to the database and, when finished, displays **Done** in the status bar at the bottom of the window.

7. Leave this window open, and go to Defining GbE Input Ports for Generic QAM Modulators.

### Define Generic QAM GbE Input Ports

After you set up the generic QAM basic parameters, you must define the GbE input ports for the generic QAM.

Complete these steps to define the GbE input ports for a generic QAM and save this information in the DNCS database.

1. Click **GbE Input Ports**. The GbE Input Ports window opens.
2. Complete the fields on the screen as described in GbE Input Port Settings - Generic QAM.

   Use the following fields when you manage the GbE input ports for a generic QAM.

| Field | Description |
|---|---|
| IP Address | The IP address of the modulator's GbE input port.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address of the modulator's GbE input port. |
| Subnet Mask | The subnet mask of the modulator's GbE input port.<br>If your system uses a standard network configuration, enter **255.255.255.0**.<br>If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Gateway IP | The gateway IP address of the modulator's GbE input port.<br>Be careful to properly place the dots (.) between numbers. |

3. Click **Save**. The system begins saving the data to the database and, when finished, displays **Done** in the status bar at the bottom of the window.
4. Leave this window open and go to Defining RF Carriers for Generic QAM Modulators.

### Define Generic QAM RF Carriers

After you have set up the generic QAM basic parameters and defined its GbE input ports, your next step is to define the RF carriers for the generic QAM.

1. In the path at the top of the window, click **Generic QAM**. The Generic QAM window opens for this generic QAM modulator.
2. Click **RF Carriers**. The RF Carrier Parameters window opens.
3. Complete the fields on the screen as described in RF Carrier Settings - Generic QAM.

Use the following fields when you manage the RF carriers for a generic QAM.

| Field | Description |
|---|---|
| Transport Stream ID | A unique number to identify the transport stream going from this generic QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365. |
| Modulation | The type of modulation this generic QAM uses. |
| Frequency | The frequency of the channel you will use to send data from this generic QAM to the hubs in your system |
| Continuous Wave Mode | Determines whether the generic QAM produces an unmodulated RF carrier.<br>Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| Disable | Determines whether you can set up additional sessions on an RF output port on the generic QAM.<br>Enable this option to prevent the DNCS from setting up any additional sessions on this RF carrier. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or, in the rare event, when a port fails. |
| Interleaver Depth | Determines the depth of interleaving for the QAM.<br>Available only if you are using Overlay technology. |

4. Click **Save**. The system begins saving the data to the database and, when finished, displays **Done** in the status bar at the bottom of the window.
5. Have you provisioned the generic QAM?
   - If **yes**, leave this window open and go to Activating the Generic QAM.
   - If **no**, leave this window open and provision the generic QAM modulator. When you have provisioned the modulator, go to Activating the Generic QAM.

   **Note:** For information on provisioning the generic QAM, refer to the documentation provided by the manufacturer of the generic QAM.

### Activating the Generic QAM

Complete these steps to activate the generic QAM.

1. If you have not already done so, define the following parameters for this generic QAM:
   - Define Generic QAM Basic Parameters
   - Define Generic QAM GbE Input Ports
   - Define Generic QAM RF Carriers
2. In the path at the top of the window, click **Generic QAM**. The Add Generic QAM window opens for this generic QAM modulator.
3. For the Administrative State, click **Online**.
4. Click **Save** to change the status of the generic QAM to online and activate the modulator. When the modulator has been activated, **Done** is displayed in the status bar at the bottom of the window.
5. Add the new generic QAM to your network map.

### Related Topics

- Add a Generic QAM
- Add a Generic QAM Model

## Set Up a Multicast Session on a Generic QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM > [Select Generic QAM] > Open > Multicast Sessions > New**

Complete these steps to set up a multicast session on a generic QAM.

1. If you have not already done so, add a generic QAM to the DNCS and create a source for the multicast session.
2. From the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Generic QAM**. The Generic QAM List window opens.
5. Select the generic QAM on which you want to set up a multicast session.
6. Click **Edit**. The Open Generic QAM window opens for the modulator you selected.
7. Click **Multicast Sessions**. The Multicast Digital Session Definition window opens. If no sessions have been set up on this modulator, the window is empty. Otherwise, sessions the modulator carries are listed in this window.
8. Click **Add**. The Add Multicast Digital Session Definition window opens.
9. Complete the fields on the screen as described in Fields Used in Setting Up a Multicast Session on a Generic QAM Modulator.

### Fields Used in Setting Up a Multicast Session on a Generic QAM Modulator

Use the following fields when you define an analog source in the DNCS.

| Field | Description |
|---|---|
| Source ID | Source that the session will use. |
| Session ID | Left Session ID field.<br>Enter 12 zeros (**00:00:00:00:00:00**). |
| | Right Session ID field.<br>The Source ID you used when you added the source to the DNCS. |
| Bandwidth | The maximum amount of bandwidth (in Mbps) that the system should allow for this device.<br>This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>▪ Standard MPEG video streams use **2** or **3** Mbps.<br>▪ HDTV streams use **13** Mbps.<br>▪ Audio streams use **0.2** Mbps.<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |

| | |
|---|---|
| Output Carrier | The output destination of the source. |
| Program Number | The MPEG program number being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Source IP Address 1 | The IP address of the first device. |
| Source IP Address 2 | The IP address of the second device (if used). |
| Source IP Address 3 | The IP address of the third device (if used). |
| Input Destination Multicast IP Address | The multicast IP address on the GQAM modulator where sources are input. |
| UDP Port | The port number on the modulator where the sources are input.<br>**Important:** If you are using GQAMs, and the multicast session is being set up as an SMDG session, the session's input port must match the input port of the SMDG. Otherwise, the session may fail. |

10. Click **Save**. The system saves the multicast session in the DNCS database and starts the session you built for it. The Multicast Digital Session Definition window updates to include the new session information.

**Note:** After a session has been set up, you can manage it from the Session List window. For more information, go to Session Summary

### Information Needed to Set Up a Multicast Session on a Generic QAM

You need the following information to set up a multicast session on a generic QAM.

**Note:** To obtain this information, consult your network map or your system administrator, unless noted otherwise in the following list.

- Source ID as you defined it when you added the content source to the DNCS
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the content from the source (refer to your network map)
- MPEG program number (from your content service provider)
- IP addresses of source devices (up to 3 different source devices can be used)
- Input destination multicast ID address on the generic QAM modulator
- Destination UDP port on the generic QAM modulator

## Set Up a Broadcast Session on a Generic QAM

Broadcast sessions are typically created when setting up services for subscribers. Click one of the following links to set up a broadcast session that can be used to provide one of the following services:

- Clear Services  Services that are delivered to subscribers unscrambled or unencrypted; for example, programming available through the three major networks (ABC, CBS, and NBC) is usually clear
- Secure Services  Services that are encrypted or scrambled so that they are protected from being accessed (stolen) by people who have not paid for the service; usually offered at a price that is in addition to the price for clear services (for example, HBO, Showtime, and music channels)
- Pay-Per-View (PPV) Services  Services that carry PPV events that subscribers can choose to purchase in addition to their normal cable programming; has some of the same characteristics as both clear and secure services

## Modify a Generic QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM > [Select modulator] > Open**

Follow these instructions to modify data for a generic QAM.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Generic QAM**. The Generic QAM List window opens.
4. Select the model whose parameters you want to modify.
5. Click **Edit**. The Open Generic QAM Model window opens for the modulator you selected.
6. Change the settings that you desire. For information about the settings in this window, click one of the following links:
   - Basic Parameter Settings - Generic QAM

   Use the following fields when you manage the basic parameters for a generic QAM.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this generic QAM. |
| Model Type | The generic QAM model upon which this modulator is based. |
| Qam Name | The name of this generic QAM.<br>You are limited to 20 alphanumeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1Q43 could represent a QAM modulator whose IP address ends in 43 that process VOD data for hub 1. |
| IP Address | The IP address of this generic QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address for this generic QAM. |
| Subnet Mask | The subnet mask where this generic QAM resides.<br>▪ If your system uses a standard network configuration, enter **255.255.255.0.**<br>▪ If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>A default gateway speeds up the reconnection process that occurs after modulator is rebooted. |
| Administrative State | Determines the availability of the modulator (**Online** or **Offline**).<br>You can activate a generic QAM modulator only after all parameters for the |

| | |
|---|---|
| | modulator have been saved, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task. |
| Pid Mapping | The type of PID mapping used by the generic QAM (**Dynamic** or **Static**). |

- GbE Input Port Settings - Generic QAM

Use the following fields when you manage the GbE input ports for a generic QAM.

| Field | Description |
|---|---|
| IP Address | The IP address of the modulator's GbE input port.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address of the modulator's GbE input port. |
| Subnet Mask | The subnet mask of the modulator's GbE input port.<br>If your system uses a standard network configuration, enter **255.255.255.0**.<br>If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Gateway IP | The gateway IP address of the modulator's GbE input port.<br>Be careful to properly place the dots (.) between numbers. |

- RF Carrier Settings - Generic QAM

Use the following fields when you manage the RF carriers for a generic QAM.

| Field | Description |
|---|---|
| Transport Stream ID | A unique number to identify the transport stream going from this generic QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365. |
| Modulation | The type of modulation this generic QAM uses. |
| Frequency | The frequency of the channel you will use to send data from this generic QAM to the hubs in your system |
| Continuous Wave Mode | Determines whether the generic QAM produces an unmodulated RF carrier.<br>Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| Disable | Determines whether you can set up additional sessions on an RF output port on the generic QAM.<br>Enable this option to prevent the DNCS from setting up any additional sessions on this RF carrier. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or, in the rare event, when a port fails. |
| Interleaver Depth | Determines the depth of interleaving for the QAM.<br>Available only if you are using Overlay technology. |

7. Click **Save**. The system begins saving the data to the database and, when finished, displays **Done** in

the status bar at the bottom of the window.

8. Click **Exit** to close the Generic QAM List window.

## Delete a Generic QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Generic QAM > [Select modulator] > Delete**

The instructions in this section describe how delete a generic QAM that is carrying no sessions.

### You Need to Know

Before You Begin

Before you delete a generic QAM, first tear down all of the sessions associated with the modulator. If you delete a modulator without first tearing down its related sessions, system performance may be degraded. Performance degrades because the DNCS uses its resources attempting to associate sessions with a modulator that no longer exists. See Tear Down Sessions on QAM Modulators to learn how to tear down sessions.

In addition, you must have your network map available.

Complete these steps to delete a generic QAM from the DNCS.

1. Are sessions associated with this generic QAM?
   - If **yes**, tear down all sessions that are running on the generic QAM you want to delete. For assistance, see Tear Down Sessions on QAM Modulators.
   - If **no**, go to step 2.
2. From the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Generic QAM**. The Generic QAM List window opens.
5. Select the model that you want to delete.
6. Click **Delete**. The system removes the modulator from the list and deletes the modulator from the DNCS database. When finished, the system displays **Done** in the status bar at the bottom of the window.
7. Click **Exit** to close the Generic QAM List window.

# Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM**

This window lists the table-based QAMs that are part of your DBDS. Table-based QAMs from us are known as Continuum DVP™ eXtra Dense QAM Array (XDQA) QAMs. If your system uses Overlay technology, your third-party QAMs are also listed in this window.

Table-based QAMs are used to provide VOD service, and, for this reason, are part of a service group. By adding table-based QAMs to the DNCS, you ensure that set-tops receive information about service groups that contain table-based QAMs. If your system uses table-based QAMs and these QAMs have not been added to the DNCS, set-tops may be unable to tune to the correct channel to receive a VOD event.

## What do you want to do?

- Review settings for table-based QAMs
- Add a table-based QAM to the DNCS
- Use the Filter to display table-based QAMs
- Modify a table-based QAM
- Delete a table-based QAM
- Manage sessions on table-based QAMs

## Table-Based QAM Settings

Use the Table-Based QAM window on the DNCS Administrative Console to manage the table-based QAM devices in your network. Three tabs in this window provide settings for the table-based QAM:

- Basic Parameters - Table-Based QAM
- RF Parameter Settings - Table-Based QAM
- Session Data Parameter Settings - Table-Based QAM

### Table-Based QAM Basic Parameter Settings

Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM.<br>You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

### Related Topics

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

### Table-Based QAM RF Parameter Settings

Use the following fields when you manage RF parameters for a table-based QAM.

| Field | Description |
|---|---|
| TSID | A unique number to identify the transport stream going from this table-based QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365.<br>**Note:** TSID ranges are defined from DNCS System Configuration. If you receive a range error message, you can change values from the following location: **DNCS tab > System Provisioning tab > DNCS System Configuration > Advanced Parameters tab** |
| Frequency | The frequency (in MHz) of the channel you will use to send data from this table-based QAM to the hubs in your system.<br>You can enter a value in 6 MHz increments from 91 to 861. |
| Modulation Type | The type of modulation this QAM uses. |
| Bandwidth | The bandwidth (in Mbps) that the system should reserve for the QAM. |
| Port Number | The carrier output port associated with the frequency you entered. |

### Related Topics

- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

### Table-Based QAM Session Data Parameter Settings

These parameters are typically loaded from a data file to automatically populate the fields. The file containing the session data uses the following format: **udp port,output port,program,low pid,high pid,optional tsid**

**Important:** If the TSID is not provided, the TSID must be derivable based on the UDP port.

After you add a table-based QAM to your system, you can modify session data for the QAM whenever needed. You can continue to upload new files with new session information or you can make changes to session information directly from the Table-Based QAMs List window. To make changes manually, directly from the Table-Based QAMs List window, see Modify Session Data for a Table-Based QAM.

### Related Topics

- Add a Table-Based QAM
- Upload Session Data File to a Table-Based QAM

## Table-Based QAM Filter

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > Filter**

From the Filter area on the Table-Based QAMs List window, you can quickly retrieve information about the table-based QAMs in your system.

**Related Topics**

- Learn about Filter settings for table-based QAMs
- Use the Filter to search and display specific Table-Based QAMs in your system
- Learn about the data that the Filter displays

### Table-Based QAM Filter Settings

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > Filter**

This section describes Table-Based QAM Filter options and provides examples to show how the Filter searches for table-based QAM data based on your selections.

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field.<br>**Note:** This field accepts only numbers. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125<br>172.1**4**.5.32<br>172.17.5.5**4** |

### Table-Based QAM Filter Options

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125 |

| | | |
|---|---|---|
| | **Note:** This field accepts only numbers. | 172.1**4**.5.32<br>172.17.5.5**4** |

## Related Topics

- Table-Based QAMs Filter Data
- Use the Filter to Display Table-Based QAMs

### Table-Based QAM Filter Settings

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > Filter**

This section describes Table-Based QAM Filter options and provides examples to show how the Filter searches for table-based QAM data based on your selections.

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field.<br>**Note:** This field accepts only numbers. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125<br>172.1**4**.5.32<br>172.17.5.5**4** |

### Table-Based QAM Filter Options

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125 |

| | | |
|---|---|---|
| | **Note:** This field accepts only numbers. | 172.1**4**.5.32<br>172.17.5.5**4** |

## Related Topics

- Table-Based QAMs Filter Data
- Use the Filter to Display Table-Based QAMs

### Use the Filter to Display Table-Based QAMs

1. Click the **By Field** arrow and select one of the following options:
   - Headend
   - IP
   - Name

**Note:** For a description of these options, see Table-Based QAM Filter Settings.

2. Click in the **By Value** field and enter data in this field, or when filtering by Headend, click the Headend arrow and select the headend containing the QAM.

**Note:** For examples of how By Value data affects searches, see Table-Based QAMs Filter Settings.

3. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Table-Based QAMs List window.

**Note:** For information about the data displayed, see Table-Based QAM Filter Data.

**Table-Based QAM Filter Data**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM**

When you use the Filter to search for and display service groups, search results are shown in the Table-Based QAMs List window, which lists the following information:

- **QAM Name** - Shows the name of the table-based QAM
- **IP Address** - Shows the GigE IP address of the table-based QAM
- **MAC Address** - Shows the GigE MAC address for the table-based QAM
- **Online** - Determines whether the QAM is active (Online enabled) or inactive (Online disabled)
- **Headend** - Shows the name of the headend containing the table-based QAM

**Related Topics**

- Add a Table-Based QAM
- Modify a Table-Based QAM Modulator
- Delete a Table-Based QAM Modulator
- Manage Table-Based QAM Sessions

## Add a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs**

From the Table-Based QAMs interface, you can add our Continuum DVP™ eXtra Dense QAM Array (XDQA) QAMs. If your system uses Overlay technology, you also add third-party QAMs using this interface.

Table-based QAMs are used to provide VOD service, and, for this reason, are part of a service group. By adding table-based QAMs to the DNCS, you ensure that DHCTs receive information about service groups that contain table-based QAMs. If your system uses table-based QAMs and these QAMs have not been added to the DNCS, DHCTs may be unable to tune to the correct channel to receive a VOD event.

### You Need to Know

Process Overview

To add table-based QAM modulators to the DNCS, you must complete the following tasks in the order presented.

1. Record your planned associations between service groups and table-based QAMs. You will need a service group ID for each table-based QAM you add.
2. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

**Notes:**

- The file uses the following format:

udp port,output port,program,low pid,high pid,optional tsid

- If the TSID is not provided, the TSID must be derivable based on the UDP port.

3. Add the table-based QAMs to the DNCS.
4. Configure RF parameters for the table-based QAMs.

### Related Topics

- Configure session data for Table-Based QAM Modulators

### Adding a Table-Based QAM Modulator

Follow these steps to add table-based QAM to the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. Click **Add**. The Add Table-Based QAM window opens.
5. Complete the fields on the screen as described in Table-Based QAM Basic Parameter Settings.

Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM. |

| | |
|---|---|
| | You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

**Related Topics**

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

6. Click **Save**. The Add Table-Based QAM window closes and the QAM you added displays in the Table-Based QAMs List window.

7. Select the QAM from the list and click **Configure RF Parameters**. The RF Parameters window opens for the QAM you selected.

8. Click **Add**. Empty data fields appear in the window.

9. Complete the fields on the screen as described in Table-Based QAM RF Parameter Settings.

Use the following fields when you manage RF parameters for a table-based QAM.

| Field | Description |
|---|---|
| TSID | A unique number to identify the transport stream going from this table-based QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365.<br>**Note:** TSID ranges are defined from DNCS System Configuration. If you receive a range error message, you can change values from the following location: **DNCS tab > System Provisioning tab > DNCS System Configuration > Advanced Parameters tab** |
| Frequency | The frequency (in MHz) of the channel you will use to send data from this table-based QAM to the hubs in your system.<br>You can enter a value in 6 MHz increments from 91 to 861. |
| Modulation Type | The type of modulation this QAM uses. |
| Bandwidth | The bandwidth (in Mbps) that the system should reserve for the QAM. |
| Port Number | The carrier output port associated with the frequency you entered. |

**Related Topics**

- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

10. Click **Save**. The system saves the information you have entered and updates the RF Parameters

window with this information. The status area of the window displays the message, "RF Parameters saved successfully.

11. Click **Exit** to close the window.

**Related Topics**

- Upload Session Data for Table-Based QAMs

## Add a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs**

From the Table-Based QAMs interface, you can add our Continuum DVP™ eXtra Dense QAM Array (XDQA) QAMs. If your system uses Overlay technology, you also add third-party QAMs using this interface.

Table-based QAMs are used to provide VOD service, and, for this reason, are part of a service group. By adding table-based QAMs to the DNCS, you ensure that DHCTs receive information about service groups that contain table-based QAMs. If your system uses table-based QAMs and these QAMs have not been added to the DNCS, DHCTs may be unable to tune to the correct channel to receive a VOD event.

### You Need to Know

Process Overview

To add table-based QAM modulators to the DNCS, you must complete the following tasks in the order presented.

1. Record your planned associations between service groups and table-based QAMs. You will need a service group ID for each table-based QAM you add.
2. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

**Notes:**

- The file uses the following format:

  udp port,output port,program,low pid,high pid,optional tsid

- If the TSID is not provided, the TSID must be derivable based on the UDP port.

3. Add the table-based QAMs to the DNCS.
4. Configure RF parameters for the table-based QAMs.

### Related Topics

- Configure session data for Table-Based QAM Modulators

### Adding a Table-Based QAM Modulator

Follow these steps to add table-based QAM to the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. Click **Add**. The Add Table-Based QAM window opens.
5. Complete the fields on the screen as described in Table-Based QAM Basic Parameter Settings.

Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM. |

| | |
|---|---|
| | You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

### Related Topics

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

6. Click **Save**. The Add Table-Based QAM window closes and the QAM you added displays in the Table-Based QAMs List window.

7. Select the QAM from the list and click **Configure RF Parameters**. The RF Parameters window opens for the QAM you selected.

8. Click **Add**. Empty data fields appear in the window.

9. Complete the fields on the screen as described in Table-Based QAM RF Parameter Settings.

Use the following fields when you manage RF parameters for a table-based QAM.

| Field | Description |
|---|---|
| TSID | A unique number to identify the transport stream going from this table-based QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365.<br>**Note:** TSID ranges are defined from DNCS System Configuration. If you receive a range error message, you can change values from the following location: **DNCS tab > System Provisioning tab > DNCS System Configuration > Advanced Parameters tab** |
| Frequency | The frequency (in MHz) of the channel you will use to send data from this table-based QAM to the hubs in your system.<br>You can enter a value in 6 MHz increments from 91 to 861. |
| Modulation Type | The type of modulation this QAM uses. |
| Bandwidth | The bandwidth (in Mbps) that the system should reserve for the QAM. |
| Port Number | The carrier output port associated with the frequency you entered. |

### Related Topics

- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

10. Click **Save**. The system saves the information you have entered and updates the RF Parameters window with this information. The status area of the window displays the message, "RF Parameters

saved successfully.

11. Click **Exit** to close the window.

**Related Topics**

- Upload Session Data for Table-Based QAMs

## Modify a Table-Based QAM

Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table- Based QAMs > [Select QAM] > Edit

You can modify several aspects of the table-based QAM:

- Modify Basic Parameters for a Table-Based QAM
- Modifying RF Parameters for a Table-Based QAM
- Modify Session Data for a Table-Based QAM

### Modify Basic Parameters for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > [Filter and Select QAM] > Edit**

After you add a table-based QAM to your system, you can modify any of its basic parameters whenever needed. Follow this procedure to modify the basic parameters for table-based QAMs.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. Use the Filter to display the QAM that you want to modify.

   **Note:** For assistance using the Filter, see Table-Based QAM Filter.

5. Select the QAM that you want to modify. A check mark appears in the box to the left of the QAM.
6. Click **Edit**. The Edit Table-Based QAM window opens for the QAM you selected.
7. Make changes to the fields as described in Table-Based QAM Basic Parameter Settings.

   Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM.<br>You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

**Related Topics**

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

8. Click **Save** to save your changes. The Edit Table-Based QAM window closes and the changes you made are shown in the Table-Based QAMs List window.
9. Click **Exit** to close the Table-Based QAMs List window.

**Related Topics**

- Modifying RF Parameters for a Table-Based QAM

- Modify Session Data for a Table-Based QAM

### Modify RF Parameters for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure RF Parameters**

After you add a table-based QAM to your system, you can modify any of its RF parameters whenever needed.

Follow these steps to modify RF Parameters for table-based QAMs.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. From the Table-Based QAMs List window, select a table-based QAM.
5. Click **Configure RF Parameters**. The RF Parameters window opens for the QAM you selected.
6. Complete one of the following steps.
   - To edit existing parameters, click in the fields you want to edit and make changes. Then, click **Save** to save your changes.
   - To add a new RF parameter, click **Add** and complete the new data fields that appear. Then, click **Save** to save your changes.
   - To delete an existing parameter, click **Delete**. When asked to confirm, click **OK**.

   **Note:** If necessary, upload a new session data file to match the RF parameter changes you have made.
7. Click **Exit** to close the window.

**Related Topics**

- Modify Session Data for a Table-Based QAM
- Table-Based QAM RF Parameter Settings

### Modify Session Data for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data**

After you upload session data for a table-based QAM, you can modify the session data whenever needed. When entering session data manually, be sure to obtain documentation listing the standard values for UDP Port, Program Number, High PID, and Low PID for the type of table-based QAM you are configuring.

Follow these steps to manually modify session data for table-based QAMs from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM whose sessions you want to modify.
5. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
6. Select the session and click **Edit**. The Edit Session Data window opens.
7. Update the information as needed, and click **Save** to save your changes. The Edit Session Data window closes and the Session Data window updates with the new data.

   **Note:** For assistance see Table-Based QAM Session Data Parameters.

   These parameters are typically loaded from a data file to automatically populate the fields. The file containing the session data uses the following format: **udp port,output port,program,low pid,high pid,optional tsid**

   **Important:** If the TSID is not provided, the TSID must be derivable based on the UDP port.

   After you add a table-based QAM to your system, you can modify session data for the QAM whenever needed. You can continue to upload new files with new session information or you can make changes to session information directly from the Table-Based QAMs List window. To make changes manually, directly from the Table-Based QAMs List window, see Modify Session Data for a Table-Based QAM.

   **Related Topics**

   - Add a Table-Based QAM
   - Upload Session Data File to a Table-Based QAM

8. Click **Exit** to close the window.

**Related Topics**

- Delete Sessions from a Table-Based QAM
- Upload Session Data to a Table-Based QAM

## Delete a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Delete**

Follow these steps to delete a table-based QAM from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM you want to delete.
5. Click **Delete**. A confirmation window opens.
6. Click **OK**. The table-based QAM is removed from the list.
7. Do you want to delete additional table-based QAMs?
   - If **yes**, repeat steps 4 and 5 for each table-based QAM you want to delete.
   - If **no**, click **Exit**.

## Manage Table-Based QAM Sessions

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Filter to show QAMs] > [Select QAM] > Configure Session Data**

From the Session Data window, you can manage sessions for your table-based QAMs.

### Related Topics

- Upload session data to a table-based QAM
- Modify session data for a table-based QAM
- Delete sessions on a table-based QAM

### Upload Session Data to a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data > File Upload**

This procedure describes how to upload session data from a file because this is the preferred method for populating this data on the DNCS. If you want to enter session data manually, be sure to obtain documentation listing the standard values for UDP Port, Program Number, High PID, and Low PID for the type of table-based QAM you are configuring.

Follow these steps to configure session data for new table-based QAMs.

1. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

   **Important:**

   - The file uses the following format: udp port,output port,program,low pid,high pid,optional tsid
   - If the TSID is not provided, the TSID must be derivable based on the UDP port.

   **Note:** To ensure that this file is saved during a system backup, place this file in the appropriate directory on the DNCS. For assistance, refer to Recommendations for Installing Applications on the DNCS and Application Server (part number 749638). To obtain a copy of this document, see Printed Resources.

2. On the DNCS Administrative Console, click the **DNCS** tab.
3. On the DNCS tab, click the **Network Element Provisioning** tab.
4. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
5. Select a newly added table-based QAM.
6. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
7. Click **File load**.
8. Click the **Browse** button.
9. From the File Upload window, navigate to the location where the session data file for this table-based QAM is stored and click **Open**. The path and the file you selected is populated in the **Select the file to be uploaded** field.
10. Click the **Load** button.
11. Wait for confirmation that all of the records were loaded with 0 errors. Click **OK** in the confirmation window.
12. Click **Save changes**.

    **Important:** You must click **Save changes** to save the session data. Clicking **OK** in the previous step does not automatically save the session data.

13. Click **Exit** to close the window.

**Related Topics**

- Modify Session Data for a Table-Based QAM

### Delete Sessions from a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data > [Select Sessions to be deleted] > Delete > OK**

This procedure describes either of the following ways to delete sessions from a table-based QAM:

- Individual sessions on a table-based QAM
- All sessions on a table-based QAM so that you can then upload new session data to the table-based QAM

Follow these steps to delete sessions from a table-based QAM.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM whose sessions you want to modify.
5. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
6. Select the sessions that you want to delete.

   **Tip:** To delete all sessions on this QAM, click the topmost selection box. Check marks appear in all selection boxes.

7. Click **Delete**. A confirmation message appears.
8. Click **OK**. The message closes and the Session Data window updates and shows that the selected sessions have been removed from the window.
9. Click **Exit** to close the window.

### Related Topics

- Upload Session Data for a Table-Based QAM (Delete Sessions from a Table-Based QAM, Upload Session Data to a Table-Based QAM)

# QPSK Modulator

A QPSK modulator processes data going downstream from the DNCS to the DHCTs, as well as data going upstream from the DHCTs to the DNCS.

For example, a QPSK modulator takes programming data for a PPV event from the DNCS, processes it onto an RF signal, and then sends it to the DHCTs. When a subscriber chooses to buy that event by using their remote control to send a signal to the DHCT, the DHCT passes that signal back to the DNCS, first through a QPSK demodulator, and then through a QPSK modulator.

For more information on QPSK modulators, refer to DAVIC QPSK Demodulator Model D9492 Installation and Operation Guide (part number 545617).

**Note:** We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data to DHCTs. For more information about this software product, contact the representative who handles your account.

## What do you want to do?

- Review QPSK modulator settings
- Add a QPSK modulator
- Modify a QPSK modulator
- Reset the QPSK modulator database
- Delete a QPSK modulator

## Information to Add a QPSK Modulator

You need the following information to add a QPSK modulator to the DNCS:

- IP address for the QPSK modulator
- MAC address for the QPSK modulator (click here for the procedure to locate)
- Subnet mask for the QPSK modulator
- IP address of the default router associated with the modulator
- Base IP address for all DHCTs within the domain of the modulator
- Subnet mask for all DHCTs within the domain of the modulator
- RF output frequency assigned to this modulator

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

## Locate a QPSK Modulator MAC Address

You can look at the sticker on the side of the QPSK modulator to locate its MAC address. Or, if the QPSK modulator is already in operation, you can complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the QPSK modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

## QPSK Modulator Settings

Use the Set Up QPSK Modulator page on the DNCS Administrative Console to manage the QPSK modulators in your network. Two tabs in this window provide settings for the QAM:

- Basic Parameters settings: Use the settings on the Basic Parameters tab to configure key settings of the QPSK modulator.
- Advanced Parameters settings: Use the settings on the Advanced Parameters tab to to view the default setting for the QPSK modulator. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### Basic Parameter Settings - QPSK Modulator

Use the following fields when you manage the basic parameters for a QPSK modulator.

| Field | Description |
|---|---|
| Hub Name | The hub associated with this content QPSK (if you have more than one defined). |
| Name | The name of this QPSK.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that allows you to easily identify the QPSK modulator and where it resides. |
| IP Address | The IP address for this QPSK.<br>Be careful to properly place the dots (.) between numbers. |
| Physical Address | The MAC address for the QPSK. |
| Subnet Mask | The subnet mask where this QPSK modulator resides. |
| Default Router | The IP address for the router associated with this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| DHCT Base IP Address | The base IP address for all DHCTs within the domain of this modulator. |
| DHCT Subnet Mask | The subnet mask for all DHCTs within the domain of this modulator. |
| Frequency | The RF output frequency assigned to this modulator.<br>This value can be from 70 MHz to 130 MHz in increments of 0.25 MHz. |
| DCM (DHCT Communications Mode) | Determines the DCM for the QPSK.<br>**Important:** Currently all DSG-capable DHCTs use a Mixed DOCSIS/DAVIC DCM. Unique code on Explorer 8300 DHCTs enables them to recognized a DCM of Mixed DOCSIS/DAVIC as DOCSIS. QPSK modulators that provide the BRF to hubs with Explorer 8300 DHCTs use a DCM of Mixed DOCSIS/DAVIC.<br>Select the appropriate DCM from one of the following choices:<br>▪**DAVIC** - Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel.<br>▪**Mixed DOCSIS/DAVIC** - Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel.<br>▪**DOCSIS** - Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.) |
| Options | **Continuous Wave Mode -** Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK. |

**Front Panel Lock -** Determines whether changes can be made from the front panel.

**Broadcast Only Mode -** Determines whether the QPSK sends priority broadcast transmissions.

**Database Persistence -** Determines whether the QPSK stores the IP addresses of DHCTs in RAM.

**Note:** Occasionally, you may need to clear the IP addresses that DHCTs are currently using and replace them with new IP addresses. To accomplish this, use the Reset and Clear DB selection on the QPSK File menu. For more information, see Reset the QPSK Modulator Persistent Database.

### Advanced Parameter Settings - QPSK Modulator

In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any advanced parameters after you have set up the basic parameters, keep in mind the following guidelines and contact Cisco Services if you need further assistance.

**Important:** If you change any of the default parameters, you must stay within the signal capacity of your plant design. Otherwise, the DHCTs might not be able to communicate with the DBDS. In addition, you must reboot the QPSK modulator and wait for all corresponding DHCTs to sign on again before any changes take effect.

| Field | Description |
|---|---|
| Configuration File Name | Do not change this parameter without first consulting Cisco Services. |
| Service Channel Frequency | Enter a value from 8 to 26.5 MHz based on your plant design.<br>This parameter establishes the frequency that the DHCTs use to broadcast to the demodulators on this hub. |
| Backup Service Channel Frequency | If you are **NOT** using a backup service channel, enter the same value in this field that you entered for the Service Channel Frequency parameter on the basic parameters tab. Otherwise, enter a value from 8 to 26.5 MHz based on your plant design.<br>**Important:** We recommend that you not use a backup service channel. The backup service channel is used when the service channel fails. All reverse channel messaging is sent over the channel on which the DHCT achieves initial sign-on. If a backup service channel is in use, the DHCT may not be able to achieve initial sign-on. |
| Tuner Input Attenuator | The DHCT calibration setting based on the design targets of your RF plant and the combining networks. If you need assistance, contact Cisco Services.<br>The system will not connect to any levels that are in the fail range. |

## Add a QPSK Modulator

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

### Process Overview

The first step in setting up the two-way communication path for your network is to add a QPSK modulator. To add a content modulator to the DNCS, complete the following tasks.

1. Set up the modulator's basic parameters.
2. Set up the modulator's advanced parameters.

**Note:** For a list of information needed to add the modulator to the DNCS, go to Information to Add a QPSK Modulator.

## Add a QPSK Modulator

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

### Process Overview

The first step in setting up the two-way communication path for your network is to add a QPSK modulator. To add a content modulator to the DNCS, complete the following tasks.

1. Set up the modulator's basic parameters.
2. Set up the modulator's advanced parameters.

**Note:** For a list of information needed to add the modulator to the DNCS, go to Information to Add a QPSK Modulator.

### Add Basic Parameters

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click **File > New > QPSK**. The Set Up QPSK Modulator window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameter Settings - QPSK Modulator.

Use the following fields when you manage the basic parameters for a QPSK modulator.

| Field | Description |
|---|---|
| Hub Name | The hub associated with this content QPSK (if you have more than one defined). |
| Name | The name of this QPSK.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that allows you to easily identify the QPSK modulator and where it resides. |
| IP Address | The IP address for this QPSK.<br>Be careful to properly place the dots (.) between numbers. |
| Physical Address | The MAC address for the QPSK. |
| Subnet Mask | The subnet mask where this QPSK modulator resides. |
| Default Router | The IP address for the router associated with this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| DHCT Base IP Address | The base IP address for all DHCTs within the domain of this modulator. |
| DHCT Subnet Mask | The subnet mask for all DHCTs within the domain of this modulator. |
| Frequency | The RF output frequency assigned to this modulator.<br>This value can be from 70 MHz to 130 MHz in increments of 0.25 MHz. |
| DCM (DHCT Communications Mode) | Determines the DCM for the QPSK.<br>**Important:** Currently all DSG-capable DHCTs use a Mixed DOCSIS/DAVIC DCM. Unique code on Explorer 8300 DHCTs enables them to recognized a DCM of Mixed DOCSIS/DAVIC as DOCSIS. QPSK modulators that provide the BRF to hubs with Explorer 8300 DHCTs use a DCM of Mixed DOCSIS/DAVIC.<br>Select the appropriate DCM from one of the following choices:<br>▪ **DAVIC** - Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel.<br>▪ **Mixed DOCSIS/DAVIC** - Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel. |

| | |
|---|---|
| | ▪ **DOCSIS** - Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.) |
| Options | **Continuous Wave Mode -** Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK. |
| | **Front Panel Lock -** Determines whether changes can be made from the front panel. |
| | **Broadcast Only Mode -** Determines whether the QPSK sends priority broadcast transmissions. |
| | **Database Persistence -** Determines whether the QPSK stores the IP addresses of DHCTs in RAM.<br>**Note:** Occasionally, you may need to clear the IP addresses that DHCTs are currently using and replace them with new IP addresses. To accomplish this, use the Reset and Clear DB selection on the QPSK File menu. For more information, see Reset the QPSK Modulator Persistent Database. |

6. To continue adding a QPSK modulator to the DNCS, set up the advanced parameters for the QPSK modulator. Go to Add Advanced Parameters.

### Add Advanced Parameters

Complete these steps to set up the QPSK modulator advanced parameters.

1. On the Set Up QPSK Modulator window, click the **Advanced Parameters** tab. The Advanced Parameters window opens.
2. In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any of these parameters, refer to the guidelines listed in Advanced Parameter Settings - QPSK Modulator.

   In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any advanced parameters after you have set up the basic parameters, keep in mind the following guidelines and contact Cisco Services if you need further assistance.

   **Important:** If you change any of the default parameters, you must stay within the signal capacity of your plant design. Otherwise, the DHCTs might not be able to communicate with the DBDS. In addition, you must reboot the QPSK modulator and wait for all corresponding DHCTs to sign on again before any changes take effect.

| Field | Description |
|---|---|
| Configuration File Name | Do not change this parameter without first consulting Cisco Services. |
| Service Channel Frequency | Enter a value from 8 to 26.5 MHz based on your plant design.<br>This parameter establishes the frequency that the DHCTs use to broadcast to the demodulators on this hub. |
| Backup Service Channel Frequency | If you are **NOT** using a backup service channel, enter the same value in this field that you entered for the Service Channel Frequency parameter on the basic parameters tab. Otherwise, enter a value from 8 to 26.5 MHz based on your plant design.<br>**Important:** We recommend that you not use a backup service channel. The backup service channel is used when the service channel fails. All reverse channel messaging is sent over the channel on which the DHCT achieves initial sign-on. If a backup service channel is in use, the DHCT may not be able to achieve initial sign-on. |
| Tuner Input Attenuator | The DHCT calibration setting based on the design targets of your RF plant and the combining networks. If you need assistance, contact Cisco Services.<br>The system will not connect to any levels that are in the fail range. |

3. Click **Save**. The system saves the advanced parameters for this modulator in the DNCS database and closes the Set Up QPSK Modulator window. The QPSK List window updates to include the new QPSK modulator.
4. Cick **File > Close** to close the QPSK List window and return to the DNCS Administrative Console.
5. Add the new QPSK modulator to your network map.

### Related Topics

- Add a QPSK Demodulator
- Register the BRF With the BFS Client - for assistance multicasting out-of-band data to Explorer 8300 DHCTs in support of DOCSIS
- Set Up PowerKEY Conditional Access - for assistance supporting secure services, such as PPV, VOD, or

Web applications

## Modify a QPSK Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Open**

After a QPSK modulator has been saved in the DNCS, you can modify any of its parameters, except for the hub to which it is assigned.

1. On the DNCS Administrative Console, click the DNCS tab.
2. Click the Network **Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator you want to modify.
5. Click **File > Open**. The Set Up QPSK Modulator window opens for the QPSK modulator you selected.
6. @ either of the following topics:
   - Basic Parameter Settings - QPSK Modulator
   - Advanced Parameter Settings - QPSK Modulator
7. When you finish making changes, click **Save**. The system saves the new QPSK modulator information in the DNCS database and closes the Set Up QPSK Modulator window. The QPSK/CMTS List window updates to include the new QPSK modulator information.
8. Update your network map to reflect these changes.
9. Click **File > Close** to close the QPSK/CMTS List window and return to the DNCS Administrative Console.

Related Topics

- Set Up Your Network
- Locate the MAC Address of a QPSK Modulator

# Reset the QPSK Modulator Persistent Database

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > Reset and Clear DB**

### Why Reset QPSK Modulator Persistent Database?

Under normal circumstances, persistent database records should not be cleared. Clearing these causes DHCTs to disconnect from the QPSK modulator. Until the DHCTs sign back on, a process that may take hours, subscribers will be unable to use interactive services, such as VOD.

There are, however, some situations when it is necessary to clear and reset the QPSK the database, for example, if you need to reallocate the IP addresses of DHCTs. In other situations, it can be helpful to clear and reset the QPSK database, for example, when moving some DHCTs from one QPSK modulator to another. This page describes how to use the Reset and Clear DB selection on the QPSK File menu to reset and clear the QPSK persistent database.

Selecting this menu option clears the persistent database records for all associated DHCT IP addresses. All package and billing information remains intact and the persistent database function is maintained for future QPSK modulator resets.

### You Need to Know

Performance Impact

During this process no DHCTs for the QPSK modulator are rebooted. As a result, you can perform this procedure at any time. However, interactive services will be unavailable to subscribers until the DHCTs on the corresponding QPSK sign back on, a process that can take from a few minutes to a few hours, depending on several factors. For this reason, you may prefer to clear the database records during a maintenance period.

### Resetting the QPSK Modulator Persistent Database

Follow this procedure to clear the persistent database records for all associated DHCT IP addresses.

1. Make sure that you are aware of how resetting database records can impact system performance.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
5. Select the QPSK modulator that you want to reset.
6. Click **File > Reset and Clear DB**. A confirmation window displays prompting you to confirm that you want to reset the QPSK modulator, associated demodulator, and clear the status of all DHCTs that the modulator feeds.
7. Click **Yes**. The persistent database records for this QPSK modulator are cleared and the persistent database function for future QPSK modulator resets is maintained.
8. Do you have additional modulators to reset?
    - If **yes**, repeat this procedure from step 4 as many times as is necessary to reset additional modulators.
    - If **no**, go to step 9.
9. Click **File > Close** to close the QPSK/CMTS List window.

### Why Reset QPSK Modulator Persistent Database?

Under normal circumstances, persistent database records should not be cleared. Clearing these causes DHCTs to disconnect from the QPSK modulator. Until the DHCTs sign back on, a process that may take hours, subscribers will be unable to use interactive services, such as VOD.

There are, however, some situations when it is necessary to clear and reset the QPSK the database, for example, if you need to reallocate the IP addresses of DHCTs. In other situations, it can be helpful to clear and reset the QPSK database, for example, when moving some DHCTs from one QPSK modulator to another. This page describes how to use the Reset and Clear DB selection on the QPSK File menu to reset and clear the QPSK persistent database.

Selecting this menu option clears the persistent database records for all associated DHCT IP addresses. All package and billing information remains intact and the persistent database function is maintained for future QPSK modulator resets.

### You Need to Know

- Performance Impact

During this process no DHCTs for the QPSK modulator are rebooted. As a result, you can perform this procedure at any time. However, interactive services will be unavailable to subscribers until the DHCTs on the corresponding QPSK sign back on, a process that can take from a few minutes to a few hours, depending on several factors. For this reason, you may prefer to clear the database records during a maintenance period.

# Reset the QPSK Modulator Persistent Database

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > Reset and Clear DB**

### Why Reset QPSK Modulator Persistent Database?

Under normal circumstances, persistent database records should not be cleared. Clearing these causes DHCTs to disconnect from the QPSK modulator. Until the DHCTs sign back on, a process that may take hours, subscribers will be unable to use interactive services, such as VOD.

There are, however, some situations when it is necessary to clear and reset the QPSK the database, for example, if you need to reallocate the IP addresses of DHCTs. In other situations, it can be helpful to clear and reset the QPSK database, for example, when moving some DHCTs from one QPSK modulator to another. This page describes how to use the Reset and Clear DB selection on the QPSK File menu to reset and clear the QPSK persistent database.

Selecting this menu option clears the persistent database records for all associated DHCT IP addresses. All package and billing information remains intact and the persistent database function is maintained for future QPSK modulator resets.

### You Need to Know

Performance Impact

During this process no DHCTs for the QPSK modulator are rebooted. As a result, you can perform this procedure at any time. However, interactive services will be unavailable to subscribers until the DHCTs on the corresponding QPSK sign back on, a process that can take from a few minutes to a few hours, depending on several factors. For this reason, you may prefer to clear the database records during a maintenance period.

### Resetting the QPSK Modulator Persistent Database

Follow this procedure to clear the persistent database records for all associated DHCT IP addresses.

1. Make sure that you are aware of how resetting database records can impact system performance.
1. On the DNCS Administrative Console, click the **DNCS** tab.
1. Click the **Network Element Provisioning** tab.
1. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
1. Select the QPSK modulator that you want to reset.
1. Click **File > Reset and Clear DB**. A confirmation window displays prompting you to confirm that you want to reset the QPSK modulator, associated demodulator, and clear the status of all DHCTs that the modulator feeds.
1. Click **Yes**. The persistent database records for this QPSK modulator are cleared and the persistent database function for future QPSK modulator resets is maintained.
1. Do you have additional modulators to reset?
    - If **yes**, repeat this procedure from step 4 as many times as is necessary to reset additional modulators.
    - If **no**, go to step 9.
1. Click **File > Close** to close the QPSK/CMTS List window.

## Delete a QPSK Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Delete**

Use this procedure to delete a QPSK modulator from the DNCS database.

**Important:** If there are any QPSK demodulators connected to a QPSK modulator when you delete the modulator, the system automatically deletes those demodulators from the DNCS database.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator you want to delete.
5. Click **File > Delete Bridge.** A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the QPSK modulator information from the DNCS database and from the QPSK/CMTS List window. If there were any QPSK demodulators connected to this QPSK modulator, the system deletes those demodulators from the DNCS database.
7. Delete the QPSK modulator from your network map.
8. Click **File > Close** to close the QPSK/CMTS List window and return to the DNCS Administrative Console.

# QPSK Demodulator

A QPSK demodulator performs data error correction, and then passes the ATM cells upstream to the QPSK modulator. The QPSK demodulator also monitors power levels and slot timing of incoming DHCT signals. You can assign up to eight QPSK demodulators to one QPSK modulator.

**Note:** We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data. For more information about this software product, contact the representative who handles your account.

## What do you want to do?

- Review QPSK demodulator settings
- Add a QPSK demodulator
- Modify a QPSK demodulator
- Delete a QPSK demodulator

## QPSK Demodulator Settings

Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br><br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br><br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your plant design.<br><br>**Important:** We recommend the following guidelines:<br><br>▪Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)<br><br>▪Set all demodulators associated with the same modulator to the same frequency. |

# Add a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select Modulator] > File > Demodulators > File > New Demod**

### Information to Add a QPSK Demodulator

Before you add a QPSK demodulator to a QPSK modulator, you need the following information:

- Name of the modulator physically connected to this demodulator
- Port number where this demodulator is physically connected to the modulator
- Name of the node set you want to associate with this demodulator

**Important:** We recommend that you assign each demodulator to a unique node set.

- RF input frequency assigned to this demodulator

**Important:** We recommend the following:

- That you set this value to equal the service channel frequency of the associated modulator.
- That you set all demodulators associated with the same modulator to the same frequency.

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Process Overview

After you have added a QPSK modulator to the DNCS database, add all QPSK demodulators that are connected to that modulator. To add a QPSK demodulator to a QPSK modulator, follow this process.

1. If you have not already done so, add a node set for the demodulator. A node set represents the point where a group of reverse signals generated from DHCTs are combined and fed into a single QPSK demodulator.
2. Add a QPSK demodulator to a QPSK modulator by assigning each demodulator to the port number on the modulator that matches the actual physical connections between the modulator and demodulator.

   **Important:** We recommend that you set all demodulators associated with the same modulator to the same frequency.

**Note:** For a list of information needed to add the demodulator to the DNCS, go to Information to Add a QPSK Demodulator.

### Information to Add a QPSK Demodulator

Before you add a QPSK demodulator to a QPSK modulator, you need the following information:

- Name of the modulator physically connected to this demodulator
- Port number where this demodulator is physically connected to the modulator
- Name of the node set you want to associate with this demodulator

**Important:** We recommend that you assign each demodulator to a unique node set.

- RF input frequency assigned to this demodulator

**Important:** We recommend the following:

- That you set this value to equal the service channel frequency of the associated modulator.
- That you set all demodulators associated with the same modulator to the same frequency.

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

# Add a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select Modulator] > File > Demodulators > File > New Demod**

### Information to Add a QPSK Demodulator

Before you add a QPSK demodulator to a QPSK modulator, you need the following information:

- Name of the modulator physically connected to this demodulator
- Port number where this demodulator is physically connected to the modulator
- Name of the node set you want to associate with this demodulator

**Important:** We recommend that you assign each demodulator to a unique node set.

- RF input frequency assigned to this demodulator

**Important:** We recommend the following:

- That you set this value to equal the service channel frequency of the associated modulator.
- That you set all demodulators associated with the same modulator to the same frequency.

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Process Overview

After you have added a QPSK modulator to the DNCS database, add all QPSK demodulators that are connected to that modulator. To add a QPSK demodulator to a QPSK modulator, follow this process.

1. If you have not already done so, add a node set for the demodulator. A node set represents the point where a group of reverse signals generated from DHCTs are combined and fed into a single QPSK demodulator.
1. Add a QPSK demodulator to a QPSK modulator by assigning each demodulator to the port number on the modulator that matches the actual physical connections between the modulator and demodulator.

   **Important:** We recommend that you set all demodulators associated with the same modulator to the same frequency.

**Note:** For a list of information needed to add the demodulator to the DNCS, go to Information to Add a QPSK Demodulator.

### Adding a QPSK Demodulator

**Important:** Be very careful when you add a QPSK demodulator to the DNCS. Incorrectly configuring demodulators causes large numbers of DHCTs to be classified as non-responding units. In addition, the network management system will falsely log errors originating from incorrectly configured QPSK demodulators.

After you add a QPSK modulator to the DNCS, complete these steps to add all QPSK demodulators that are connected to that modulator.

1. Does a node set exist for this demodulator.
   - If **yes**, go to step 2.
   - If **no**, add a node set and then go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
5. Select the modulator to which you need to assign this demodulator.
6. Click **File > Demodulators**. The QPSK Modem window opens with an illustration of the modulator and its eight possible port connections.
7. Click **File > New Demod**. The Set Up QPSK Demodulator window opens.
8. Complete the fields on the screen as described in QPSK Demodulator Settings.

Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your plant design.<br>**Important:** We recommend the following guidelines:<br>▪ Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)<br>▪ Set all demodulators associated with the same modulator to the same frequency. |

9. Check the associated modulator service channel frequency (on the Advanced Parameters tab of the QPSK modulator window). The QPSK modulator's service channel frequency must match the frequency

of at least one of the associated demodulators. If at least one of the demodulator's frequencies does not match the service channel frequency of the associated modulator, change the frequency of one of the demodulators accordingly. For assistance changing the frequency, go to Modify a QPSK Demodulator.

10. Click **Save**.
    - The system saves the demodulator information in the DNCS database and closes the Set Up QPSK Demodulator window.
    - Then, the QPSK Modem window opens with the new demodulator appearing in the illustration.
    - An information window opens.
11. Click **OK** to close the information window.
12. Add the new QPSK demodulator to your network map.

## Modify a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator] > File > Open Demod**

After a QPSK demodulator has been saved in the DNCS, you can modify only the node set and RF output frequency assigned to that demodulator. To change any other parameters, you must delete the QPSK demodulator and then re-add it to the DNCS, using the new information.

**Important:** We recommend that you assign each demodulator to a unique node set. In addition, set all demodulators associated with the same modulator to the same frequency as the service channel for that modulator.

### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

### Modifying a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to modify.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the picture of the demodulator you want to modify, and then click **File > Open Demod**. The Set Up QPSK Demodulator window opens for the demodulator you selected.

   **Note:** You could also open this window by clicking the right mouse button on the demodulator picture on the QPSK Modem window, and then selecting **Open** from the menu that appears.

7. Make changes to the fields as described in QPSK Demodulator Settings.

   Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br><br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br><br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your |

plant design.

**Important:** We recommend the following guidelines:

- Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)
- Set all demodulators associated with the same modulator to the same frequency.

8. When you finish making changes, click **Save**. The system saves the demodulator information in the DNCS database. The Set Up QPSK Demodulator window closes. The QPSK Modem window opens with the new demodulator appearing in the illustration. An information window opens and directs you to check the associated modulator service channel frequency. The service channel frequency must match the frequency of at least one of the associated demodulators.

9. Click **OK** to close the information window.

10. Update your network map to reflect these changes.

## Modify a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator] > File > Open Demod**

After a QPSK demodulator has been saved in the DNCS, you can modify only the node set and RF output frequency assigned to that demodulator. To change any other parameters, you must delete the QPSK demodulator and then re-add it to the DNCS, using the new information.

**Important:** We recommend that you assign each demodulator to a unique node set. In addition, set all demodulators associated with the same modulator to the same frequency as the service channel for that modulator.

### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

### Modifying a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to modify.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the picture of the demodulator you want to modify, and then click **File > Open Demod**. The Set Up QPSK Demodulator window opens for the demodulator you selected.

   **Note:** You could also open this window by clicking the right mouse button on the demodulator picture on the QPSK Modem window, and then selecting **Open** from the menu that appears.

7. Make changes to the fields as described in QPSK Demodulator Settings.

   Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br><br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br><br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your |

plant design.

**Important:** We recommend the following guidelines:

- Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)
- Set all demodulators associated with the same modulator to the same frequency.

8. When you finish making changes, click **Save**. The system saves the demodulator information in the DNCS database. The Set Up QPSK Demodulator window closes. The QPSK Modem window opens with the new demodulator appearing in the illustration. An information window opens and directs you to check the associated modulator service channel frequency. The service channel frequency must match the frequency of at least one of the associated demodulators.

9. Click **OK** to close the information window.

10. Update your network map to reflect these changes.

## Delete a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator Name] > File > Delete Demod**

Use this procedure to delete a QPSK demodulator from the DNCS.

### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

### Deleting a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to delete.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the demodulator you want to delete, and then click **File > Delete Demod**. A confirmation window opens.

   **Note:** You could also click the right mouse button on the demodulator picture, and then select **Delete** from the menu that appears.

7. Click **Yes**. The confirmation window closes. The system removes the QPSK demodulator information from the DNCS database and from the QPSK Modem window.
8. Remove the QPSK demodulator from your network map.

## Delete a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator Name] > File > Delete Demod**

Use this procedure to delete a QPSK demodulator from the DNCS.

### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

### Deleting a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to delete.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the demodulator you want to delete, and then click **File > Delete Demod**. A confirmation window opens.

   **Note:** You could also click the right mouse button on the demodulator picture, and then select **Delete** from the menu that appears.

7. Click **Yes**. The confirmation window closes. The system removes the QPSK demodulator information from the DNCS database and from the QPSK Modem window.
8. Remove the QPSK demodulator from your network map.

# Set-Tops

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

From the DHCT Provisioning area you can manage the set-tops in your network.

## What do you want to do?

- Set up a set-top
- Modify a set-top
- Delete a set-top
- Manually Add Devices to the DNCS
- Link Devices to CVT Files
- Configure the Device Image File
- Customize set-top behavior (Customizing Functionality to Enhance Subscribers' Experience, Ways to Send Customized Behavior to Set-Tops)
- Authorize a set-top for a service
- Create and Update CVT Test Groups
- Load New Image Files onto the BFS
- Manage Device Images

## Setting Up Set-Tops

After you have set up all of your other network elements, you are ready to set up your set-tops in the DNCS.

### You Need to Know

Before You Begin

Before you begin setting up your set-top, you must make sure that you have set up all of your network elements and defined your system as being OpenCable compliant (if applicable).

### Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
2. Set up existing DHCTs.
3. Set up Aptiv Digital networks.

### Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

### Setting Up Existing DHCTs

To upgrade the operating system (OS) and Resident Application (ResApp) software on DHCTs that are already deployed, refer to the appropriate upgrade instructions for each DHCT model. If you cannot locate these instructions, contact Cisco Services.

To use the DHCT Configuration change or authorize services for an existing DHCT, see Authorizing a DHCT or CableCARD Module for Service.

### Setting Up Aptiv Digital Networks

If your network uses an Aptiv Digital Resident Application Server, contact your Aptiv Digital representative for compatibility requirements.

### Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
2. Set up existing DHCTs.
3. Set up Aptiv Digital networks.

### Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

### Setting Up Existing DHCTs

To upgrade the operating system (OS) and Resident Application (ResApp) software on DHCTs that are already deployed, refer to the appropriate upgrade instructions for each DHCT model. If you cannot locate these instructions, contact Cisco Services.

To use the DHCT Configuration change or authorize services for an existing DHCT, see Authorizing a DHCT or CableCARD Module for Service.

## Setting Up Set-Tops

After you have set up all of your other network elements, you are ready to set up your set-tops in the DNCS.

### You Need to Know

Before You Begin

Before you begin setting up your set-top, you must make sure that you have set up all of your network elements and defined your system as being OpenCable compliant (if applicable).

### Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
1. Set up existing DHCTs.
1. Set up Aptiv Digital networks.

### Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

### Setting Up Existing DHCTs

To upgrade the operating system (OS) and Resident Application (ResApp) software on DHCTs that are already deployed, refer to the appropriate upgrade instructions for each DHCT model. If you cannot locate these instructions, contact Cisco Services.

To use the DHCT Configuration change or authorize services for an existing DHCT, see Authorizing a DHCT or CableCARD Module for Service.

### Setting Up Aptiv Digital Networks

If your network uses an Aptiv Digital Resident Application Server, contact your Aptiv Digital representative for compatibility requirements.

## Manually Add Devices to the DNCS

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Select Option > New**

Devices (DHCTs and CableCARD modules) are normally added to the database through CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to add devices to the database.

## What do you want to do?

- Learn about Device Settings
- Learn about Adding Devices

### Device Settings

Use the following fields when you manage devices in the DNCS.

| Field | Description |
|---|---|
| Admin Status | Defines the administration status of the DHCT.<br>Click the arrow to select one of the following options from the Admin Status list:<br>▪Out of Service<br>▪In Service One Way<br>▪In Service Two Way select for CableCARD modules<br>▪Deployed |
| DHCT Type | Defines the device type you are adding.<br>Select the device type from the drop-down list. |
| Boot Page | Boot page for this device (if used). Leave blank if you are using bootloader |
| Primary VASP Name | Primary VASP for this device.<br>Click the arrow to select the Primary VASP Name from the drop-down list (leave blank if you are using bootloader). |
| S/W Table of Contents | The TOC file specific to this device type.<br>Click **Select** to browse to the correct toc file for this device (leave blank if you are using bootloader).<br>When you load the EMMs into the DNCS for a shipment of devices, a table of contents file (TOC file) is created and is available to your billing system. The TOC file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all devices in the shipment. |
| Billing ID | Billing ID of the device. |
| IP Address | IP address of the DNCS server. |
| IPV6 Address | If you have the IPv6 feature enabled, this field displays the IPv6 address of the DHCT. It is a read-only field. |
| DHCT Serial Number | Serial number of the device. |

### Related Topics

▪Adding Devices

### Adding Devices

1. On the Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** field, click **New**.
5. Click **By MAC Address** and type the MAC address of the device you want to add.
6. Click **Continue**. The Set Up DHCT window opens.
7. Enter information as described in Device Settings.

Use the following fields when you manage devices in the DNCS.

| Field | Description |
|---|---|
| Admin Status | Defines the administration status of the DHCT.<br>Click the arrow to select one of the following options from the Admin Status list:<br>▪ Out of Service<br>▪ In Service One Way<br>▪ In Service Two Way select for CableCARD modules<br>▪ Deployed |
| DHCT Type | Defines the device type you are adding.<br>Select the device type from the drop-down list. |
| Boot Page | Boot page for this device (if used). Leave blank if you are using bootloader |
| Primary VASP Name | Primary VASP for this device.<br>Click the arrow to select the Primary VASP Name from the drop-down list (leave blank if you are using bootloader). |
| S/W Table of Contents | The TOC file specific to this device type.<br>Click **Select** to browse to the correct toc file for this device (leave blank if you are using bootloader).<br>When you load the EMMs into the DNCS for a shipment of devices, a table of contents file (TOC file) is created and is available to your billing system. The TOC file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all devices in the shipment. |
| Billing ID | Billing ID of the device. |
| IP Address | IP address of the DNCS server. |
| IPV6 Address | If you have the IPv6 feature enabled, this field displays the IPv6 address of the DHCT. It is a read-only field. |
| DHCT Serial Number | Serial number of the device. |

8. Click **Save**.
9. Repeat this procedure from step 4 for every device you need to add to the database.
10. Close the Set Up DHCT window and the DHCT Provisioning window.
11. Your next step is to link the devices to CVT files. Go to Link Devices to CVT Files

## Link Devices to CVT Files

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Type > File > New**

Devices (DHCTs and CableCARD modules) are normally linked to their CVT files using the CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to link the devices to their CVT files.

## What do you want to do?

- Learn about CVT File Settings
- Learn about Linking Devices to CVT Files

### CVT File Settings

Use the following fields when you link devices to CVT files in the DNCS.

| Field | Description |
|---|---|
| DHCT Type Number | The DHCT Type number of the device that you are linking to the CVT file. |
| Revision | Software revision represented by the CVT files. |
| Org. Unit ID | The OUI portion of the device MAC address.<br>Type **00:02:DE**. |
| Name | The name representing the type of device you are linking. |
| Vendor | Manufacturer of this device.<br>Type **Scientific Atlanta**. |
| S/W Table of Contents | Table of contents (TOC) file related to the CVT file.<br>Click **Select** to browse to the correct TOC file (leave blank if you are using bootloader). |
| Boot Page Name | The name of the boot page associated with this device.<br>Click the arrow to select the boot page from the drop-down list (leave blank if you are using bootloader). |

### Related Topics

- Linking Devices to CVT Files

### Linking Devices to CVT Files

1. On the Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens.
4. Click **File > New**. The DHCT Type Details window opens.
5. Enter information as described in CVT File Settings.

Use the following fields when you link devices to CVT files in the DNCS.

| Field | Description |
|---|---|
| DHCT Type Number | The DHCT Type number of the device that you are linking to the CVT file. |
| Revision | Software revision represented by the CVT files. |
| Org. Unit ID | The OUI portion of the device MAC address.<br>Type **00:02:DE**. |
| Name | The name representing the type of device you are linking. |
| Vendor | Manufacturer of this device.<br>Type **Scientific Atlanta**. |
| S/W Table of Contents | Table of contents (TOC) file related to the CVT file.<br>Click **Select** to browse to the correct TOC file (leave blank if you are using bootloader). |
| Boot Page Name | The name of the boot page associated with this device.<br>Click the arrow to select the boot page from the drop-down list (leave blank if you are using bootloader). |

6. Click **Save** to close the DHCT Type Details window.
7. Click **File > Close** to close the DHCT Type List window.
8. Your next step is to configure the device image file. Go to Configure the Device Image File.

## Configure the Device Image File

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New**

After you link the devices (DHCTs and CableCARD modules) to their image files, you need to configure the image files.

## What do you want to do?

- Learn about the Device Image File Settings
- Learn about Configuring the Device Image File

### Device Image File Settings

Use the following fields when you configure device image files in the DNCS.

| Field | Description |
|---|---|
| Downloadable Files Tab | |
| Image ID | Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID.<br>**Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends. |
| File | The name of the image file.<br>Click **Browse** to select the appropriate set-top image file. |
| Description | Description of the image file. |
| DHCT Groups Tab | |
| Group ID | The group ID associated with this image file (if any). |
| Group Name | The name of the group associated with this image. |
| DHCT Downloads Tab | |
| DHCT Resource File | The resource file (settop.res) associated with this image.<br>Click **Browse** to locate the /dvs/resapp/settop.res file. |

### Related Topics

- Configuring the Device Image File

### Configuring the Device Image File

1. On the Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. Click **File > New**. The Set Up Downloadable File window opens.
6. Enter information as described in Device Image File Settings.

Use the following fields when you configure device image files in the DNCS.

| Field | Description |
|---|---|
| Downloadable Files Tab | |
| Image ID | Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID.<br>**Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends. |
| File | The name of the image file.<br>Click **Browse** to select the appropriate set-top image file. |
| Description | Description of the image file. |
| DHCT Groups Tab | |
| Group ID | The group ID associated with this image file (if any). |
| Group Name | The name of the group associated with this image. |
| DHCT Downloads Tab | |
| DHCT Resource File | The resource file (settop.res) associated with this image.<br>Click **Browse** to locate the /dvs/resapp/settop.res file. |

7. Click **Save**.
8. On the Image List window, click the **DHCT Groups** tab. The window updates to display device groups.
9. Click **File > New**. The Set Up DHCT Group window opens.
10. Enter information as described in Device Image File Settings.

Use the following fields when you configure device image files in the DNCS.

| Field | Description |
|---|---|
| Downloadable Files Tab | |
| Image ID | Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID.<br>**Note:** Typing a specific image ID allows you to use the |

| | |
|---|---|
| | same image ID for this image across multiple headends. |
| File | The name of the image file.<br>Click **Browse** to select the appropriate set-top image file. |
| Description | Description of the image file. |
| DHCT Groups Tab | |
| Group ID | The group ID associated with this image file (if any). |
| Group Name | The name of the group associated with this image. |
| DHCT Downloads Tab | |
| DHCT Resource File | The resource file (settop.res) associated with this image.<br>Click **Browse** to locate the /dvs/resapp/settop.res file. |

11. Click **Save** and close the Set Up DHCT Group window.
12. On the Image List window, click the **DHCT Downloads** tab. The window updates to display device downloads configured with the appropriate type and group.
13. Click **Advanced > Load DHCT Resource File**. The Load DHCT Resource File window opens.
14. Click **Browse** and select the **/dvs/resapp/settop.res** file.
15. Click **Save**.
16. Click **File > New**.
17. Change the group to the Group Name assigned to this image, if necessary.
18. Click **Save**.

## Modify a Set-Top

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Open**

Use this procedure to modify the settings for an individual set-top in your network.

### You Need to Know

Before You Begin

Before you begin, you must have either the MAC address or the serial number of the DHCT you want to modify. In addition, you must have your network map readily available.

### Modifying a Set-Top

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** area, click the **Open** option, if it is not already selected.
5. Do you know the MAC address for the set-top you want to modify?
   - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the set-top you want to modify.
   - If **no**, click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the set-top you want to modify.
6. Click **Continue**. The Set Up DHCT window opens for the set-top you selected.
7. Make the desired changes. If you need help completing any fields, refer to the appropriate staging or upgrade guide for this set-top model. If you cannot locate these guides, contact Cisco Services.
8. When you finish making changes, click **Save**. The system saves the new set-top information in the DNCS database.
9. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.
10. Update your network map to reflect these changes.
11. Do you need to modify another set-top?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.
12. Continue making any other changes that you need to make to your network.

## Modify a Set-Top

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Open**

Use this procedure to modify the settings for an individual set-top in your network.

### You Need to Know

Before You Begin

Before you begin, you must have either the MAC address or the serial number of the DHCT you want to modify. In addition, you must have your network map readily available.

### Modifying a Set-Top

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** area, click the **Open** option, if it is not already selected.
5. Do you know the MAC address for the set-top you want to modify?
   - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the set-top you want to modify.
   - If **no**, click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the set-top you want to modify.
6. Click **Continue**. The Set Up DHCT window opens for the set-top you selected.
7. Make the desired changes. If you need help completing any fields, refer to the appropriate staging or upgrade guide for this set-top model. If you cannot locate these guides, contact Cisco Services.
8. When you finish making changes, click **Save**. The system saves the new set-top information in the DNCS database.
9. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.
10. Update your network map to reflect these changes.
11. Do you need to modify another set-top?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.
12. Continue making any other changes that you need to make to your network.

## Delete a Set-Top

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Delete**

Use this procedure to delete an individual set-top from the DNCS.

### You Need to Know

Before You Begin

Before you begin, you must have either the MAC address or the serial number of the DHCT you want to modify. In addition, you must have your network map readily available.

### Deleting a Set-Top

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** area, click the **Delete** option.
5. Do you know the MAC address for the set-top you want to delete?
   - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the set-top you want to delete.
   - If **no**, click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the set-top you want to delete.
6. Click **Continue**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes and returns you to the DHCT Provisioning window. The system removes the set-top information from the DNCS database. If the set-top is powered on and connected to a television, it will now display encrypted video.
8. Delete the set-top from your network map.
9. Do you need to delete another set-top?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

## Delete a Set-Top

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Delete**

Use this procedure to delete an individual set-top from the DNCS.

### You Need to Know

Before You Begin

Before you begin, you must have either the MAC address or the serial number of the DHCT you want to modify. In addition, you must have your network map readily available.

### Deleting a Set-Top

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** area, click the **Delete** option.
5. Do you know the MAC address for the set-top you want to delete?
   - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the set-top you want to delete.
   - If **no**, click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the set-top you want to delete.
6. Click **Continue**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes and returns you to the DHCT Provisioning window. The system removes the set-top information from the DNCS database. If the set-top is powered on and connected to a television, it will now display encrypted video.
8. Delete the set-top from your network map.
9. Do you need to delete another set-top?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

## Customizing Functionality to Enhance Subscribers' Experience

Special software on our set-tops allows you to customize how a set-top functions so that you can tailor set-tops to meet the needs of your subscribers.

### Ways to Customize Set-Top Behavior

The following list gives only a few examples of the ways that you can customize a set-top.

- Allow subscribers to skip unauthorized channels.
- Allow subscribers to select which channel the set-top tunes to when powered on.
- Allow subscribers to select a preferred audio language for digital services.
- Choose the language that is most common for your area to be used with a set-top's wireless keyboard.
- Allow subscribers to choose a color scheme for the set-top user screens, or select a color scheme for subscribers.

### Ways to Send Customized Behavior to Set-Tops

After you have customized how you want the set-top to function, you can send this configuration to the set-tops in your system in any of the following ways:

- For all set-tops in the network (global configuration)
- For a single set-top (addressable configuration)
- For all set-tops in a specific hub (hub configuration)
- During the staging process, so that all set-tops receive this configuration when they are staged (staging defaults)

For assistance performing any of these tasks, refer to Enhancing Your Subscribers' Experience: SARA Configurable Options (part number 4002178). To obtain a copy of this publication, see Printed Resources.

### Ways to Customize Set-Top Behavior

The following list gives only a few examples of the ways that you can customize a set-top.

- Allow subscribers to skip unauthorized channels.
- Allow subscribers to select which channel the set-top tunes to when powered on.
- Allow subscribers to select a preferred audio language for digital services.
- Choose the language that is most common for your area to be used with a set-top's wireless keyboard.
- Allow subscribers to choose a color scheme for the set-top user screens, or select a color scheme for subscribers.

## Customizing Functionality to Enhance Subscribers' Experience

Special software on our set-tops allows you to customize how a set-top functions so that you can tailor set-tops to meet the needs of your subscribers.

### Ways to Customize Set-Top Behavior

The following list gives only a few examples of the ways that you can customize a set-top.

- Allow subscribers to skip unauthorized channels.
- Allow subscribers to select which channel the set-top tunes to when powered on.
- Allow subscribers to select a preferred audio language for digital services.
- Choose the language that is most common for your area to be used with a set-top's wireless keyboard.
- Allow subscribers to choose a color scheme for the set-top user screens, or select a color scheme for subscribers.

### Ways to Send Customized Behavior to Set-Tops

After you have customized how you want the set-top to function, you can send this configuration to the set-tops in your system in any of the following ways:

- For all set-tops in the network (global configuration)
- For a single set-top (addressable configuration)
- For all set-tops in a specific hub (hub configuration)
- During the staging process, so that all set-tops receive this configuration when they are staged (staging defaults)

For assistance performing any of these tasks, refer to Enhancing Your Subscribers' Experience: SARA Configurable Options (part number 4002178). To obtain a copy of this publication, see Printed Resources.

## Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

### Authorizing a Set-Top or CableCARD Module for a Service

1. Make sure the test set-top is connected to a television, as well as to an RF feed into your network.
2. Make sure both the set-top and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the set-top or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected already when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the **Admin Status** field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the set-top or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each package.

- If your system uses a Brick mode package, the set-top or CableCARD module must be authorized for that package as well. This should have been done when the set-top or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the Selected field.

12. In the **Options** area, make the following selections as appropriate:

    - **IPPV Enable** - If this set-top or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
    - **DMS Enable** - Enable this option to allow the set-top or CableCARD module to receive secure services.
    - **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
    - **Analog Enable** - If this set-top needs to display secure analog services, enable this option.

      **Note:** Your system and the set-top must be designed to display secure analog services for this option to work properly. If necessary, refer to the Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see Printed Resources.

    - **Fast Refresh Enable** - This option is used to send EMMs to set-top or CableCARD modules during staging. For more information, refer to the Explorer Digital Home Communications Terminal Staging Guide (part number 734375).
    - **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this set-top or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service. Go to Verify a Successful Service Setup for more information.

## Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

### Authorizing a Set-Top or CableCARD Module for a Service

1. Make sure the test set-top is connected to a television, as well as to an RF feed into your network.
2. Make sure both the set-top and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the set-top or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected already when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the **Admin Status** field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the set-top or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each package.

- If your system uses a Brick mode package, the set-top or CableCARD module must be authorized for that package as well. This should have been done when the set-top or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the Selected field.

12. In the **Options** area, make the following selections as appropriate:

    - **IPPV Enable** - If this set-top or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
    - **DMS Enable** - Enable this option to allow the set-top or CableCARD module to receive secure services.
    - **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
    - **Analog Enable** - If this set-top needs to display secure analog services, enable this option.

      **Note:** Your system and the set-top must be designed to display secure analog services for this option to work properly. If necessary, refer to the Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see Printed Resources.

    - **Fast Refresh Enable** - This option is used to send EMMs to set-top or CableCARD modules during staging. For more information, refer to the Explorer Digital Home Communications Terminal Staging Guide (part number 734375).
    - **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this set-top or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service. Go to Verify a Successful Service Setup for more information.

## Create and Update CVT Test Groups

**Quick Path - Create: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > DHCT Groups tab > File > New**

**Quick Path - Update: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > DHCT Groups tab > [select group] > File > Open**

To ensure a successful software download to all devices in the network, we recommend that you create a unique test group to test the CVT download process and the operation of the new software in your network.

This section provides instructions to create test groups.

### Related Topics

- CVT Test Group Settings
- Creating CVT Test Groups
- Updating CVT Test Groups
- Download Images to CVT Test Groups
- Verify that Test Devices Downloaded Software

### CVT Test Group Settings

Use the following fields when you manage CVT test groups in the DNCS.

| Field | Description |
|---|---|
| Group ID | The group ID for this CVT test group.<br>Type a unique group ID number (other than zero). |
| Group Name | The name of this CVT test group. |
| DHCT MAC Address | The MAC address of a device you want to add to the group.<br>**Note:** Before you add a CableCARD module to the group, the module must be installed in a host and functioning correctly. |

### Related Topics

- Creating CVT Test Groups
- Updating CVT Test Groups

### Creating CVT Test Groups

**Note:** If you have already created CVT test groups, do not complete this procedure. Go to Updating CVT Test Groups.

Complete the following steps to create CVT test groups for devices in the network.

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **DHCT Groups** tab. The DHCT Groups tab opens.
5. Select **File > New**. The Set Up DHCT Group window opens.
6. Configure the fields on the Set Up DHCT Group window as described in CVT Test Group Settings.

   Use the following fields when you manage CVT test groups in the DNCS.

| Field | Description |
|---|---|
| Group ID | The group ID for this CVT test group.<br>Type a unique group ID number (other than zero). |
| Group Name | The name of this CVT test group. |
| DHCT MAC Address | The MAC address of a device you want to add to the group.<br>**Note:** Before you add a CableCARD module to the group, the module must be installed in a host and functioning correctly. |

7. Click **Add**. The MAC address of the device moves to the Associated DHCTs column.
8. Repeat steps 6 and 7 for each device you want to add to the group.
9. Click **Save**. The new group appears in the list of group descriptions on the DHCT Groups tab.

**Note:** A device should be connected to the network within 2 hours of adding it to the group. If the device is not connected within 2 hours, the device does not receive a group assignment until the DNCS database cycles through all in-service devices (at a rate of approximately one device per second). Depending on the number of devices in your system, this process could take a significant amount of time.

10. Choose one of the following options to confirm that the device was successfully added to the test group:

    - **Set-tops:** Go to the diagnostic screens and view the **Group ID** field. This group ID should match the group ID displayed in the Set Up DHCT Group window on the DNCS.

      **Note:** The group ID on the DHCT diagnostic screen is in hexadecimal format. The group ID on the DNCS is in decimal format. You might need to convert the group ID to verify this step.

    - **CableCARD modules:** You cannot determine the group assignment of the CableCARD module from its diagnostic screens. Diagnostic screens are different for each host vendor. You can only determine that the CableCARD module downloaded software after you complete the download process. Go to Updating CVT Test Groups.

11. Do the Group ID values match?

- If **yes**, go to Updating CVT Test Groups.
- If **no**, contact Cisco Services.

### Updating CVT Test Groups

**Note:** If you need to create CVT test groups, do not complete this procedure. Go to Creating CVT Test Groups.

Complete the following steps to update test groups for devices in the network.

1. From the DHCT Groups tab in the Image List window, select the group you want to update from the list.
2. Click **File > Open**. The Set Up DHCT Group window for the group you selected opens.
3. Evaluate the list in the **Associated DHCTs** list. Are the Associated DHCTs listed correct?
   - If **yes**, click **Cancel**, and then go to Load New Image Files onto the BFS.
   - If **no**, add or remove MAC addresses (as needed), then click **Save**.
4. Do you need to modify another group?
   - If **yes**, repeat this procedure.
   - If **no**, go to Load New Image Files onto the BFS.

## Load New Image Files onto the BFS

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New**

The next step is to load the image files onto the BFS. Load only the image files for the devices that you have in your system.

**Important:**

- If a file is used by more than one device type or device revision, you only need to add that file once.
- Unnecessary files will slow the software download. Be careful to load only those files currently required by your system. Refer to Delete Unused Device Types from the Database for more information.

**Loading New Image Files onto the BFS**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. On the Image List window, click **File > New**. The Set Up Downloadable File window opens.
6. Do you want to specify an image ID?
   - If **yes**, type a unique **Image ID**.
   - If **no**, leave the Image ID field blank, and the DNCS will automatically assign an Image ID.

   **Note:** Typing a specific image ID allows you to use the same name for the image ID across multiple headends.
7. Click **Browse**. The Select Image File window opens.
8. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
9. Choose one of the following options for the Filter field:
   - **DHCTs:** Type **/dvs/resapp/xxx*rom**
   - **CableCARD modules:** Type **/dvs/cablecard/xxx*rom**

   **Note:** The "xxx" is part of the file name provided in the software release notes document.

   **Example:** For a DHCT, type **/dvs/resapp/141*rom**.
10. Click **Filter**. The directory entered becomes the working directory and a filters file list opens.
11. In the **Files** column, select the ROM file that you want to add to the list of downloadable files.

    **Example: 1419pe4a7.rom**
12. Click **OK**. The file path for the ROM file opens on the Set Up Downloadable File window.
13. In the **Downloadable File** window, copy or type the file name without the path in the **Description** field.

    **Example: 1419pe4a7.rom**
14. Click **Save**. The new file and file description appear in the Image List window.

**Note:** If the save fails, the file may already exist in the list.

## Load New Image Files onto the BFS

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New**

The next step is to load the image files onto the BFS. Load only the image files for the devices that you have in your system.

**Important:**

- If a file is used by more than one device type or device revision, you only need to add that file once.
- Unnecessary files will slow the software download. Be careful to load only those files currently required by your system. Refer to Delete Unused Device Types from the Database for more information.

**Loading New Image Files onto the BFS**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. On the Image List window, click **File > New**. The Set Up Downloadable File window opens.
6. Do you want to specify an image ID?
   - If **yes**, type a unique **Image ID**.
   - If **no**, leave the Image ID field blank, and the DNCS will automatically assign an Image ID.

   **Note:** Typing a specific image ID allows you to use the same name for the image ID across multiple headends.
7. Click **Browse**. The Select Image File window opens.
8. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
9. Choose one of the following options for the Filter field:
   - **DHCTs:** Type **/dvs/resapp/xxx*rom**
   - **CableCARD modules:** Type **/dvs/cablecard/xxx*rom**

   **Note:** The "xxx" is part of the file name provided in the software release notes document.

   **Example:** For a DHCT, type **/dvs/resapp/141*rom**.
10. Click **Filter**. The directory entered becomes the working directory and a filters file list opens.
11. In the **Files** column, select the ROM file that you want to add to the list of downloadable files.

    **Example: 1419pe4a7.rom**
12. Click **OK**. The file path for the ROM file opens on the Set Up Downloadable File window.
13. In the **Downloadable File** window, copy or type the file name without the path in the **Description** field.

    **Example: 1419pe4a7.rom**
14. Click **Save**. The new file and file description appear in the Image List window.

**Note:** If the save fails, the file may already exist in the list.

## Manage Device Images

This section is an overview of configuring and downloading client software to test groups or to your device population. For a full discussion of the procedures, including all the prerequisites required before your software download, refer to Downloading New Client Application Platform Installation Instructions (part number 4003052).

**Notes:**

- These procedures are valid for CVT downloads only. OSM downloads require different procedures. Refer to Explorer Digital Home Communications Terminal Staging Guide (part number 734375) for more information on OSM download requirements.
- You will need a secure GUI password to set up the image files. Obtain a secure GUI password from Cisco Services. This provides Cisco Services the opportunity to communicate known issues about the software as well as other information that may be needed before loading the software onto your network.

## What do you want to do?

- Delete Unused Device Types from the Database
- Load the settop.res File into the Database
- Download Images to CVT Test Groups
- Verify that Test Devices Downloaded Software
- Download Client Software to Devices

**Delete Unused Device Types from the Database**

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning > Type > [select type] > File > Delete**

**Delete Unused Device Types from the Database**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens, listing the device type, revision, OUI, and name.
4. Look at each entry in the list. Is the entry used in your system?
   - If **yes**, there is no need to delete this entry. Look at the next entry.
   - If **no**, or if you are not certain, go to step 5.
5. From the drop-down menu at the top of the DHCT Type List window, click **File > Delete**. The following message appears:

   **Are you sure you want to delete the current item?**

6. Click **Yes**.
7. Did an **Unspecified Error** message appear?
   - If **yes**, the selected device type is used in your system and you cannot delete it.
   - If **no**, the selected device type is not used in your system, and the DNCS deletes it from the database.
8. Repeat steps 4 through 7 for each device type in the DHCT Type List.
9. From the DHCT Type List window, click **File > Close**. The DHCT Type List closes.

**Delete Unused Device Types from the Database**

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning > Type > [select type] > File > Delete**

**Delete Unused Device Types from the Database**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens, listing the device type, revision, OUI, and name.
4. Look at each entry in the list. Is the entry used in your system?
   - If **yes**, there is no need to delete this entry. Look at the next entry.
   - If **no**, or if you are not certain, go to step 5.
5. From the drop-down menu at the top of the DHCT Type List window, click **File > Delete**. The following message appears:

   **Are you sure you want to delete the current item?**

6. Click **Yes**.
7. Did an **Unspecified Error** message appear?
   - If **yes**, the selected device type is used in your system and you cannot delete it.
   - If **no**, the selected device type is not used in your system, and the DNCS deletes it from the database.
8. Repeat steps 4 through 7 for each device type in the DHCT Type List.
9. From the DHCT Type List window, click **File > Close**. The DHCT Type List closes.

### Load the settop.res File into the Database

For CVT downloads, you must install the set-top resource file (settop.vxx) that contains the device types installed in your network. The system refers to this data during the image file download assignment process to verify software compatibility with the selected device type.

**Note:** The DNCS user interface for the CVT download was created before CableCARD modules existed. Therefore, the interface displays DHCT in several places where the more generic term **devices** would be more accurate. This is a cosmetic issue; all screens work as required for CableCARD modules.

### Loading the settop.res File into the Database

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List opens.
4. Click **Advanced > Load DHCT Resource File**. The Load DHCT Resource File window opens.

   **Note:** Though the screen only mentions DHCTs, you can load CableCARD module software using this screen.

5. Click **Browse**. The Select Control File window opens.
6. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
7. Choose one of the following options:
   - If you are installing the resource file from an FTP server, type / **export/home/dncs/download/settop*** in the Filter field.
   - If you are installing the resource file from a CD, complete the following steps.
   - Insert the CD containing the resource file into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.
   - Type **/cdrom/cdrom0/settop*** in the Filter field.
8. Click **Filter**. The Selection field updates with the directory from which you selected the resource file.
9. Click **settop.vxx** in the Files column.

   **Note:** This file is named settop.v followed by a version number (for example, **settop.v62**). Be sure that you select the latest version of this file.

10. Click **OK**. The DHCT Resource File field in the Load DHCT Resource File window updates to display the resource file path.
11. Click **Save**. Process Control file saved message appears on the Image List window.
12. On the Image List window, click **File > Close**.
13. Did you install the resource file from a CD?
    - If **yes**, type **eject cdrom** (in either the CD window or in an xterm window on the DNCS) and press **Enter**. The DNCS ejects the CD from the CD drive.
    - If **no**, you are finished with this procedure.

### Load the settop.res File into the Database

For CVT downloads, you must install the set-top resource file (settop.vxx) that contains the device types installed in your network. The system refers to this data during the image file download assignment process to verify software compatibility with the selected device type.

**Note:** The DNCS user interface for the CVT download was created before CableCARD modules existed. Therefore, the interface displays DHCT in several places where the more generic term **devices** would be more accurate. This is a cosmetic issue; all screens work as required for CableCARD modules.

### Loading the settop.res File into the Database

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List opens.
4. Click **Advanced > Load DHCT Resource File**. The Load DHCT Resource File window opens.

   **Note:** Though the screen only mentions DHCTs, you can load CableCARD module software using this screen.

5. Click **Browse**. The Select Control File window opens.
6. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
7. Choose one of the following options:
   - If you are installing the resource file from an FTP server, type / **export/home/dncs/download/settop*** in the Filter field.
   - If you are installing the resource file from a CD, complete the following steps.
   - Insert the CD containing the resource file into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.
   - Type **/cdrom/cdrom0/settop*** in the Filter field.
8. Click **Filter**. The Selection field updates with the directory from which you selected the resource file.
9. Click **settop.vxx** in the Files column.

   **Note:** This file is named settop.v followed by a version number (for example, **settop.v62**). Be sure that you select the latest version of this file.

10. Click **OK**. The DHCT Resource File field in the Load DHCT Resource File window updates to display the resource file path.
11. Click **Save**. Process Control file saved message appears on the Image List window.
12. On the Image List window, click **File > Close**.
13. Did you install the resource file from a CD?
    - If **yes**, type **eject cdrom** (in either the CD window or in an xterm window on the DNCS) and press **Enter**. The DNCS ejects the CD from the CD drive.
    - If **no**, you are finished with this procedure.

### Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

### Downloading Images to CVT Test Groups

**Important:** You will need a SW TOC Verification password (or secure GUI password) to complete the following steps. Contact Cisco Services to obtain a SW TOC Verification password.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter**.
3. Type **doctor -q** and press **Enter**. Initially, this command sends a ping command to the QAM to ensure the QAM is communicating with the DNCS. Then, a remote procedure call (RPC) request is sent to each QAM to validate that the higher-level functions in the QAM are working correctly.
4. Are all of the QAMs active in the network?
   - If **yes**, go to step 5.
   - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If the non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from the non-responding QAMs.

5. Click **Image**. The Image List window opens.
6. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.
7. Click on the top of the **Group** column to sort the list of device types by group.
8. Does a configured download already exist for the device type, revision, and group that you are testing?

- If **yes**, click to highlight the download and select **File > Open**.
- If **no**, go to step 10.

9. At the **File Description** field, click the down arrow and choose the new software. Go to step 12.
10. Select **File > New**. The Set Up DHCT Download window opens.
11. Complete the following steps to configure the Set Up DHCT Download window for the test download.
    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select the test group.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select **Emergency**.
12. On the Set Up DHCT Download window, click **Save**.

**Note:** An emergency download begins instantaneously and no barker opens to the subscriber.

**Result:** The Association Verification window opens.

13. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.
14. Configure the following fields on the Association Verification window:
    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.
15. Click **OK**.

**Results:**

- The Association Verification window closes.
- The Image List window is updated with the newly defined test download schedule.
- The software download to the device test groups begins.

16. Do you have more devices or groups to test?
    - If **yes**, repeat steps 7 through 15 for each group being tested.

      **Note:** Since a group can contain multiple device types, you might have multiple downloads to the same device group.

    - If **no**, in the Image List window, click **File > Close** to return to the Admin Console window.
17. Open an xterm window on the DNCS.
18. Type **cd /export/home/dncs/doctor** and press **Enter**.
19. Type **doctor -q** and press **Enter**.
20. Are all of the QAMs still active in the network?
    - If **yes**, go to step 21.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.
21. Your next step is to verify that the test device or devices downloaded software and operate as

expected. Go to Verify that Test Devices Downloaded Software for more information.

### Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

### Downloading Images to CVT Test Groups

**Important:** You will need a SW TOC Verification password (or secure GUI password) to complete the following steps. Contact Cisco Services to obtain a SW TOC Verification password.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter**.
3. Type **doctor -q** and press **Enter**. Initially, this command sends a ping command to the QAM to ensure the QAM is communicating with the DNCS. Then, a remote procedure call (RPC) request is sent to each QAM to validate that the higher-level functions in the QAM are working correctly.
4. Are all of the QAMs active in the network?
   - If **yes**, go to step 5.
   - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If the non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from the non-responding QAMs.

5. Click **Image**. The Image List window opens.
6. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.
7. Click on the top of the **Group** column to sort the list of device types by group.
8. Does a configured download already exist for the device type, revision, and group that you are testing?

- If **yes**, click to highlight the download and select **File > Open**.
- If **no**, go to step 10.

9. At the **File Description** field, click the down arrow and choose the new software. Go to step 12.
10. Select **File > New**. The Set Up DHCT Download window opens.
11. Complete the following steps to configure the Set Up DHCT Download window for the test download.
    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select the test group.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select **Emergency**.
12. On the Set Up DHCT Download window, click **Save**.

**Note:** An emergency download begins instantaneously and no barker opens to the subscriber.

**Result:** The Association Verification window opens.

13. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.
14. Configure the following fields on the Association Verification window:
    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.
15. Click **OK**.

**Results:**

- The Association Verification window closes.
- The Image List window is updated with the newly defined test download schedule.
- The software download to the device test groups begins.

16. Do you have more devices or groups to test?
    - If **yes**, repeat steps 7 through 15 for each group being tested.

      **Note:** Since a group can contain multiple device types, you might have multiple downloads to the same device group.

    - If **no**, in the Image List window, click **File > Close** to return to the Admin Console window.
17. Open an xterm window on the DNCS.
18. Type **cd /export/home/dncs/doctor** and press **Enter**.
19. Type **doctor -q** and press **Enter**.
20. Are all of the QAMs still active in the network?
    - If **yes**, go to step 21.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.
21. Your next step is to verify that the test device or devices downloaded software and operate as

expected. Go to Verify that Test Devices Downloaded Software for more information.

### Verify that Test Devices Downloaded Software

Verify that the test devices operate as expected by checking the following:

### Verifying that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-top.

### Verifying that CableCARD Modules Downloaded Software

- Verify that each host can display all authorized services.

### Verifying that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-top.

### Verify that Test Devices Downloaded Software

Verify that the test devices operate as expected by checking the following:

### Verifying that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-top.

### Verifying that CableCARD Modules Downloaded Software

- Verify that each host can display all authorized services.

### Download Client Software to Devices

The instructions in this section provide the steps to prepare and download the application platform software release to devices using the CVT method.

**Note:** This procedure is for downloading client software to your entire population of devices (set-tops and CableCARD modules). If you need the procedure to download only to a specific CVT group, follow the procedure in Download Images to CVT Test Groups.

### Examples of File Names and Version Numbers

The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

### Downloading Client Software to All Devices

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter**.
3. Type **doctor -q** and press **Enter**.
4. Are all of the QAMs active in the network?
   - If **yes**, go to step 5.
   - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from a non-responding QAM. This may cause the device to download incorrect software.

5. On the DNCS Administrative Console, select the **DNCS** tab and then select the **Home Element**

**Provisioning** tab.

6. Click **Image**. The Image List window opens.

7. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.

8. In the **DHCT Type** column, select the device type that will receive the new software where the value in the Group column is labeled Default.

9. Click **File > Delete**.

10. Repeat steps 8 and 9 for each device type that is receiving new software.

11. In an xterm window on the DNCS, type **listCVT** and press **Enter**. The listCVT report displays. Look for unused files in the report.

12. On the Image List window, select the **Downloadable Files** tab and compare the list of files displayed with the list of unused files listed in the listCVT report.

13. Select any unused file on the Downloadable Files tab.

14. Click **File > Delete**.

**Note:** The DNCS will not allow you to delete a file that is already associated with a download.

15. Repeat steps 13 and 14 until you have deleted all unused files.

16. On the Image List window, select the **DHCT Downloads** tab.

17. Click **File > New**. The Set Up DHCT Download window opens.

18. Complete the following steps to configure the Set Up DHCT Download window for the test download.

    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select **Default**.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old files or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select one of the following, based on the device type:
      - **DHCTs:** Select either **Normal** or **Immediate**. A Normal download does not begin until the DHCT is turned off.
      - **CableCARD modules**: Select **Immediate**.

19. Click **Save**. The Association Verification window opens.

20. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.

21. Configure the following fields on the Association Verification window:

    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.

22. Click **OK**. The system schedules the software download according to the schedule you configured earlier in this section.

23. Repeat steps 17 through 22 for each device type that you want to receive the software using the CVT method.

24. In an xterm window on the DNCS, type **cd /export/home/dncs/doctor** and press **Enter**.

25. Type **doctor -q** and press **Enter**.

26. Are all of the QAMs still active in the network?

    - If **yes**, you are finished with this procedure.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, contact Cisco Services.

### Examples of File Names and Version Numbers

The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

### Download Client Software to Devices

The instructions in this section provide the steps to prepare and download the application platform software release to devices using the CVT method.

**Note:** This procedure is for downloading client software to your entire population of devices (set-tops and CableCARD modules). If you need the procedure to download only to a specific CVT group, follow the procedure in Download Images to CVT Test Groups.

### Examples of File Names and Version Numbers

The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

### Downloading Client Software to All Devices

1. Open an xterm window on the DNCS.
1. Type **cd /export/home/dncs/doctor** and press **Enter**.
1. Type **doctor -q** and press **Enter**.
1. Are all of the QAMs active in the network?
    - If **yes**, go to step 5.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from a non-responding QAM. This may cause the device to download incorrect software.

1. On the DNCS Administrative Console, select the **DNCS** tab and then select the **Home Element**

**Provisioning** tab.

1. Click **Image**. The Image List window opens.

1. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.

1. In the **DHCT Type** column, select the device type that will receive the new software where the value in the Group column is labeled Default.

1. Click **File > Delete**.

1. Repeat steps 8 and 9 for each device type that is receiving new software.

1. In an xterm window on the DNCS, type **listCVT** and press **Enter**. The listCVT report displays. Look for unused files in the report.

1. On the Image List window, select the **Downloadable Files** tab and compare the list of files displayed with the list of unused files listed in the listCVT report.

1. Select any unused file on the Downloadable Files tab.

1. Click **File > Delete**.

**Note:** The DNCS will not allow you to delete a file that is already associated with a download.

1. Repeat steps 13 and 14 until you have deleted all unused files.

1. On the Image List window, select the **DHCT Downloads** tab.

1. Click **File > New**. The Set Up DHCT Download window opens.

1. Complete the following steps to configure the Set Up DHCT Download window for the test download.

    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select **Default**.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old files or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select one of the following, based on the device type:
        - **DHCTs:** Select either **Normal** or **Immediate**. A Normal download does not begin until the DHCT is turned off.
        - **CableCARD modules**: Select **Immediate**.

1. Click **Save**. The Association Verification window opens.

1. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.

1. Configure the following fields on the Association Verification window:

    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.

1. Click **OK**. The system schedules the software download according to the schedule you configured earlier in this section.

1. Repeat steps 17 through 22 for each device type that you want to receive the software using the CVT method.

1. In an xterm window on the DNCS, type **cd /export/home/dncs/doctor** and press **Enter**.
1. Type **doctor -q** and press **Enter**.
1. Are all of the QAMs still active in the network?
    - If **yes**, you are finished with this procedure.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, contact Cisco Services.

# PowerKEY CableCARD Modules

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

From the CableCARD Summary window you can display and manage the CableCARD modules in your system.

## What do you want to do?

- Learn about the different kinds of CableCARD modules and host devices
- Configure the DNCS for CableCARD and M-Card support
- Use the Filter to display information about CableCARD modules in your system
- Review Server Configuration options
- Manage CableCARD modules and hosts
- Maintain the host certificate revocation list (CRL)
- Set up the CableCARD MMI Copy Protection screen
- Identify error-handling conditions

## About CableCARD Modules

The PowerKEY CableCARD module complies with the OpenCable specification for a removable security device that separates a retail cable device from a cable provider's  conditional access system.

A CableCARD module  inserts into a slot on a host device, such as a set-top or a digital cable-ready television. Once inserted, the CableCARD module controls access to secure digital content so that authorized host devices can receive this content according to the CCI data for the program or event.

The host device, which can be purchased from a retail store or elsewhere, supplies all other basic tuning, navigation, and video display capabilities. If the host device is capable of receiving clear digital content, and the subscriber does not want to receive secure digital content, a CableCARD module is not required. However, if the subscriber wants to receive secure digital content, a CableCARD module is required.

The CableCARD module uses the PowerKEY Conditional Access System in the same manner as an Explorer DHCT to decrypt secure digital content. In fact, you authorize CableCARD modules for services in the same way that you authorize Explorer DHCTs.

### Related Topics

- M-Card Modules and SSC DHCTs
- Binding CableCARD Modules and Hosts
- PowerKEY CableCARD Modules

### M-Card Modules and SSC DHCTs

In addition to CableCARD modules, Separable Security Hosts with CableCARD Modules (SSC) set-tops also comply with OpenCable specification for a removable security device.

An SSC set-top includes the functionality of the stand-alone set-top, but adds the convenience of a factory-installed PowerKEY Multi-Stream CableCARD module (or M-Card ).

The M-Card module is mounted in the rear of the set-top and is secured with a cover plate to deter tampering. A label on the rear panel of the set-top provides the bar codes for the serial number and MAC address of the M-Card module.

Service providers should make every effort to ensure that the SSC combination (of the set-top and the CableCARD or M-Card module) remains together. If this combination is separated, the convenience of having the combination is lost, and you must either implement manual processes to redeploy either unit or return the set-top to us for repair.

### Related Topics

- About CableCARD Modules
- Binding CableCARD Modules and Hosts
- PowerKEY CableCARD Modules

### Binding CableCARD Modules and Hosts

For hosts to provide the high-value, copy-protected services authorized by a conditional access system, a CableCARD module and host must be bound.

Binding is a DNCS function that matches the MAC address of the CableCARD to the host ID of the host.

You must bind a CableCARD module to its host to authorize the bound pair to present "high-value" copy-protected services (services with copy protection settings of either copy one generation or copy never). However, services that are copy protected with the copy-protection setting of copy freely can be viewed by an unbound CableCARD and host pair.

SSC set-tops and M-Card modules use the combo-binding method. With this method, the SSC set-top downloads its EMMs during staging and the DNCS populates its database with the SSC pairing information from the staging inventory file.

The DNCS then sends pairing information (as a file named podData) to the BFS, which allows the SSC set-tops and M-Card modules to bind. This file contains two lists: an authorized list and an unauthorized list. Each list contains information on the SSC DHCT and its paired M-Card module.

The M-Card module reads the pairing information from the file. If the M-Card module finds its SSC pairing in the authorized list, it authorizes the binding between it and the SSC set-top. If it finds its SSC pairing in the unauthorized list, or if it does not find its SSC pairing in either list, it does not authorize the binding.

### Related Topics

- About CableCARD Modules
- M-Card Modules and SSC DHCTs
- PowerKEY CableCARD Modules

### CableCARD Module Binding Methods

Binding is a DNCS function that matches the MAC address of the CableCARD to the host ID of the host. You must bind a CableCARD module to its host before the CableCARD module can receive "high-value" copy-protected services (services with copy protection settings of either copy once or copy never). Services that are copy protected with the copy protection setting of copy freely can be viewed by an unbound host.

**Important:** Until you bind the SSC set-top and the CableCARD module, the set-top will not be able to display high-value, copy-protected services even if the set-top is authorized to receive these services.

You can choose to use one of the following copy protection binding methods:

- **Combo-binding** occurs when the SSC set-top downloads EMMs during staging. Sending the EMMs to the SSC set-top starts a process that adds the CableCARD module/host pair to a file (podData) on the BFS. After the pair is added to the file, the SSC set-top receives the podData file that authorizes the CableCARD module and the set-top to be bound.
- **Autobinding** matches a CableCARD module and host when the CableCARD module is inserted into the host and the host goes into two-way mode. Autobinding is available for two-way hosts only if **all** of the following conditions are met:
  - The DNCS is set up for autobinding.
  - The CableCARD module and host can be staged in a one-way or two-way environment.

    **Note:** To use autobinding, the CableCARD module and host must be bound in a two-way environment to view high-value content. Once bound, they can be used in a one-way environment.

  - The host is not on the certificate revocation list (CRL).
- **Manual binding** allows binding of the CableCARD module and host from either the DNCS or the billing system. From the DNCS, the CableCARD module ID and host ID are added to the DNCS through the CableCARD interface.
- **Billing-transaction** binding occurs from the billing system interface using the RegisterHost command. Contact your billing vendor to see if they support this option.

### Related Topics

- About CableCARD Modules
- M-Card Modules and SSC DHCTs
- PowerKEY CableCARD Modules

## CableCARD Summary Window

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

From the CableCARD Summary window you can display and manage the CableCARD modules in your system.

## What do you want to do?

- Learn more about CableCARD modules and host devices
- Learn about the fields in the CableCARD Data Summary window
- Review Server Configuration tasks
- Add a new CableCARD module and its associated host device to the DNCS database
- Modify a CableCARD module and its associated host device
- Delete a CableCARD module and its associated host device from the DNCS database
- Maintain the host certificate revocation list (CRL)
- Set up the CableCARD MMI Copy Protection screen
- Close the CableCARD Data Summary window by clicking **Exit all CableCARD screens**.

### CableCARD Summary Data

When you use the Filter to search for and display CableCARD modules, search results are shown in the CableCARD Summary window. The following table describes the settings listed in the CableCARD Summary window.

| Setting | Description |
|---|---|
| CableCARD ID | The unique identifier for the CableCARD module. This is the ID number that typically appears on the television screen immediately after the subscriber installs the CableCARD module. |
| CableCARD MAC Address | The MAC address for the CableCARD module. |
| Host ID | The unique identifier for the host device.<br><br>In one-way systems or in two-way systems with one-way hosts, this ID appears on the television screen immediately after the subscriber installs the CableCARD module. In two-way systems using two-way hosts, this ID appears in the CableCARD Summary window on the DNCS after the subscriber installs the CableCARD module if autobinding is enabled<br><br>**Important:** Although a host ID automatically appears in the CableCARD Summary window on the DNCS for autobinding of two-way hosts on two-way systems, you should verify that the host ID is valid. Otherwise, content-protection features may not function as expected. See CableCARD MMI Copy Protection Screen for information on configuring the behavior of the MMI screen in two-way hosts. |
| Host MAC Address | The MAC address of the CableCARD host. |
| Encoded Host ID | A Hexadecimal value derived from the host ID that identifies the manufacturer of the host device. |
| Host Change Count | Indicates the number of times that a given CableCARD host has been changed, including the current host.<br><br>This number is reset to zero (0) if the CableCARD host change count is equal to or greater than the Maximum Host Change Count Allowed setting when binding with a new host is performed via the CableCARD window or billing. |
| Host Bound | Indicates whether or not a host device associated with a specific CableCARD module is authorized to receive copy-protected content as follows:<br><br>▪**No** - the host is not authorized to receive copy-protected content<br>▪**Yes** - the host is authorized to receive copy-protected content |
| Active File Date | Indicates when the CableCARD/Host data will be, or was, removed from the podData file on the BFS. A date of 1/1/70 00:00:00 indicates that the module and host were never bound.<br><br>**Note:** During staging, a module/host pair is added to the podData file for the amount of time defined by the Authorization Time-Out Period setting for the CableCARD server. When the Authorization Time-out Period is reached, the module/host pair is removed from the file. |

### Related Topics

- CableCARD Filter

- CableCARD Module Binding Methods

## Manage CableCARD Modules and Hosts

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

From the CableCARD Summary window you can display and manage the CableCARD modules in the following ways:

- Add a new CableCARD module and its associated host device to the DNCS for manual binding
- Modify a CableCARD module and its associated host device
- Delete a CableCARD module and its associated host device from the DNCS database
- Remove conditional access services from CableCARD and M-Card modules

### Add a CableCARD Module and Host Pair

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Add CableCARD**

Each CableCARD module must be paired with a host device in the DNCS database before the host device can receive high-value, secure digital content.

Complete these steps to add a CableCARD module and its associated host device to the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **Add CableCARD**. The Add CableCARD window opens.
5. Enter the **CableCARD ID** or a **CableCARD MAC Address**, but not both, for this CableCARD module.

   **Note:** The system automatically completes the CableCARD MAC Address field, based on the CableCARD ID, after you save the CableCARD module information.

6. Click in the **Host ID** field and type the ID for the host device that is associated with this CableCARD module.

   **Note:** For best results, enter the Host ID and not the Host MAC Address.

7. In the **Host Bound** column, click **Yes** to allow the module and the host to bind.
8. Click **Save**. The CableCARD Summary window opens and displays the message "CableCARD saved successfully" in the status are of the window.
9. Do you need to add another CableCARD module and host device?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to return to the DNCS Administrative Console.

### Related Topics

- CableCARD Module and Host Pair Settings
- Manage CableCARD Modules and Hosts

### CableCARD Module and Host Pair Settings

Use the following fields when you manage CableCARD modules and host pairs in the DNCS.

| Field | Description |
|---|---|
| CableCARD ID | The ID for the CableCARD module. |
| CableCARD MAC Address | The MAC address of the CableCARD module.<br>The DNCS automatically completes this field based on the CableCARD ID you enter. |
| Host ID | The ID for the host associated with the CableCARD module. |
| Host MAC Address | The MAC address of the CableCARD host.<br>For example, an SSC set-top or a CableCARD-ready TV.<br>For best results, enter the **Host ID** and not the Host MAC Address. |
| Host Bound (Yes or No) | Determines whether the host and CableCARD module are unbound<br>Select one of the following options:<br>▪**Yes:** The host is authorized to receive high-value copy-protected content.<br>▪**No:** The host is not authorized to receive high-value copy-protected content. |

### Related Topics

- Add a CableCARD Module and Host Pair
- Manage CableCARD Modules and Hosts

### Modify a CableCARD Module and Host Pair

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > [Select CableCARD/ Host Pair] > Modify Selected CableCARD**

After you save a CableCARD module and its associated host device in the DNCS database, you can modify the following information about the module and host pair:

- Host device information
- Whether or not the host device is authorized to receive copy-protected content.

To modify the CableCARD module ID, delete the pair, and then re-add them with the updated information.

Complete these steps to modify the host device information for a specific CableCARD module and host pair.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD.** The CableCARD Data Summary window opens.
4. Click the corresponding circle in the **Select** column to choose the CableCARD module and host device that you need to modify.
5. Click **Modify Selected CableCARD**. The Modify CableCARD window opens for that CableCARD module and host device.
6. To change the ID of the host device, click in the **Host ID f**ield and type the new information.
7. To change whether or not the host device is authorized to receive high-value copy-protected content, in the **Host Bound** column, click **Yes** or **No** based on the following considerations:
   - Click **Yes** if the host device is authorized to receive high-value copy-protected content.
   - Click **No** if the host device is not authorized to receive high-value copy-protected content.
8. When you finish making changes, click **Save CableCARD**. The system saves the new information in the DNCS database and closes the Modify CableCARD window. The CableCARD Data Summary window updates to include the new information.
9. Do you need to modify another host device for a particular CableCARD module?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Exit All CableCARD screens** to return to the DNCS Administrative Console.

### Related Topics

- Fields Used to Modify a CableCARD Modules and Host Pair
- Manage CableCARD Modules and Hosts

### Fields Used to Modify CableCARD Module and Host Pair

Use the following fields when you modify a CableCARD module and host pair in the DNCS.

| Field | Description | Notes |
|---|---|---|
| Host ID | The ID for the host associated with the CableCARD module | Enter the ID for the host associated with the CableCARD module you are adding to the DNCS. |
| Host MAC Address | The MAC address of the CableCARD host | For example, an SSC set-top or a CableCARD-ready TV.<br>For best results, enter the **Host ID** and not the Host MAC Address. |
| Host Bound (Yes or No) | Determines whether the host and CableCARD module are unbound | Select one of the following options:<br>▪**Yes:** The host is authorized to receive high-value copy-protected content.<br>▪**No:** The host is not authorized to receive high-value copy-protected content. |

### Related Topics

- Modify a CableCARD Module and Host Pair
- Manage CableCARD Modules and Hosts

### Delete a CableCARD Module and Host Pair

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > [Select CableCARD/Host Pair] > Delete Selected CableCARD**

Complete these steps to separate (delete) a CableCARD module from its associated host device on the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click the corresponding circle in the **Select** column to choose the CableCARD module and host device that you want to delete.
5. Click **Delete Selected CableCARD**. A confirmation window opens asking if you are sure you want to delete the selected CableCARD module and host pair.
6. Click **OK** to confirm your decision. The question window closes and an alert window opens stating that the CableCARD module and host pair has been deleted.
7. Click **OK** to close the alert window. The CableCARD Data Summary window updates so that the deleted CableCARD module and host pair is no longer listed.
8. Do you need to delete another CableCARD module and host pair?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Exit all CableCARD screens** to return to the DNCS Administrative Console.

### Related Topics

- Manage CableCARD Modules and Hosts

### Remove Conditional Access Services from CableCARD and M-CARD Modules

When CableCARD or M-CARD modules are taken out of service, you only need to remove the conditional access to deauthorize the services on the CableCARD or M-CARD modules. These services may be reactivated when the CableCARD or M-CARD module is returned to service. You can remove the conditional access using the billing system or the DNCS as described in the following procedure.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Select the **By MAC Address** option and type the MAC Address of the CableCARD or M-CARD module.
5. Click **Continue**. The Set Up DHCT window opens. A CableCARD or M-CARD entry appears in the DHCT Type box.
6. Click the **Secure Services** tab. The Secure Services tab moves to the forefront.
7. In the **Packages** area, select the first package in the Selected list. Scroll to the bottom of the list, hold down the Shift key, and select the last package in the list to highlight all of the packages in the list.
8. Click **Remove**. All of the packages move to the Available list.
9. In the **Options** area, select the options that are required by your internal procedures.
10. Click **Save**. Your changes are saved and all package authorizations are removed from the CableCARD or M-CARD module.
11. Click **Close**. The Set Up DHCT window closes.

### Related Topics

- Manage CableCARD Modules and Hosts
- PowerKEY CableCARD Modules

## Server Configuration Window

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Server Configuration**

From the Server Configuration window, you can configure the CableCARD server process so that the DNCS can send information to CableCARD modules.The CableCARD server provides a CableCARD module/host pair with information that allows the CableCARD module to be authorized and activated for use. The authorization process differs according to the type of system and host used.

## What do you want to do?

- Learn about the CableCARD authorization process
- Review the information needed to configure the CableCARD server
- View the CableCARD server settings
- Configure the CableCARD server

### CableCARD Server Authorization Process

The CableCARD server provides a CableCARD module/host pair with information that allows the CableCARD module to be authorized and activated for use. The authorization process differs according to the type of system and host used.

In a **one-way system** or in a **two-way system with one-way hosts**, the CableCARD server provides the host with information that enables the host to display a message on its screen. The message prompts the subscriber to call the telephone number displayed to activate the CableCARD module.

In a **two-way system with two-way hosts**, the CableCARD server monitors a dedicated port on the DNCS to manage incoming requests from CableCARD modules. The server handles requests in one of two ways depending upon how the MMI CP screen is configured. If the MMI CP screen is configured to display for two-way hosts (the default setting), the server provides the host with information that enables the host to display a message. The message prompts the subscriber to call the telephone number displayed to activate the CableCARD module.

On the other hand, if the MMI CP screen is not configured to display for two-way hosts, the server uses a process called autobinding to automatically authorize the CableCARD module without requiring the subscriber to telephone for authorization.

**Note:** To view the current settings for the MMI CP screen, see Displaying the Set CableCARD MMI Copy Protection Window. To change these settings, see Configuring the CableCARD MMI CP Screen.

### Related Topics

- Information Needed to Configure the CableCARD Server
- CableCARD Server Settings
- Configure the CableCARD Server

### Information Needed to Configure the CableCARD Server

Before you begin, you must have the following information if you want to use autobinding for CableCARD modules:

- IP address of the server that is running the CCardServer process (usually the DNCS)
- Port number on the DNCS that the CableCARD server monitors for incoming CableCARD module requests (two-way systems only)

### Related Topics

- CableCARD Server Settings
- Configure the CableCARD Server

### CableCARD Server Settings

Use the following fields when you manage a CableCARD server in the DNCS.

| Field | Description |
|---|---|
| **CableCARD Server Address** | |
| IP Address | The IP address of the server that is running the CableCARD Server.<br>Typically, this is the IP address on the DNCS that connects to the QPSKs. For example, 10.253.0.1.<br>**Notes:**<br>▪Autobinding on: **IP address**<br>▪Autobinding off: **0.0.0.0**<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Port Number | The port number on the DNCS that the CableCARD server will monitor for incoming CableCARD module requests.<br>**Notes:**<br>▪Autobinding on: 13830<br>▪Autobinding off: 0 |
| **CableCARD Module Parameters** | |
| Authorization Time-Out Period (Hours) | The length of time the Host-CableCARD pair copy-protection authorization data is kept in the file on the BFS.<br>Enter **2** in this field.<br>**Notes:**<br>▪Negative values are not permitted in this field.<br>▪If you define a value greater than 2, be aware of the following issues:<br>•The podData file can contain no more than 1500 authorization entries. During staging, a pod/host pair is added to the podData file for the amount of time defined in this field. When the Authorization Time-out Period is reached, the pod/host pair is removed from the file.<br>•If you attempt to exceed 1500 entries during the timeout period you have defined, then pod/host pairs will be unable to bind. |
| DeAuthorization Time-Out Period (Days) | The number of days that the copy-protection deauthorization message for the CableCARD module/host pair is kept in the file on the BFS.<br>Enter **30** in this field. |
| Maximum Key Session Period (Decaseconds) | The rate (in decaseconds for single-stream capable mode and minutes for multi-stream capable mode) that the copy protection key changes.<br>Enter **10** in this field.<br>**Example:** For example, typing a 10 in this field would cause the copy protection key to change once every 100 seconds for modules in single-stream mode, and 10 minutes for modules in multi-stream mode. This occurs because any CableCARD or M-Card module in single-stream mode interprets this value in decaseconds, while any M-Card module in multi-stream mode interprets this value |

| | |
|---|---|
| | in minutes.<br><br>**Important:** Defining a rate less than 10 requires a large number of unnecessary calculations on the CableCARD. Defining a rate greater than 20 does not coincide with best security practices. |
| Maximum Host Change Count Allowed | The maximum number of times that a CableCARD module is allowed to autobind with a different host. When a module's Host Change Count equals this limit, it will no longer be allowed to autobind with a different host.<br><br>This feature can help prevent a subscriber's unauthorized use of CableCARD modules.<br><br>You can enter a value in the range from **0 to 99**.<br><br>▪Entering **0** in this field disables autobinding.<br><br>▪Entering **99** indicates that an unlimited number of autobindings can occur. This is the default setting. |
| RF Output | The channel over which the system delivers digital services.<br><br>Select **Channel 3**. |
| Card Authorization Phone Number | The telephone number that subscribers call to verify that their CableCARD module was authorized.<br><br>You can enter up to 20 alphanumeric characters, including spaces. |
| Maximum Bindings within Authorization Time-Out Period | The number of CableCARD modules and set-tops that can be bound during each staging period.<br><br>The recommended value for this setting is **1500**.<br><br>**Note:** This value cannot be changed from the Server Configuration window. To change this value, execute the modCCardStagingLimit script. For assistance using this script, refer to Change the CableCARD Module Staging Limit (part number 4020737). To obtain a copy of this publication, see Printed Resources. |

### Configure the CableCARD Server

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Summary window opens.
4. Click **Server Configuration**. The Server Configuration window opens.
5. Complete the fields on the screen as described in CableCARD Server Settings.

Use the following fields when you manage a CableCARD server in the DNCS.

| Field | Description |
|---|---|
| **CableCARD Server Address** | |
| IP Address | The IP address of the server that is running the CableCARD Server.<br>Typically, this is the IP address on the DNCS that connects to the QPSKs. For example, 10.253.0.1.<br>**Notes:**<br>▪ Autobinding on: **IP address**<br>▪ Autobinding off: **0.0.0.0**<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Port Number | The port number on the DNCS that the CableCARD server will monitor for incoming CableCARD module requests.<br>**Notes:**<br>▪ Autobinding on: 13830<br>▪ Autobinding off: 0 |
| **CableCARD Module Parameters** | |
| Authorization Time-Out Period (Hours) | The length of time the Host-CableCARD pair copy-protection authorization data is kept in the file on the BFS.<br>Enter **2** in this field.<br>**Notes:**<br>▪ Negative values are not permitted in this field.<br>▪ If you define a value greater than 2, be aware of the following issues:<br>▪ The podData file can contain no more than 1500 authorization entries. During staging, a pod/host pair is added to the podData file for the amount of time defined in this field. When the Authorization Time-out Period is reached, the pod/host pair is removed from the file.<br>▪ If you attempt to exceed 1500 entries during the timeout period you have defined, then pod/host pairs will be unable to bind. |
| DeAuthorization Time-Out Period (Days) | The number of days that the copy-protection deauthorization message for the CableCARD module/host pair is kept in the file on the BFS.<br>Enter **30** in this field. |

| | |
|---|---|
| Maximum Key Session Period (Decaseconds) | The rate (in decaseconds for single-stream capable mode and minutes for multi-stream capable mode) that the copy protection key changes.<br><br>Enter **10** in this field.<br><br>**Example:** For example, typing a 10 in this field would cause the copy protection key to change once every 100 seconds for modules in single-stream mode, and 10 minutes for modules in multi-stream mode. This occurs because any CableCARD or M-Card module in single-stream mode interprets this value in decaseconds, while any M-Card module in multi-stream mode interprets this value in minutes.<br><br>**Important:** Defining a rate less than 10 requires a large number of unnecessary calculations on the CableCARD. Defining a rate greater than 20 does not coincide with best security practices. |
| Maximum Host Change Count Allowed | The maximum number of times that a CableCARD module is allowed to autobind with a different host. When a module's Host Change Count equals this limit, it will no longer be allowed to autobind with a different host.<br><br>This feature can help prevent a subscriber's unauthorized use of CableCARD modules.<br><br>You can enter a value in the range from **0 to 99**.<br><br>▪ Entering **0** in this field disables autobinding.<br><br>▪ Entering **99** indicates that an unlimited number of autobindings can occur. This is the default setting. |
| RF Output | The channel over which the system delivers digital services.<br><br>Select **Channel 3**. |
| Card Authorization Phone Number | The telephone number that subscribers call to verify that their CableCARD module was authorized.<br><br>You can enter up to 20 alphanumeric characters, including spaces. |
| Maximum Bindings within Authorization Time-Out Period | The number of CableCARD modules and set-tops that can be bound during each staging period.<br><br>The recommended value for this setting is **1500**.<br><br>**Note:** This value cannot be changed from the Server Configuration window. To change this value, execute the modCCardStagingLimit script. For assistance using this script, refer to Change the CableCARD Module Staging Limit (part number 4020737). To obtain a copy of this publication, see Printed Resources. |

6. Click **Save**. The system saves the new information in the DNCS database and closes the Configure Server window. The message "CableCARD Server Configuration Saved Successfully" appears in the status area of the screen.

## Related Topics

- Server Configuration Window
- Information Needed to Configure the CableCARD Server

## CableCARD Filter

From the Filter area on the CableCARD Summary window, you can quickly retrieve information about the PowerKEY® CableCARD™ modules in your system. The Filter allows you to select CableCARD attributes, such as CableCARD ID or Host MAC address, and find the CableCARD modules in your system that meet your search criteria.

## What do you want to do?

- Learn about CableCARD Filter settings
- Review the information needed to filter CableCARD modules
- Use the Filter to display specific CableCARD modules in your system.

### CableCARD Filter Settings

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Filter**

This section describes CableCARD Filter options and provides examples to show how the Filter searches for CableCARD data based on your selections.

### Related Topics

- CableCARD Summary Data
- Learn about the Information Needed to Filter CableCARD modules
- Filter CableCARD Modules

### CableCARD Filter Options

The following table describes the Filter options for searching CableCARD modules.

| By Field | By Value | Examples |
|---|---|---|
| **CCard MAC Address** | Enter any part of a CableCARD MAC address in the By Value field to have the filter display CableCARD modules with MAC addresses that match any portion of the text entered in this field.<br>**Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons. | If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules with any of the following MAC addresses:<br>▪**AA:BB**:CC:EE:DD:FF<br>▪CC:**AA:BB**:CC:DD:EE<br>▪CC:FF:FF:DD:**AA:BB**<br>**Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above. |
| **Host MAC Address** | Enter any part of a Host MAC address in the By Value field to have the filter display CableCARD modules paired with hosts whose MAC addresses match any portion of the text entered in this field.<br>**Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons. | If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts that have any of the following MAC addresses:<br>▪**AA:BB**:CC:EE:DD:FF<br>▪CC:**AA:BB**:CC:DD:EE<br>▪CC:FF:FF:DD:**AA:BB**<br>**Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above. |
| **Vendor ID**<br>**Note:** The Vendor ID consists of the first three digits of a Host ID. These first three digits are used to identify the manufacturer (or vendor) of the host device. | Enter the Vendor ID for a host device in the By Value field to have the filter display CableCARD modules whose hosts have the same vendor ID.<br>**Note:** Enter only numbers in this field. | If you enter **0-38** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts whose Host IDs begin with 0-38.<br>Example: Any of the following Host IDs might be found:<br>▪**0-38**0-000-022-331<br>▪**0-38**0-000-022-141 |
| **CCard Binding** | ▪**Active Binding** - Only those | |

| | | |
|---|---|---|
| | CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the DNCS.<br>▪**Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast by the DNCS.<br>▪**Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content.<br>▪**Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content.<br>▪**Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content.<br>**Note:** For more information on revoked hosts, see Certification Revocation List. | |
| **CCard ID** | Enter any part of a CableCARD ID in the By Value field to have the filter display CableCARD modules with IDs that match any portion of the text entered in this field. | If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with CableCARD IDs that contain this number.<br>Example: The Filter would find any of the following CableCARD IDs: |

| | | |
|---|---|---|
| | | ▪**0-010**-670-850-691<br>▪0-011-028-3**00-10**8<br>▪0-011-039-01**0-010** |
| **Host ID** | Enter any part of a Host ID in the By Value field to have the filter display CableCARD modules with Host IDs that contain the number you have entered.<br><br>**Note:** Enter only numbers in this field. | If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with Host IDs that contain this number.<br><br>Example: The Filter would find any of the following Host IDs:<br><br>▪**0-010**-670-186-813<br>▪0-380-0**00-10**0-251<br>▪0-380-0**00-10**8-460 |

### CableCARD Filter Settings

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Filter**

This section describes CableCARD Filter options and provides examples to show how the Filter searches for CableCARD data based on your selections.

### Related Topics

- CableCARD Summary Data
- Learn about the Information Needed to Filter CableCARD modules
- Filter CableCARD Modules

### CableCARD Filter Options

The following table describes the Filter options for searching CableCARD modules.

| By Field | By Value | Examples |
|---|---|---|
| **CCard MAC Address** | Enter any part of a CableCARD MAC address in the By Value field to have the filter display CableCARD modules with MAC addresses that match any portion of the text entered in this field.<br>**Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons. | If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules with any of the following MAC addresses:<br>▪**AA:BB**:CC:EE:DD:FF<br>▪CC:**AA:BB**:CC:DD:EE<br>▪CC:FF:FF:DD:**AA:BB**<br>**Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above. |
| **Host MAC Address** | Enter any part of a Host MAC address in the By Value field to have the filter display CableCARD modules paired with hosts whose MAC addresses match any portion of the text entered in this field.<br>**Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons. | If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts that have any of the following MAC addresses:<br>▪**AA:BB**:CC:EE:DD:FF<br>▪CC:**AA:BB**:CC:DD:EE<br>▪CC:FF:FF:DD:**AA:BB**<br>**Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above. |
| **Vendor ID**<br>**Note:** The Vendor ID consists of the first three digits of a Host ID. These first three digits are used to identify the manufacturer (or vendor) of the host device. | Enter the Vendor ID for a host device in the By Value field to have the filter display CableCARD modules whose hosts have the same vendor ID.<br>**Note:** Enter only numbers in this field. | If you enter **0-38** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts whose Host IDs begin with 0-38.<br>Example: Any of the following Host IDs might be found:<br>▪**0-38**0-000-022-331<br>▪**0-38**0-000-022-141 |
| **CCard Binding** | ▪**Active Binding** - Only those | |

| | | |
|---|---|---|
| | CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the DNCS.<br>▪**Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast by the DNCS.<br>▪**Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content.<br>▪**Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content.<br>▪**Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content.<br>**Note:** For more information on revoked hosts, see Certification Revocation List. | |
| **CCard ID** | Enter any part of a CableCARD ID in the By Value field to have the filter display CableCARD modules with IDs that match any portion of the text entered in this field. | If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with CableCARD IDs that contain this number.<br>Example: The Filter would find any of the following CableCARD IDs: |

| | | |
|---|---|---|
| | | ▪**0-010**-670-850-691<br>▪0-011-028-3**00-10**8<br>▪0-011-039-01**0-010** |
| **Host ID** | Enter any part of a Host ID in the By Value field to have the filter display CableCARD modules with Host IDs that contain the number you have entered.<br><br>**Note:** Enter only numbers in this field. | If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with Host IDs that contain this number.<br><br>Example: The Filter would find any of the following Host IDs:<br><br>▪**0-010**-670-186-813<br>▪0-380-0**00-10**0-251<br>▪0-380-0**00-10**8-460 |

### Information Needed to Filter

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following CableCARD module/host pair parameters:

- CableCARD MAC address
- Host MAC address
- Vendor ID (The prefix consists of the first three digits of the Host ID. However,you can enter up to 13 digits and the system will search for hosts with IDs that match the digits that begin with the digits you entered.)
- CableCARD ID
- Host ID
- CableCARD binding status
  - **Active Binding** - Only those CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the DNCS.
  - **Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast by the DNCS.
  - **Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content.
  - **Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content (that is, unprovisioned), or have been deauthorized for copy-protected content.
  - **Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content.

### Related Topics

- CableCARD Filter Settings
- Display CableCARD Module Data

### Filter CableCARD Modules

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Filter**

Follow these instructions to use the Filter to display specific CableCARD modules in your system.

1. Click the **By Field** arrow and select one of the following options:
   - CCard MAC Address
   - Host MAC Address
   - Vendor ID (ID Prefix)
   - CCard Binding
   - CCard ID
   - Host ID

   **Note:** For a description of these options, see CableCARD Filter Settings.

2. Information in the By Value field varies according to the selection you made in step 1. Perform one of the following actions as appropriate:
   - Click in the **By Value** field and enter data in this field.
   - Click the **By Value** arrow and select the appropriate value.

   **Note:** For examples of how By Value data affects searches, see CableCARD Filter Settings.

3. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the CableCARD Summary window.

   **Notes:**

   - For information about the data displayed in the CableCARD Summary window, see CableCARD Summary Data.
   - You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: CableCARD ID, CableCARD MAC Address, Host ID, Host MAC Address, or Host Change Count. Clicking the same heading again displays the column in descending order.

### Related Topics

- Information Needed to Filter
- CableCARD Filter Options

## Manually Add Devices to the DNCS

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Select Option > New**

Devices (DHCTs and CableCARD modules) are normally added to the database through CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to add devices to the database.

## What do you want to do?

- Learn about Device Settings
- Learn about Adding Devices

### Device Settings

Use the following fields when you manage devices in the DNCS.

| Field | Description |
|---|---|
| Admin Status | Defines the administration status of the DHCT.<br>Click the arrow to select one of the following options from the Admin Status list:<br>▪Out of Service<br>▪In Service One Way<br>▪In Service Two Way select for CableCARD modules<br>▪Deployed |
| DHCT Type | Defines the device type you are adding.<br>Select the device type from the drop-down list. |
| Boot Page | Boot page for this device (if used). Leave blank if you are using bootloader |
| Primary VASP Name | Primary VASP for this device.<br>Click the arrow to select the Primary VASP Name from the drop-down list (leave blank if you are using bootloader). |
| S/W Table of Contents | The TOC file specific to this device type.<br>Click **Select** to browse to the correct toc file for this device (leave blank if you are using bootloader).<br>When you load the EMMs into the DNCS for a shipment of devices, a table of contents file (TOC file) is created and is available to your billing system. The TOC file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all devices in the shipment. |
| Billing ID | Billing ID of the device. |
| IP Address | IP address of the DNCS server. |
| IPV6 Address | If you have the IPv6 feature enabled, this field displays the IPv6 address of the DHCT. It is a read-only field. |
| DHCT Serial Number | Serial number of the device. |

### Related Topics

▪Adding Devices

### Adding Devices

1. On the Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. In the **Select Option** field, click **New**.
5. Click **By MAC Address** and type the MAC address of the device you want to add.
6. Click **Continue**. The Set Up DHCT window opens.
7. Enter information as described in Device Settings.

Use the following fields when you manage devices in the DNCS.

| Field | Description |
|---|---|
| Admin Status | Defines the administration status of the DHCT.<br>Click the arrow to select one of the following options from the Admin Status list:<br>▪ Out of Service<br>▪ In Service One Way<br>▪ In Service Two Way select for CableCARD modules<br>▪ Deployed |
| DHCT Type | Defines the device type you are adding.<br>Select the device type from the drop-down list. |
| Boot Page | Boot page for this device (if used). Leave blank if you are using bootloader |
| Primary VASP Name | Primary VASP for this device.<br>Click the arrow to select the Primary VASP Name from the drop-down list (leave blank if you are using bootloader). |
| S/W Table of Contents | The TOC file specific to this device type.<br>Click **Select** to browse to the correct toc file for this device (leave blank if you are using bootloader).<br>When you load the EMMs into the DNCS for a shipment of devices, a table of contents file (TOC file) is created and is available to your billing system. The TOC file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all devices in the shipment. |
| Billing ID | Billing ID of the device. |
| IP Address | IP address of the DNCS server. |
| IPV6 Address | If you have the IPv6 feature enabled, this field displays the IPv6 address of the DHCT. It is a read-only field. |
| DHCT Serial Number | Serial number of the device. |

8. Click **Save**.
9. Repeat this procedure from step 4 for every device you need to add to the database.
10. Close the Set Up DHCT window and the DHCT Provisioning window.
11. Your next step is to link the devices to CVT files. Go to Link Devices to CVT Files

## Link Devices to CVT Files

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Type > File > New**

Devices (DHCTs and CableCARD modules) are normally linked to their CVT files using the CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to link the devices to their CVT files.

## What do you want to do?

- Learn about CVT File Settings
- Learn about Linking Devices to CVT Files

### CVT File Settings

Use the following fields when you link devices to CVT files in the DNCS.

| Field | Description |
|---|---|
| DHCT Type Number | The DHCT Type number of the device that you are linking to the CVT file. |
| Revision | Software revision represented by the CVT files. |
| Org. Unit ID | The OUI portion of the device MAC address.<br>Type **00:02:DE**. |
| Name | The name representing the type of device you are linking. |
| Vendor | Manufacturer of this device.<br>Type **Scientific Atlanta**. |
| S/W Table of Contents | Table of contents (TOC) file related to the CVT file.<br>Click **Select** to browse to the correct TOC file (leave blank if you are using bootloader). |
| Boot Page Name | The name of the boot page associated with this device.<br>Click the arrow to select the boot page from the drop-down list (leave blank if you are using bootloader). |

### Related Topics

- Linking Devices to CVT Files

### Linking Devices to CVT Files

1. On the Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens.
4. Click **File > New**. The DHCT Type Details window opens.
5. Enter information as described in CVT File Settings.

Use the following fields when you link devices to CVT files in the DNCS.

| Field | Description |
|---|---|
| DHCT Type Number | The DHCT Type number of the device that you are linking to the CVT file. |
| Revision | Software revision represented by the CVT files. |
| Org. Unit ID | The OUI portion of the device MAC address.<br>Type **00:02:DE**. |
| Name | The name representing the type of device you are linking. |
| Vendor | Manufacturer of this device.<br>Type **Scientific Atlanta**. |
| S/W Table of Contents | Table of contents (TOC) file related to the CVT file.<br>Click **Select** to browse to the correct TOC file (leave blank if you are using bootloader). |
| Boot Page Name | The name of the boot page associated with this device.<br>Click the arrow to select the boot page from the drop-down list (leave blank if you are using bootloader). |

6. Click **Save** to close the DHCT Type Details window.
7. Click **File > Close** to close the DHCT Type List window.
8. Your next step is to configure the device image file. Go to Configure the Device Image File.

## Configure the Device Image File

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New**

After you link the devices (DHCTs and CableCARD modules) to their image files, you need to configure the image files.

## What do you want to do?

- Learn about the Device Image File Settings
- Learn about Configuring the Device Image File

### Device Image File Settings

Use the following fields when you configure device image files in the DNCS.

| Field | Description |
|---|---|
| Downloadable Files Tab | |
| Image ID | Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID.<br>**Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends. |
| File | The name of the image file.<br>Click **Browse** to select the appropriate set-top image file. |
| Description | Description of the image file. |
| DHCT Groups Tab | |
| Group ID | The group ID associated with this image file (if any). |
| Group Name | The name of the group associated with this image. |
| DHCT Downloads Tab | |
| DHCT Resource File | The resource file (settop.res) associated with this image.<br>Click **Browse** to locate the /dvs/resapp/settop.res file. |

### Related Topics

- Configuring the Device Image File

### Configuring the Device Image File

1. On the Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. Click **File > New**. The Set Up Downloadable File window opens.
6. Enter information as described in Device Image File Settings.

Use the following fields when you configure device image files in the DNCS.

| Field | Description |
|---|---|
| Downloadable Files Tab | |
| Image ID | Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID.<br>**Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends. |
| File | The name of the image file.<br>Click **Browse** to select the appropriate set-top image file. |
| Description | Description of the image file. |
| DHCT Groups Tab | |
| Group ID | The group ID associated with this image file (if any). |
| Group Name | The name of the group associated with this image. |
| DHCT Downloads Tab | |
| DHCT Resource File | The resource file (settop.res) associated with this image.<br>Click **Browse** to locate the /dvs/resapp/settop.res file. |

7. Click **Save**.
8. On the Image List window, click the **DHCT Groups** tab. The window updates to display device groups.
9. Click **File > New**. The Set Up DHCT Group window opens.
10. Enter information as described in Device Image File Settings.

Use the following fields when you configure device image files in the DNCS.

| Field | Description |
|---|---|
| Downloadable Files Tab | |
| Image ID | Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID.<br>**Note:** Typing a specific image ID allows you to use the |

| | |
|---|---|
| | same image ID for this image across multiple headends. |
| File | The name of the image file.<br>Click **Browse** to select the appropriate set-top image file. |
| Description | Description of the image file. |
| DHCT Groups Tab | |
| Group ID | The group ID associated with this image file (if any). |
| Group Name | The name of the group associated with this image. |
| DHCT Downloads Tab | |
| DHCT Resource File | The resource file (settop.res) associated with this image.<br>Click **Browse** to locate the /dvs/resapp/settop.res file. |

11. Click **Save** and close the Set Up DHCT Group window.
12. On the Image List window, click the **DHCT Downloads** tab. The window updates to display device downloads configured with the appropriate type and group.
13. Click **Advanced > Load DHCT Resource File**. The Load DHCT Resource File window opens.
14. Click **Browse** and select the **/dvs/resapp/settop.res** file.
15. Click **Save**.
16. Click **File > New**.
17. Change the group to the Group Name assigned to this image, if necessary.
18. Click **Save**.

## Create and Update CVT Test Groups

**Quick Path - Create: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > DHCT Groups tab > File > New**

**Quick Path - Update: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > DHCT Groups tab > [select group] > File > Open**

To ensure a successful software download to all devices in the network, we recommend that you create a unique test group to test the CVT download process and the operation of the new software in your network.

This section provides instructions to create test groups.

### Related Topics

- CVT Test Group Settings
- Creating CVT Test Groups
- Updating CVT Test Groups
- Download Images to CVT Test Groups
- Verify that Test Devices Downloaded Software

### CVT Test Group Settings

Use the following fields when you manage CVT test groups in the DNCS.

| Field | Description |
|---|---|
| Group ID | The group ID for this CVT test group.<br>Type a unique group ID number (other than zero). |
| Group Name | The name of this CVT test group. |
| DHCT MAC Address | The MAC address of a device you want to add to the group.<br>**Note:** Before you add a CableCARD module to the group, the module must be installed in a host and functioning correctly. |

### Related Topics

- Creating CVT Test Groups
- Updating CVT Test Groups

### Creating CVT Test Groups

**Note:** If you have already created CVT test groups, do not complete this procedure. Go to Updating CVT Test Groups.

Complete the following steps to create CVT test groups for devices in the network.

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **DHCT Groups** tab. The DHCT Groups tab opens.
5. Select **File > New**. The Set Up DHCT Group window opens.
6. Configure the fields on the Set Up DHCT Group window as described in CVT Test Group Settings.

   Use the following fields when you manage CVT test groups in the DNCS.

| Field | Description |
|---|---|
| Group ID | The group ID for this CVT test group.<br>Type a unique group ID number (other than zero). |
| Group Name | The name of this CVT test group. |
| DHCT MAC Address | The MAC address of a device you want to add to the group.<br>**Note:** Before you add a CableCARD module to the group, the module must be installed in a host and functioning correctly. |

7. Click **Add**. The MAC address of the device moves to the Associated DHCTs column.
8. Repeat steps 6 and 7 for each device you want to add to the group.
9. Click **Save**. The new group appears in the list of group descriptions on the DHCT Groups tab.

**Note:** A device should be connected to the network within 2 hours of adding it to the group. If the device is not connected within 2 hours, the device does not receive a group assignment until the DNCS database cycles through all in-service devices (at a rate of approximately one device per second). Depending on the number of devices in your system, this process could take a significant amount of time.

10. Choose one of the following options to confirm that the device was successfully added to the test group:

    - **Set-tops:** Go to the diagnostic screens and view the **Group ID** field. This group ID should match the group ID displayed in the Set Up DHCT Group window on the DNCS.

      **Note:** The group ID on the DHCT diagnostic screen is in hexadecimal format. The group ID on the DNCS is in decimal format. You might need to convert the group ID to verify this step.

    - **CableCARD modules:** You cannot determine the group assignment of the CableCARD module from its diagnostic screens. Diagnostic screens are different for each host vendor. You can only determine that the CableCARD module downloaded software after you complete the download process. Go to Updating CVT Test Groups.

11. Do the Group ID values match?

- If **yes**, go to Updating CVT Test Groups.
- If **no**, contact Cisco Services.

### Updating CVT Test Groups

**Note:** If you need to create CVT test groups, do not complete this procedure. Go to Creating CVT Test Groups.

Complete the following steps to update test groups for devices in the network.

1. From the DHCT Groups tab in the Image List window, select the group you want to update from the list.
2. Click **File > Open**. The Set Up DHCT Group window for the group you selected opens.
3. Evaluate the list in the **Associated DHCTs** list. Are the Associated DHCTs listed correct?
   - If **yes**, click **Cancel**, and then go to Load New Image Files onto the BFS.
   - If **no**, add or remove MAC addresses (as needed), then click **Save**.
4. Do you need to modify another group?
   - If **yes**, repeat this procedure.
   - If **no**, go to Load New Image Files onto the BFS.

## Load New Image Files onto the BFS

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New**

The next step is to load the image files onto the BFS. Load only the image files for the devices that you have in your system.

**Important:**

- If a file is used by more than one device type or device revision, you only need to add that file once.
- Unnecessary files will slow the software download. Be careful to load only those files currently required by your system. Refer to Delete Unused Device Types from the Database for more information.

**Loading New Image Files onto the BFS**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. On the Image List window, click **File > New**. The Set Up Downloadable File window opens.
6. Do you want to specify an image ID?
   - If **yes**, type a unique **Image ID**.
   - If **no**, leave the Image ID field blank, and the DNCS will automatically assign an Image ID.

   **Note:** Typing a specific image ID allows you to use the same name for the image ID across multiple headends.
7. Click **Browse**. The Select Image File window opens.
8. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
9. Choose one of the following options for the Filter field:
   - **DHCTs:** Type **/dvs/resapp/xxx*rom**
   - **CableCARD modules:** Type **/dvs/cablecard/xxx*rom**

   **Note:** The "xxx" is part of the file name provided in the software release notes document.

   **Example:** For a DHCT, type **/dvs/resapp/141*rom**.
10. Click **Filter**. The directory entered becomes the working directory and a filters file list opens.
11. In the **Files** column, select the ROM file that you want to add to the list of downloadable files.

    **Example: 1419pe4a7.rom**
12. Click **OK**. The file path for the ROM file opens on the Set Up Downloadable File window.
13. In the **Downloadable File** window, copy or type the file name without the path in the **Description** field.

    **Example: 1419pe4a7.rom**
14. Click **Save**. The new file and file description appear in the Image List window.

**Note:** If the save fails, the file may already exist in the list.

## Load New Image Files onto the BFS

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > Image > Downloadable Files tab > File > New**

The next step is to load the image files onto the BFS. Load only the image files for the devices that you have in your system.

**Important:**

- If a file is used by more than one device type or device revision, you only need to add that file once.
- Unnecessary files will slow the software download. Be careful to load only those files currently required by your system. Refer to Delete Unused Device Types from the Database for more information.

**Loading New Image Files onto the BFS**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. On the Image List window, click **File > New**. The Set Up Downloadable File window opens.
6. Do you want to specify an image ID?
   - If **yes**, type a unique **Image ID**.
   - If **no**, leave the Image ID field blank, and the DNCS will automatically assign an Image ID.

   **Note:** Typing a specific image ID allows you to use the same name for the image ID across multiple headends.
7. Click **Browse**. The Select Image File window opens.
8. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
9. Choose one of the following options for the Filter field:
   - **DHCTs:** Type **/dvs/resapp/xxx*rom**
   - **CableCARD modules:** Type **/dvs/cablecard/xxx*rom**

   **Note:** The "xxx" is part of the file name provided in the software release notes document.

   **Example:** For a DHCT, type **/dvs/resapp/141*rom**.
10. Click **Filter**. The directory entered becomes the working directory and a filters file list opens.
11. In the **Files** column, select the ROM file that you want to add to the list of downloadable files.

    **Example: 1419pe4a7.rom**
12. Click **OK**. The file path for the ROM file opens on the Set Up Downloadable File window.
13. In the **Downloadable File** window, copy or type the file name without the path in the **Description** field.

    **Example: 1419pe4a7.rom**
14. Click **Save**. The new file and file description appear in the Image List window.

**Note:** If the save fails, the file may already exist in the list.

## Manage Device Images

This section is an overview of configuring and downloading client software to test groups or to your device population. For a full discussion of the procedures, including all the prerequisites required before your software download, refer to Downloading New Client Application Platform Installation Instructions (part number 4003052).

**Notes:**

- These procedures are valid for CVT downloads only. OSM downloads require different procedures. Refer to Explorer Digital Home Communications Terminal Staging Guide (part number 734375) for more information on OSM download requirements.
- You will need a secure GUI password to set up the image files. Obtain a secure GUI password from Cisco Services. This provides Cisco Services the opportunity to communicate known issues about the software as well as other information that may be needed before loading the software onto your network.

## What do you want to do?

- Delete Unused Device Types from the Database
- Load the settop.res File into the Database
- Download Images to CVT Test Groups
- Verify that Test Devices Downloaded Software
- Download Client Software to Devices

**Delete Unused Device Types from the Database**

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning > Type > [select type] > File > Delete**

**Delete Unused Device Types from the Database**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens, listing the device type, revision, OUI, and name.
4. Look at each entry in the list. Is the entry used in your system?
   - If **yes**, there is no need to delete this entry. Look at the next entry.
   - If **no**, or if you are not certain, go to step 5.
5. From the drop-down menu at the top of the DHCT Type List window, click **File > Delete**. The following message appears:

   **Are you sure you want to delete the current item?**

6. Click **Yes**.
7. Did an **Unspecified Error** message appear?
   - If **yes**, the selected device type is used in your system and you cannot delete it.
   - If **no**, the selected device type is not used in your system, and the DNCS deletes it from the database.
8. Repeat steps 4 through 7 for each device type in the DHCT Type List.
9. From the DHCT Type List window, click **File > Close**. The DHCT Type List closes.

**Delete Unused Device Types from the Database**

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning > Type > [select type] > File > Delete**

**Delete Unused Device Types from the Database**

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens, listing the device type, revision, OUI, and name.
4. Look at each entry in the list. Is the entry used in your system?
   - If **yes**, there is no need to delete this entry. Look at the next entry.
   - If **no**, or if you are not certain, go to step 5.
5. From the drop-down menu at the top of the DHCT Type List window, click **File > Delete**. The following message appears:

   **Are you sure you want to delete the current item?**

6. Click **Yes**.
7. Did an **Unspecified Error** message appear?
   - If **yes**, the selected device type is used in your system and you cannot delete it.
   - If **no**, the selected device type is not used in your system, and the DNCS deletes it from the database.
8. Repeat steps 4 through 7 for each device type in the DHCT Type List.
9. From the DHCT Type List window, click **File > Close**. The DHCT Type List closes.

### Load the settop.res File into the Database

For CVT downloads, you must install the set-top resource file (settop.vxx) that contains the device types installed in your network. The system refers to this data during the image file download assignment process to verify software compatibility with the selected device type.

**Note:** The DNCS user interface for the CVT download was created before CableCARD modules existed. Therefore, the interface displays DHCT in several places where the more generic term **devices** would be more accurate. This is a cosmetic issue; all screens work as required for CableCARD modules.

### Loading the settop.res File into the Database

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List opens.
4. Click **Advanced > Load DHCT Resource File**. The Load DHCT Resource File window opens.

   **Note:** Though the screen only mentions DHCTs, you can load CableCARD module software using this screen.

5. Click **Browse**. The Select Control File window opens.
6. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
7. Choose one of the following options:
   - If you are installing the resource file from an FTP server, type / **export/home/dncs/download/settop*** in the Filter field.
   - If you are installing the resource file from a CD, complete the following steps.
   - Insert the CD containing the resource file into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.
   - Type **/cdrom/cdrom0/settop*** in the Filter field.
8. Click **Filter**. The Selection field updates with the directory from which you selected the resource file.
9. Click **settop.vxx** in the Files column.

   **Note:** This file is named settop.v followed by a version number (for example, **settop.v62**). Be sure that you select the latest version of this file.

10. Click **OK**. The DHCT Resource File field in the Load DHCT Resource File window updates to display the resource file path.
11. Click **Save**. Process Control file saved message appears on the Image List window.
12. On the Image List window, click **File > Close**.
13. Did you install the resource file from a CD?
    - If **yes**, type **eject cdrom** (in either the CD window or in an xterm window on the DNCS) and press **Enter**. The DNCS ejects the CD from the CD drive.
    - If **no**, you are finished with this procedure.

### Load the settop.res File into the Database

For CVT downloads, you must install the set-top resource file (settop.vxx) that contains the device types installed in your network. The system refers to this data during the image file download assignment process to verify software compatibility with the selected device type.

**Note:** The DNCS user interface for the CVT download was created before CableCARD modules existed. Therefore, the interface displays DHCT in several places where the more generic term **devices** would be more accurate. This is a cosmetic issue; all screens work as required for CableCARD modules.

### Loading the settop.res File into the Database

1. On the DNCS Administrative Console, select the **DNCS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List opens.
4. Click **Advanced > Load DHCT Resource File**. The Load DHCT Resource File window opens.

   **Note:** Though the screen only mentions DHCTs, you can load CableCARD module software using this screen.

5. Click **Browse**. The Select Control File window opens.
6. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
7. Choose one of the following options:
   - If you are installing the resource file from an FTP server, type / **export/home/dncs/download/settop*** in the Filter field.
   - If you are installing the resource file from a CD, complete the following steps.
   - Insert the CD containing the resource file into the CD drive of the DNCS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.
   - Type **/cdrom/cdrom0/settop*** in the Filter field.
8. Click **Filter**. The Selection field updates with the directory from which you selected the resource file.
9. Click **settop.vxx** in the Files column.

   **Note:** This file is named settop.v followed by a version number (for example, **settop.v62**). Be sure that you select the latest version of this file.

10. Click **OK**. The DHCT Resource File field in the Load DHCT Resource File window updates to display the resource file path.
11. Click **Save**. Process Control file saved message appears on the Image List window.
12. On the Image List window, click **File > Close**.
13. Did you install the resource file from a CD?
    - If **yes**, type **eject cdrom** (in either the CD window or in an xterm window on the DNCS) and press **Enter**. The DNCS ejects the CD from the CD drive.
    - If **no**, you are finished with this procedure.

### Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

### Downloading Images to CVT Test Groups

**Important:** You will need a SW TOC Verification password (or secure GUI password) to complete the following steps. Contact Cisco Services to obtain a SW TOC Verification password.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter**.
3. Type **doctor -q** and press **Enter**. Initially, this command sends a ping command to the QAM to ensure the QAM is communicating with the DNCS. Then, a remote procedure call (RPC) request is sent to each QAM to validate that the higher-level functions in the QAM are working correctly.
4. Are all of the QAMs active in the network?
   - If **yes**, go to step 5.
   - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If the non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from the non-responding QAMs.

5. Click **Image**. The Image List window opens.
6. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.
7. Click on the top of the **Group** column to sort the list of device types by group.
8. Does a configured download already exist for the device type, revision, and group that you are testing?

- If **yes**, click to highlight the download and select **File > Open**.
- If **no**, go to step 10.

9. At the **File Description** field, click the down arrow and choose the new software. Go to step 12.
10. Select **File > New**. The Set Up DHCT Download window opens.
11. Complete the following steps to configure the Set Up DHCT Download window for the test download.
    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select the test group.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select **Emergency**.
12. On the Set Up DHCT Download window, click **Save**.

**Note:** An emergency download begins instantaneously and no barker opens to the subscriber.

**Result:** The Association Verification window opens.

13. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.
14. Configure the following fields on the Association Verification window:
    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.
15. Click **OK**.

**Results:**

- The Association Verification window closes.
- The Image List window is updated with the newly defined test download schedule.
- The software download to the device test groups begins.

16. Do you have more devices or groups to test?
    - If **yes**, repeat steps 7 through 15 for each group being tested.

      **Note:** Since a group can contain multiple device types, you might have multiple downloads to the same device group.

    - If **no**, in the Image List window, click **File > Close** to return to the Admin Console window.
17. Open an xterm window on the DNCS.
18. Type **cd /export/home/dncs/doctor** and press **Enter**.
19. Type **doctor -q** and press **Enter**.
20. Are all of the QAMs still active in the network?
    - If **yes**, go to step 21.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.
21. Your next step is to verify that the test device or devices downloaded software and operate as

expected. Go to Verify that Test Devices Downloaded Software for more information.

### Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

### Downloading Images to CVT Test Groups

**Important:** You will need a SW TOC Verification password (or secure GUI password) to complete the following steps. Contact Cisco Services to obtain a SW TOC Verification password.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter**.
3. Type **doctor -q** and press **Enter**. Initially, this command sends a ping command to the QAM to ensure the QAM is communicating with the DNCS. Then, a remote procedure call (RPC) request is sent to each QAM to validate that the higher-level functions in the QAM are working correctly.
4. Are all of the QAMs active in the network?
   - If **yes**, go to step 5.
   - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If the non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from the non-responding QAMs.

5. Click **Image**. The Image List window opens.
6. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.
7. Click on the top of the **Group** column to sort the list of device types by group.
8. Does a configured download already exist for the device type, revision, and group that you are testing?

- If **yes**, click to highlight the download and select **File > Open**.
- If **no**, go to step 10.

9. At the **File Description** field, click the down arrow and choose the new software. Go to step 12.
10. Select **File > New**. The Set Up DHCT Download window opens.
11. Complete the following steps to configure the Set Up DHCT Download window for the test download.
    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select the test group.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select **Emergency**.
12. On the Set Up DHCT Download window, click **Save**.

**Note:** An emergency download begins instantaneously and no barker opens to the subscriber.

**Result:** The Association Verification window opens.

13. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.
14. Configure the following fields on the Association Verification window:
    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.
15. Click **OK**.

**Results:**

- The Association Verification window closes.
- The Image List window is updated with the newly defined test download schedule.
- The software download to the device test groups begins.

16. Do you have more devices or groups to test?
    - If **yes**, repeat steps 7 through 15 for each group being tested.

      **Note:** Since a group can contain multiple device types, you might have multiple downloads to the same device group.

    - If **no**, in the Image List window, click **File > Close** to return to the Admin Console window.
17. Open an xterm window on the DNCS.
18. Type **cd /export/home/dncs/doctor** and press **Enter**.
19. Type **doctor -q** and press **Enter**.
20. Are all of the QAMs still active in the network?
    - If **yes**, go to step 21.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.
21. Your next step is to verify that the test device or devices downloaded software and operate as

expected. Go to Verify that Test Devices Downloaded Software for more information.

### Verify that Test Devices Downloaded Software

Verify that the test devices operate as expected by checking the following:

### Verifying that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-top.

### Verifying that CableCARD Modules Downloaded Software

- Verify that each host can display all authorized services.

### Verifying that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-top.

### Verify that Test Devices Downloaded Software

Verify that the test devices operate as expected by checking the following:

### Verifying that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-top.

### Verifying that CableCARD Modules Downloaded Software

- Verify that each host can display all authorized services.

### Download Client Software to Devices

The instructions in this section provide the steps to prepare and download the application platform software release to devices using the CVT method.

**Note:** This procedure is for downloading client software to your entire population of devices (set-tops and CableCARD modules). If you need the procedure to download only to a specific CVT group, follow the procedure in Download Images to CVT Test Groups.

### Examples of File Names and Version Numbers

The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

### Downloading Client Software to All Devices

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs/doctor** and press **Enter**.
3. Type **doctor -q** and press **Enter**.
4. Are all of the QAMs active in the network?
   - If **yes**, go to step 5.
   - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from a non-responding QAM. This may cause the device to download incorrect software.

5. On the DNCS Administrative Console, select the **DNCS** tab and then select the **Home Element**

**Provisioning** tab.

6. Click **Image**. The Image List window opens.

7. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.

8. In the **DHCT Type** column, select the device type that will receive the new software where the value in the Group column is labeled Default.

9. Click **File > Delete**.

10. Repeat steps 8 and 9 for each device type that is receiving new software.

11. In an xterm window on the DNCS, type **listCVT** and press **Enter**. The listCVT report displays. Look for unused files in the report.

12. On the Image List window, select the **Downloadable Files** tab and compare the list of files displayed with the list of unused files listed in the listCVT report.

13. Select any unused file on the Downloadable Files tab.

14. Click **File > Delete**.

**Note:** The DNCS will not allow you to delete a file that is already associated with a download.

15. Repeat steps 13 and 14 until you have deleted all unused files.

16. On the Image List window, select the **DHCT Downloads** tab.

17. Click **File > New**. The Set Up DHCT Download window opens.

18. Complete the following steps to configure the Set Up DHCT Download window for the test download.

    - Click the **DHCT Type** arrow and select a device that needs to receive the new software.
    - Click the **Group** arrow and select **Default**.
    - Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

      **Note:** Unless you have old files or test versions still posted, there should be only one choice.

    - Click the **Download Scheduling** arrow and select one of the following, based on the device type:
      - **DHCTs:** Select either **Normal** or **Immediate**. A Normal download does not begin until the DHCT is turned off.
      - **CableCARD modules**: Select **Immediate**.

19. Click **Save**. The Association Verification window opens.

20. Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.

21. Configure the following fields on the Association Verification window:

    - **Are you SURE you want to do this?:** Type **yes**.
    - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
    - **Password:** Type the password you received from Cisco Services.

22. Click **OK**. The system schedules the software download according to the schedule you configured earlier in this section.

23. Repeat steps 17 through 22 for each device type that you want to receive the software using the CVT method.

24. In an xterm window on the DNCS, type **cd /export/home/dncs/doctor** and press **Enter**.

25. Type **doctor -q** and press **Enter**.

26. Are all of the QAMs still active in the network?

    - If **yes**, you are finished with this procedure.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, contact Cisco Services.

### Examples of File Names and Version Numbers

The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

### Download Client Software to Devices

The instructions in this section provide the steps to prepare and download the application platform software release to devices using the CVT method.

**Note:** This procedure is for downloading client software to your entire population of devices (set-tops and CableCARD modules). If you need the procedure to download only to a specific CVT group, follow the procedure in Download Images to CVT Test Groups.

### Examples of File Names and Version Numbers

The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

### Downloading Client Software to All Devices

1. Open an xterm window on the DNCS.
1. Type **cd /export/home/dncs/doctor** and press **Enter**.
1. Type **doctor -q** and press **Enter**.
1. Are all of the QAMs active in the network?
    - If **yes**, go to step 5.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

**Example:** The following is an example list of network elements that has a non-responding QAM.

```
OK: QAM BCASTQAM1 172.16.4.201 is alive.

OK: QAM BCASTQAM1 172.16.4.201 RPC working.

Error: QAM VODMBQAM1 172.16.4.210 is not pingable.

OK: QAM BCASTQAM2 172.16.4.202 is alive.

OK: QAM BCASTQAM2 172.16.4.202 RPC working.

OK: QAM BCASTQAM3 172.16.4.203 is alive.

OK: QAM BCASTQAM3 172.16.4.203 RPC working.

OK: QAM VODMQAM2 172.16.4.212 is alive.

OK: QAM VODMQAM2 172.16.4.212 RPC working.

OK: BIG CVLab 172.16.4.101 is alive.

OK: TED dncsted 192.168.1.2 is alive.
```

**Important:** Non-responding QAMs may have an old CVT table retained in memory. If non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from a non-responding QAM. This may cause the device to download incorrect software.

1. On the DNCS Administrative Console, select the **DNCS** tab and then select the **Home Element**

**Provisioning** tab.

1.Click **Image**. The Image List window opens.

1.On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.

1.In the **DHCT Type** column, select the device type that will receive the new software where the value in the Group column is labeled Default.

1.Click **File > Delete**.

1.Repeat steps 8 and 9 for each device type that is receiving new software.

1.In an xterm window on the DNCS, type **listCVT** and press **Enter**. The listCVT report displays. Look for unused files in the report.

1.On the Image List window, select the **Downloadable Files** tab and compare the list of files displayed with the list of unused files listed in the listCVT report.

1.Select any unused file on the Downloadable Files tab.

1.Click **File > Delete**.

**Note:** The DNCS will not allow you to delete a file that is already associated with a download.

1.Repeat steps 13 and 14 until you have deleted all unused files.

1.On the Image List window, select the **DHCT Downloads** tab.

1.Click **File > New**. The Set Up DHCT Download window opens.

1.Complete the following steps to configure the Set Up DHCT Download window for the test download.

- Click the **DHCT Type** arrow and select a device that needs to receive the new software.
- Click the **Group** arrow and select **Default**.
- Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

  **Note:** Unless you have old files or test versions still posted, there should be only one choice.

- Click the **Download Scheduling** arrow and select one of the following, based on the device type:
  - **DHCTs:** Select either **Normal** or **Immediate**. A Normal download does not begin until the DHCT is turned off.
  - **CableCARD modules**: Select **Immediate**.

1.Click **Save**. The Association Verification window opens.

1.Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.

1.Configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?:** Type **yes**.
- **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password:** Type the password you received from Cisco Services.

1.Click **OK**. The system schedules the software download according to the schedule you configured earlier in this section.

1.Repeat steps 17 through 22 for each device type that you want to receive the software using the CVT method.

1. In an xterm window on the DNCS, type **cd /export/home/dncs/doctor** and press **Enter**.
1. Type **doctor -q** and press **Enter**.
1. Are all of the QAMs still active in the network?
    - If **yes**, you are finished with this procedure.
    - If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, contact Cisco Services.

## Maintain CRL

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Maintain CRL**

The Maintain CRL window allows you to keep track of host devices that CableLabs has placed on its Certification Revocation List (CRL). Hosts listed on the CRL are devices that CableLabs considers to be compromised or untrustworthy. These host devices should be unbound from their CableCARD modules so that they are no longer able to decrypt copy-protected content.

Whenever CableLabs sends you a CRL, enter the hosts listed on the CableLabs CRL in the Maintain CRL window. By adding hosts to the Maintain CRL window, you keep a comprehensive list of all host devices CableLabs has identified should have their ability to decrypt copy-protected content copy-protected content revoked.

**Important:** In order to ensure that the CRL host devices cannot decrypt copy-protected content, you must unbind any CableCARD modules that are bound to these CRL hosts. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. In addition, all services should be removed from the module. To view list of CableCARD modules that are bound with CRL hosts, select **CableCARDs with CRL Hosts** in the upper left portion of the Maintain CRL window.

## What do you want to do?

- Add a Host Device to the Maintain CRL Window
- Remove a Host Device From the Maintain CRL Window
- View CableCARDs with CRL Hosts
- Remove Conditional Access Services from CableCARD and M-CARD Modules

### Add a Host Device to the Maintain CRL Window

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Maintain CRL > Add New CRL Item**

This topic describes how to add to the Maintain CRL window the host devices that CableLabs has placed on its Certification Revocation List (CRL). CableLabs publishes the CRL periodically to notify you of devices with digital certificates that are no longer trustworthy. These host devices should have their ability to decrypt copy-protected content revoked.

Whenever CableLabs sends you a new CRL, you should add the host devices listed in the CRL to the Maintain CRL window. Adding the devices to this window ensures that you have a comprehensive list of all host devices that CableLabs has identified as having untrustworthy digital certificates. On the other hand, should CableLabs notify you that devices have been removed from the CRL, you should remove these devices from the Maintain CRL window.

**Note:** In order to ensure that the devices listed in the Maintain CRL window cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host. To determine if a CableCARD module is bound to a host, see View CableCARD Module/Host Pairs on the CRL.

#### You Need to Know

Before You Begin

Before you begin, you must have the ID of the host device that you want to add to the Maintain CRL window.

#### Adding a Host Device to the Maintain CRL Window

Complete these steps to add a host device listed in the CableLabs CRL to the Maintain CRL window.

1. Is the Maintain CRL window open?
   - If **yes**, go to step 6
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Home Element Provisioning** tab.
4. Click **CableCARD**. The CableCARD Data Summary window opens.
5. Click **Maintain CRL**. The Maintain CRL window opens.
6. Click **Add**. A field containing a dummy ID appears in the Host ID table
7. Click in the empty and type the ID of the host device you want to add to the Maintain CRL window.
8. Click **Save**. The ID is added to the Host ID table and the message "CRL Item Saved Successfully" appears in the status area of the window.
9. Do you need to add another host device to the Maintain CRL window?
   - If **yes**, repeat step 6 and 7.
   - If **no**, make certain to unbind all hosts/module pairs so that the host devices you have added to the Maintain CRL window are no longer authorized to receive copy-protected content. To determine if a CableCARD module is bound to a host, go to View CableCARD Module/Host Pairs

on the CRL.

**Important:** In order to ensure that the devices listed in the Maintain CRL window cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.

10. Click **Cancel** to return to the CableCARD Summary window. Or click **File > Close** to return to the DNCS Administrative Console.

### Add a Host Device to the Maintain CRL Window

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Maintain CRL > Add New CRL Item**

This topic describes how to add to the Maintain CRL window the host devices that CableLabs has placed on its Certification Revocation List (CRL). CableLabs publishes the CRL periodically to notify you of devices with digital certificates that are no longer trustworthy. These host devices should have their ability to decrypt copy-protected content revoked.

Whenever CableLabs sends you a new CRL, you should add the host devices listed in the CRL to the Maintain CRL window. Adding the devices to this window ensures that you have a comprehensive list of all host devices that CableLabs has identified as having untrustworthy digital certificates. On the other hand, should CableLabs notify you that devices have been removed from the CRL, you should remove these devices from the Maintain CRL window.

**Note:** In order to ensure that the devices listed in the Maintain CRL window cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host. To determine if a CableCARD module is bound to a host, see View CableCARD Module/Host Pairs on the CRL.

#### You Need to Know

Before You Begin

Before you begin, you must have the ID of the host device that you want to add to the Maintain CRL window.

#### Adding a Host Device to the Maintain CRL Window

Complete these steps to add a host device listed in the CableLabs CRL to the Maintain CRL window.

1. Is the Maintain CRL window open?
   - If **yes**, go to step 6
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Home Element Provisioning** tab.
4. Click **CableCARD**. The CableCARD Data Summary window opens.
5. Click **Maintain CRL**. The Maintain CRL window opens.
6. Click **Add**. A field containing a dummy ID appears in the Host ID table
7. Click in the empty and type the ID of the host device you want to add to the Maintain CRL window.
8. Click **Save**. The ID is added to the Host ID table and the message "CRL Item Saved Successfully" appears in the status area of the window.
9. Do you need to add another host device to the Maintain CRL window?
   - If **yes**, repeat step 6 and 7.
   - If **no**, make certain to unbind all hosts/module pairs so that the host devices you have added to the Maintain CRL window are no longer authorized to receive copy-protected content. To determine if a CableCARD module is bound to a host, go to View CableCARD Module/Host Pairs

on the CRL.

**Important:** In order to ensure that the devices listed in the Maintain CRL window cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.

10. Click **Cancel** to return to the CableCARD Summary window. Or click **File > Close** to return to the DNCS Administrative Console.

### Remove a Host Device From the Maintain CRL Window

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Maintain CRL > [Select Revoked Host] > Delete**

If you have inadvertently placed a host device on the CRL or if a host device is removed from the CableLabs CRL list, then you can remove the host from the Maintain CRL window. This topic describes how to remove a device from the Maintain CRL window.

Hosts listed in the Maintain CRL window should not be bound to any CableCARD modules.

### You Need to Know

Before You Begin

Before you can remove a host device from the Maintain CRL window, you must know the ID for that host.

To determine if a CableCARD module is associated to a host, go to View CableCARD Module/Host Pairs on the CRL.

**Note:** Removing a host from the CRL does not cause a CableCARD module/host pair's binding status to change. Any hosts that are removed from the CRL and unbound from a CableCARD module can only be re-bound by changing the CableCARD module's Host Bound status to "Yes" in the Edit CableCARD window or by sending a billing transaction to bind the module and host.

### Removing a Host Device from the CRL

Complete these steps to remove a host device from the Maintain CRL window.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **Maintain CRL**. The Maintain CRL window opens.
5. Select the boxes next to the host devices that you want to remove from the Maintain CRL window.
6. Click **Delete**. A confirmation window opens asking if you are sure you want to delete the selected items.
7. Click **OK** to confirm your decision. The confirmation window closes and the list updates so that the host devices are no longer listed. The message "CRL Item Deleted Successfully" appears in the status area of the window.

   **Note:** Removing a host from the CRL does not cause a CableCARD module/host pair's binding status to change. Any hosts that are removed from the CRL and unbound from a CableCARD module can only be re-bound by changing the CableCARD module's Host Bound status to "Yes" in the Edit CableCARD window or by sending a billing transaction to bind the module and host. To determine if a CableCARD module is associated to a host, go to View CableCARD Module/Host Pairs on the CRL.

8. To return to the CableCARD Summary window, click **CableCARD Summary**. To return to the DNCS Administrative Console, click **File > Close**.

### Remove a Host Device From the Maintain CRL Window

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Maintain CRL > [Select Revoked Host] > Delete**

If you have inadvertently placed a host device on the CRL or if a host device is removed from the CableLabs CRL list, then you can remove the host from the Maintain CRL window. This topic describes how to remove a device from the Maintain CRL window.

Hosts listed in the Maintain CRL window should not be bound to any CableCARD modules.

#### You Need to Know

Before You Begin

Before you can remove a host device from the Maintain CRL window, you must know the ID for that host.

To determine if a CableCARD module is associated to a host, go to View CableCARD Module/Host Pairs on the CRL.

**Note:** Removing a host from the CRL does not cause a CableCARD module/host pair's binding status to change. Any hosts that are removed from the CRL and unbound from a CableCARD module can only be re-bound by changing the CableCARD module's Host Bound status to "Yes" in the Edit CableCARD window or by sending a billing transaction to bind the module and host.

#### Removing a Host Device from the CRL

Complete these steps to remove a host device from the Maintain CRL window.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **Maintain CRL**. The Maintain CRL window opens.
5. Select the boxes next to the host devices that you want to remove from the Maintain CRL window.
6. Click **Delete**. A confirmation window opens asking if you are sure you want to delete the selected items.
7. Click **OK** to confirm your decision. The confirmation window closes and the list updates so that the host devices are no longer listed. The message "CRL Item Deleted Successfully" appears in the status area of the window.

   **Note:** Removing a host from the CRL does not cause a CableCARD module/host pair's binding status to change. Any hosts that are removed from the CRL and unbound from a CableCARD module can only be re-bound by changing the CableCARD module's Host Bound status to "Yes" in the Edit CableCARD window or by sending a billing transaction to bind the module and host. To determine if a CableCARD module is associated to a host, go to View CableCARD Module/Host Pairs on the CRL.

8. To return to the CableCARD Summary window, click **CableCARD Summary**. To return to the DNCS Administrative Console, click **File > Close**.

### View CableCARDs with CRL Hosts

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > Maintain CRL > CableCARDs with CRL Hosts**

Use this procedure to determine which CableCARD modules, if any, are associated (or paired) with the host devices that are listed in the Maintain CRL window.

If any hosts in the Maintain CRL window are bound to CableCARD modules, then these CableCARD module/host pairs should be unbound or deauthorized in order to prevent them from receiving copy-protected content. In addition, conditional access services should be removed from these CableCARD modules. For assistance removing services from modules, see Remove Conditional Access Services from CableCARD or M-Card Modules.

**Note:** A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.

Complete these steps to view a list of CableCARD modules that are bound with hosts in the Maintain CRL window.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **Maintain CRL**. The Maintain CRL window opens.
5. Click **CableCARDs with CRL Hosts**. The CableCARDs with CRL Hosts window opens and lists any CableCARD modules that are associated with CRL hosts.
6. Are any CableCARD modules listed in the CableCARDs with CRL Hosts window?
   - If **no**, this indicates that no CableCARD modules are associated (or paired) with a CRL host. As a result, the host device is unable to decrypt copy-protected content. Go to step 8.
   - If **yes**, this indicates that a CRL host is bound to the modules listed in the window. As a result, the host is able to decrypt copy-protected content. Unbind the host and modules so that the host is unable to decrypt copy-protected content. In addition, these CableCARD modules should be removed from any services. For assistance removing services from modules, see Remove Conditional Access Services from CableCARD or M-Card Modules.

     **Note:** A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.
7. To return to the CableCARD Summary window, click **CableCARD Summary**. To return to the DNCS Administrative Console, click **File > Close**.

### Remove Conditional Access Services from CableCARD and M-CARD Modules

When CableCARD or M-CARD modules are taken out of service, you only need to remove the conditional access to deauthorize the services on the CableCARD or M-CARD modules. These services may be reactivated when the CableCARD or M-CARD module is returned to service. You can remove the conditional access using the billing system or the DNCS as described in the following procedure.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Select the **By MAC Address** option and type the MAC Address of the CableCARD or M-CARD module.
5. Click **Continue**. The Set Up DHCT window opens. A CableCARD or M-CARD entry appears in the DHCT Type box.
6. Click the **Secure Services** tab. The Secure Services tab moves to the forefront.
7. In the **Packages** area, select the first package in the Selected list. Scroll to the bottom of the list, hold down the Shift key, and select the last package in the list to highlight all of the packages in the list.
8. Click **Remove**. All of the packages move to the Available list.
9. In the **Options** area, select the options that are required by your internal procedures.
10. Click **Save**. Your changes are saved and all package authorizations are removed from the CableCARD or M-CARD module.
11. Click **Close**. The Set Up DHCT window closes.

### Related Topics

- Manage CableCARD Modules and Hosts
- PowerKEY CableCARD Modules

## CableCARD MMI Copy Protection Screen

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

This Configure MMI Screen Data window allows you to make the following changes to the MMI Copy Protection (CP) screen that CableCARD hosts display to subscribers:

- Customize the default message that the CableCARD host displays to prompt subscribers to telephone for CableCARD authorization
- Configure the MMI CP screen to display information that is useful in verifying correct CableCARD installation
- Define the conditions under which the CableCARD host displays the MMI CP screen

## What do you want to do?

- Learn about the Configure MMI Screen Data Settings
- View a MMI Copy Protection Sample
- Display the settings for the MMI CP screen
- Configure the CableCARD MMI Screen
- Learn about Previewing the MMI CP Screen
- Authorize a Set-Top or CableCARD Module for a Service
- Identify Error-Handling Conditions
- Click **Reset to Defaults** to return the values for the Set CableCARD MMI Copy Protection window to default values

### Configure MMI Screen Data Settings

Use the following fields when you manage the MMI screen in the DNCS.

| Field | Description |
|---|---|
| **MMI Options** | |
| Display MMI for bi-directional device | Determines whether or not two-way CableCARD hosts display the MMI CP screen:<br>▪**Disabled (no checkmark displayed - DEFAULT)** - Two-way CableCARD hosts never display the MMI CP screen. (To turn **autobinding on**, make sure that **no checkmark** is displayed.)<br>▪**Enabled (checkmark displayed)** - Two-way CableCARD hosts display the MMI CP screen according to the Bidirectional timeout value. (To turn **autobinding off**, make sure that the **checkmark is** displayed.) |
| Bidirectional timeout (decimal seconds) | Defines how long two-way CableCARD hosts wait to display the CP MMI screen.<br>▪To turn **autobinding on**, set this to **180** seconds (3 minutes).<br>▪To turn **autobinding off**, set this to **0**.<br>Enter a value that defines how long two-way CableCARD hosts wait to display the CP MMI screen after the host determines that it cannot connect to the DNCS or receive a response from the DNCS.<br>The **default setting (0)** indicates that the host should display the MMI CP immediately after it determines that it cannot connect to the DNCS or did not receive a response from the DNCS.<br>Valid characters for this field are numerical characters in the range of 0 to 65535. |
| Network failure operation -- Display CP MMI | Defines the criterion that two-way CableCARD hosts use to determine when to display the MMI CP screen:<br>▪**Disabled (DEFAULT)** - The host always uses the Bidirectional timeout to determine when to display the MMI CP screen<br>▪**Enabled** - The host displays the MMI CP screen if no network boot occurs. |
| **Choose Fields** | |
| Line | Defines the line number on the MMI CP screen where this field appears. Enter a line number based on the following criteria:<br>▪The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen.<br>▪Options for this field are the numbers 0 to 16.<br>▪Selecting 0 indicates that the field is not to be displayed in the MMI CP screen. |
| Field | Lists the fields that can be displayed in the MMI CP screen.<br>The values for these fields are obtained from the data in the CableCARD Data Summary window. |
| Display Label<br>**Important:** The maximum number of | Defines the label that displays in the MMI CP screen for the following fields. (Because each line is limited to 32 characters, the display label must take into account the number of characters required for both the display label and the field value. In cases where the field value requires many characters, you may |

characters that can be entered for any of these fields must take into account the number of characters required for both the display label and the field value.

Taking the characters for the field's value into account is necessary because a single line on the MMI CP screen can contain a maximum of 32 characters, including the field

label field value, and any blank spaces.

For example, if you assign the label "Host ID:" to the Host Copy Protection ID field,

and the field has a value of "0-100-331-784-015, " the total number of characters

used is 25.

need to shorten the display label. For example, you might configure the MMI CP screen to use the display label "Host MAC:" for the Host MAC Address field.)

| | |
|---|---|
| **Host MAC Address** - Displays the MAC address of the host | Enter the MAC address of the host, based on the following criteria:<br>▪A maximum of 15 characters can be entered for this display label<br>▪The address itself requires 17 characters<br>▪The default label is **Host MAC:** |
| **Host Copy Protection ID** - Displays the copy protection ID of the host | Enter the copy protection ID of the host, based on the following criteria:<br>▪A maximum of 15 characters can be entered for this display label<br>▪The ID itself requires 17 characters<br>▪The default label is **Host ID:** |
| **Cable Modem MAC Address** - Displays the MAC address of the cable modem | Enter the MAC address of the cable modem, based on the following criteria:<br>▪A maximum of 15 characters can be entered for this display label<br>▪The address itself requires 17 characters<br>▪The default label is **CM MAC:** |
| **CableCARD Copy Protection ID** - Displays the copy protection ID of the CableCARD module | Enter the copy protection ID of the CableCARD module, based on the following criteria:<br>▪A maximum of 15 characters can be entered for this display label<br>▪The ID itself requires 17 characters<br>▪The default label is **CableCARD ID:** |
| **Host Direction** - Displays the direction of the host | Enter the host direction, based on the following criteria:<br>▪A maximum of 32 characters can be entered for both the Display Label and the corresponding Text.<br>▪The default label is **Type:** |
| **Host Attributes** - Displays attributes of the host | Enter the host attributes, based on the following criteria:<br>A maximum of 32 characters can be entered for both the Display Label and the corresponding Text.<br>The default label is **Host Code:**. |

Available Options

Defines the types of hosts (one-way or two-way) that display the following fields in the MMI CP screen.

| | |
|---|---|
| **Host MAC Address** | Select one of the following options, based on the directionality of the host:<br>▪**One-Way Host** |

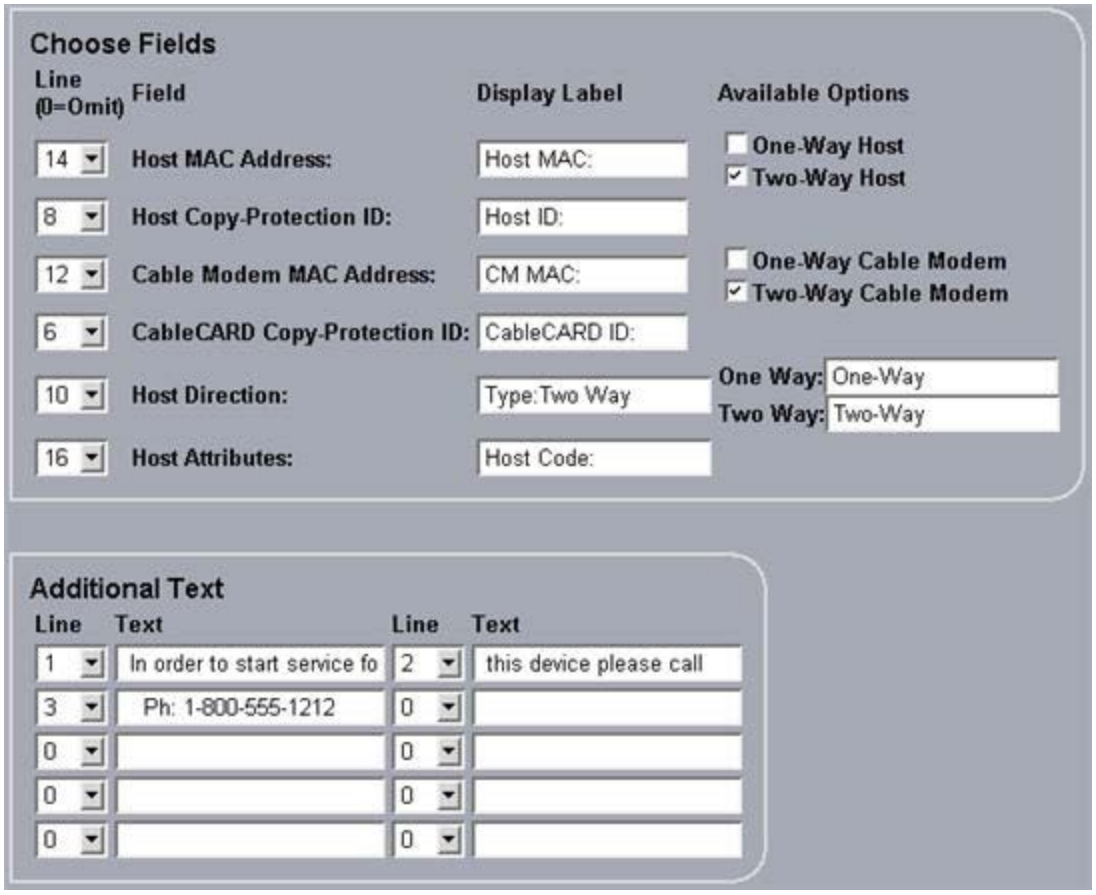
| | | |
|---|---|---|
| | | ▪**Two-Way Host** |
| | **Cable Modem MAC Address** | Select one of the following options, based on the directionality of the cable modem:<br>▪**One-Way Cable Modem**<br>▪**Two-way Cable Modem** |
| | **One-way -** Defines the values that appear in the Host Direction field for one-way hosts. | You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **One-Way**. |
| | **Two-way -** Defines the values that appear in the Host Direction field for two-way hosts. | You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **Two-Way**. |
| Text | Defines the values that appear in the Host Direction field for one-way and two-way hosts. | |
| Additional text -- indicate line number Fields | Settings in the following fields allow you to define custom text to be displayed in the MMI CP screen. | |
| | **Line** - Determines where on the MMI CP screen the custom text appears | Enter the line number on the MMI CP screen where custom text appears, based on the following criteria:<br>▪Options for this field are the numbers 0 to 16.<br>▪Selecting 0 indicates that no custom text is to be displayed in the MMI CP screen.<br>▪To display a blank line, assign a line number to a text field, but leave the text field empty.<br>**Note:** The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen. |
| | **Text** - Determines the custom text | Enter the custom text to be displayed in the MMI CP screen for the selected line number.<br>**Note:** Each line can contain a maximum of 32 characters, including marks of punctuation and blank spaces. For example, to display "In order to start service for this device, please call 1-800-555-1212." in the MMI CP screen, you would need to break the text up into a minimum of three lines because there are 70 characters in this sentence. |
| Default Values | The default values for lines 1 to 3:<br>▪Line 1 - The default value is **In order to start service for**.<br>▪Line 2 - The default value is **this device please call**.<br>▪Line 3 - The default value is taken from the **Card Authorization Phone Number** value on the Configure CableCARD Server window. | |

### MMI Copy Protection Sample

The following example shows how MMI CP information might appear on the screen of a host device, such as a TV. The actual text that is displayed depends upon how you have configured the settings in the Set CableCARD MMI Copy Protection window.

**Important:** When configuring settings for the MMI CP screen, keep in mind that MMI CP information is limited to 16 lines, including any blank lines. The lines are numbered in order from 1 to 16, starting at the top of the screen. Each line can contain a maximum of 32 characters, including marks of punctuation and blank spaces. All 16 lines are used in this example.


To configure the MMI CP screen to display as shown in the above example, the following options were set as indicated:


Choose Fields
Line (0=Omit)
Field
Display Label
Available Options
14
Host MAC Address:
Host MAC:
One-Way Host
Two-Way Host
8
Host Copy-Protection ID:
Host ID:
12
Cable Modem MAC Address:
CM MAC:
One-Way Cable Modem
Two-Way Cable Modem
6
CableCARD Copy-Protection ID:
CableCARD ID:
10
Host Direction:
Type:Two Way
One Way:
One-Way
Two Way:
Two-Way
16
Host Attributes:
Host Code:
Additional Text
Line
Text
Line
Text
1
In order to start service fo
2
this device please call
3
Ph: 1-800-555-1212
0
0
0
0
0
0
0
0

### Display the Configure MMI Screen Data Window

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > System Provisioning tab > CableCARD > MMI Screen Format**

This topic describes how to display the Configure MMI Screen Data window so that you can view the settings and determine if they meet the needs of your system.

Complete the following steps to display the Configure MMI Screen Data window.

1. Is the CableCARD Summary window open?
   - If **yes**, go to step 5.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Home Element Provisioning** tab.
4. Click **CableCARD**. The CableCARD Summary window opens.
5. Click **MMI Screen Format**. The Configure MMI Screen Data window opens.
6. Do the settings in this window meet the needs of your system? (For a description of the settings in this window, go to Configure MMI Screen Data Settings.

Use the following fields when you manage the MMI screen in the DNCS.

| Field | Description |
|---|---|
| MMI Options | |
| Display MMI for bi-directional device | Determines whether or not two-way CableCARD hosts display the MMI CP screen:<br>▪**Disabled (no checkmark displayed - DEFAULT)** - Two-way CableCARD hosts never display the MMI CP screen. (To turn **autobinding on**, make sure that **no checkmark** is displayed.)<br>▪**Enabled (checkmark displayed)** - Two-way CableCARD hosts display the MMI CP screen according to the Bidirectional timeout value. (To turn **autobinding off**, make sure that the **checkmark is** displayed.) |
| Network failure operation -- Display CP MMI | Defines the criterion that two-way CableCARD hosts use to determine when to display the MMI CP screen:<br>▪**Disabled (DEFAULT)** - The host always uses the Bidirectional timeout to determine when to display the MMI CP screen<br>▪**Enabled** - The host displays the MMI CP screen if no network boot occurs. |
| Bidirectional timeout (decimal seconds) | Defines how long two-way CableCARD hosts wait to display the CP MMI screen.<br>▪To turn **autobinding on**, set this to **180** seconds (3 minutes).<br>▪To turn **autobinding off**, set this to **0**.<br>Enter a value that defines how long two-way CableCARD hosts wait to display the CP MMI screen after the host determines that it cannot connect to the DNCS or receive a response from the DNCS.<br>The **default setting (0)** indicates that the host should display the MMI |

| | |
|---|---|
| | CP immediately after it determines that it cannot connect to the DNCS or did not receive a response from the DNCS.<br><br>Valid characters for this field are numerical characters in the range of 0 to 65535. |

## Choose Fields

| | |
|---|---|
| Line | Defines the line number on the MMI CP screen where this field appears. Enter a line number based on the following criteria:<br><br>▪The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen.<br><br>▪Options for this field are the numbers 0 to 16.<br><br>▪Selecting 0 indicates that the field is not to be displayed in the MMI CP screen. |
| Field | Lists the fields that can be displayed in the MMI CP screen.<br><br>The values for these fields are obtained from the data in the CableCARD Data Summary window. |
| Display Label<br><br>**Important:** The maximum number of characters that can be entered for any of these fields must take into account the number of characters required for both the display label and the field value.<br><br>Taking the characters for the field's value into account is necessary because a single line on the MMI CP screen can contain a maximum of 32 characters, including the field<br><br>label field value, and any blank spaces.<br><br>For example, if you assign the label "Host ID:" to the Host Copy Protection ID field,<br><br>and the field has a value of "0-100-331-784-015, " the total number of characters<br><br>used is 25. | Defines the label that displays in the MMI CP screen for the following fields. (Because each line is limited to 32 characters, the display label must take into account the number of characters required for both the display label and the field value. In cases where the field value requires many characters, you may need to shorten the display label. For example, you might configure the MMI CP screen to use the display label "Host MAC:" for the Host MAC Address field.) |
| **Host MAC Address** - Displays the MAC address of the host | Enter the MAC address of the host, based on the following criteria:<br><br>▪A maximum of 15 characters can be entered for this display label<br><br>▪The address itself requires 17 characters<br><br>▪The default label is **Host MAC:** |
| **Host Copy Protection ID** - Displays the copy protection ID of the host | Enter the copy protection ID of the host, based on the following criteria:<br><br>▪A maximum of 15 characters can be entered for this display label<br><br>▪The ID itself requires 17 characters<br><br>▪The default label is **Host ID:** |
| **Cable Modem MAC Address** - Displays the MAC address of the cable modem | Enter the MAC address of the cable modem, based on the following criteria:<br><br>▪A maximum of 15 characters can be entered for this display label<br><br>▪The address itself requires 17 characters<br><br>▪The default label is **CM** |

| | | |
|---|---|---|
| | | **MAC:** |
| | **CableCARD Copy Protection ID** - Displays the copy protection ID of the CableCARD module | Enter the copy protection ID of the CableCARD module, based on the following criteria:<br>▪A maximum of 15 characters can be entered for this display label<br>▪The ID itself requires 17 characters<br>▪The default label is **CableCARD ID:** |
| | **Host Direction** - Displays the direction of the host | Enter the host direction, based on the following criteria:<br>▪A maximum of 32 characters can be entered for both the Display Label and the corresponding Text.<br>▪The default label is **Type:** |
| | **Host Attributes** - Displays attributes of the host | Enter the host attributes, based on the following criteria:<br>▪A maximum of 32 characters can be entered for both the Display Label and the corresponding Text.<br>▪The default label is **Host Code:**. |
| Available Options | Defines the types of hosts (one-way or two-way) that display the following fields in the MMI CP screen. | |
| | **Host MAC Address** | Select one of the following options, based on the directionality of the host:<br>▪**One-Way Host**<br>▪**Two-Way Host** |
| | **Cable Modem MAC Address** | Select one of the following options, based on the directionality of the cable modem:<br>▪**One-Way Cable Modem**<br>▪**Two-way Cable Modem** |
| | **One-way -** Defines the values that appear in the Host Direction field for one-way hosts. | You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **One-Way**. |
| | **Two-way -** Defines the values that appear in the Host Direction field for two-way hosts. | You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **Two-Way**. |
| Additional Text | Settings in the following fields allow you to define custom text to be displayed in the MMI CP screen. | |
| | **Line** - Determines where on the MMI CP screen the custom text appears | Enter the line number on the MMI CP screen where custom text appears, based on the following criteria: |

| | | |
|---|---|---|
| | | ▪Options for this field are the numbers 0 to 16.<br>▪Selecting 0 indicates that no custom text is to be displayed in the MMI CP screen.<br>▪To display a blank line, assign a line number to a text field, but leave the text field empty.<br>**Note:** The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen. |
| | **Text** - Determines the custom text | Enter the custom text to be displayed in the MMI CP screen for the selected line number.<br>**Note:** Each line can contain a maximum of 32 characters, including marks of punctuation and blank spaces. For example, to display "In order to start service for this device, please call 1-800-555-1212." in the MMI CP screen, you would need to break the text up into a minimum of three lines because there are 70 characters in this sentence. |
| Default Values | The default values for lines 1 to 3:<br>▪Line 1 - The default value is **In order to start service for**.<br>▪Line 2 - The default value is **this device please call**.<br>▪Line 3 - The default value is taken from the **Card Authorization Phone Number** value on the Configure CableCARD Server window. | |

▪If **yes**, click **File** and select **Close** to close the window.

▪If **no**, change the settings that you desire. For assistance, go to Configure the CableCARD MMI CP Screen.

## Related Topics

▪MMI Copy Protection Sample

▪Previewing the MMI CP Screen

### Configure the CableCARD MMI Screen

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

Complete these steps to replaces the default values on the CableCARD MMI CP screen with values appropriate to your site.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **MMI Screen Format**. The Configure MMI Screen Data window opens.
5. Complete the fields on the screen as described in Configure MMI Screen Data Settings.

Use the following fields when you manage the MMI screen in the DNCS.

| Field | Description |
|---|---|
| **MMI Options** | |
| Display MMI for bi-directional device | Determines whether or not two-way CableCARD hosts display the MMI CP screen:<br>▪ **Disabled (no checkmark displayed - DEFAULT)** - Two-way CableCARD hosts never display the MMI CP screen. (To turn **autobinding on**, make sure that **no checkmark** is displayed.)<br>▪ **Enabled (checkmark displayed)** - Two-way CableCARD hosts display the MMI CP screen according to the Bidirectional timeout value. (To turn **autobinding off**, make sure that the **checkmark is** displayed.) |
| Network failure operation -- Display CP MMI | Defines the criterion that two-way CableCARD hosts use to determine when to display the MMI CP screen:<br>▪ **Disabled (DEFAULT)** - The host always uses the Bidirectional timeout to determine when to display the MMI CP screen<br>▪ **Enabled** - The host displays the MMI CP screen if no network boot occurs. |
| Bidirectional timeout (decimal seconds) | Defines how long two-way CableCARD hosts wait to display the CP MMI screen.<br>▪ To turn **autobinding on**, set this to **180** seconds (3 minutes).<br>▪ To turn **autobinding off**, set this to **0**.<br>Enter a value that defines how long two-way CableCARD hosts wait to display the CP MMI screen after the host determines that it cannot connect to the DNCS or receive a response from the DNCS.<br>The **default setting (0)** indicates that the host should display the MMI CP immediately after it determines that it cannot connect to the DNCS or did not receive a response from the DNCS.<br>Valid characters for this field are numerical characters in the range of 0 to 65535. |
| **Choose Fields** | |

| | |
|---|---|
| Line | Defines the line number on the MMI CP screen where this field appears. Enter a line number based on the following criteria:<br>▪ The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen.<br>▪ Options for this field are the numbers 0 to 16.<br>▪ Selecting 0 indicates that the field is not to be displayed in the MMI CP screen. |
| Field | Lists the fields that can be displayed in the MMI CP screen.<br>The values for these fields are obtained from the data in the CableCARD Data Summary window. |
| Display Label<br>**Important:** The maximum number of characters that can be entered for any of these fields must take into account the number of characters required for both the display label and the field value.<br>Taking the characters for the field's value into account is necessary because a single line on the MMI CP screen can contain a maximum of 32 characters, including the field<br>label field value, and any blank spaces.<br>For example, if you assign the label "Host ID:" to the Host Copy Protection ID field,<br>and the field has a value of "0-100-331-784-015, " the total number of characters<br>used is 25. | Defines the label that displays in the MMI CP screen for the following fields. (Because each line is limited to 32 characters, the display label must take into account the number of characters required for both the display label and the field value. In cases where the field value requires many characters, you may need to shorten the display label. For example, you might configure the MMI CP screen to use the display label "Host MAC:" for the Host MAC Address field.) |
| **Host MAC Address** - Displays the MAC address of the host | Enter the MAC address of the host, based on the following criteria:<br>▪ A maximum of 15 characters can be entered for this display label<br>▪ The address itself requires 17 characters<br>▪ The default label is **Host MAC:** |
| **Host Copy Protection ID** - Displays the copy protection ID of the host | Enter the copy protection ID of the host, based on the following criteria:<br>▪ A maximum of 15 characters can be entered for this display label<br>▪ The ID itself requires 17 characters<br>▪ The default label is **Host ID:** |
| **Cable Modem MAC Address** - Displays the MAC address of the cable modem | Enter the MAC address of the cable modem, based on the following criteria:<br>▪ A maximum of 15 characters can be entered for this display label<br>▪ The address itself requires 17 characters<br>▪ The default label is **CM MAC:** |
| **CableCARD Copy Protection ID** - Displays the copy protection ID of the CableCARD module | Enter the copy protection ID of the CableCARD module, based on the following criteria:<br>▪ A maximum of 15 characters can be entered for this display label<br>▪ The ID itself requires 17 characters<br>▪ The default label is **CableCARD ID:** |

| | | |
|---|---|---|
| | **Host Direction** - Displays the direction of the host | Enter the host direction, based on the following criteria:<br>▪ A maximum of 32 characters can be entered for both the Display Label and the corresponding Text.<br>▪ The default label is **Type:** |
| | **Host Attributes** - Displays attributes of the host | Enter the host attributes, based on the following criteria:<br>▪ A maximum of 32 characters can be entered for both the Display Label and the corresponding Text.<br>▪ The default label is **Host Code:**. |
| Available Options | Defines the types of hosts (one-way or two-way) that display the following fields in the MMI CP screen. | |
| | **Host MAC Address** | Select one of the following options, based on the directionality of the host:<br>▪ **One-Way Host**<br>▪ **Two-Way Host** |
| | **Cable Modem MAC Address** | Select one of the following options, based on the directionality of the cable modem:<br>▪ **One-Way Cable Modem**<br>▪ **Two-way Cable Modem** |
| | **One-way -** Defines the values that appear in the Host Direction field for one-way hosts. | You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **One-Way**. |
| | **Two-way -** Defines the values that appear in the Host Direction field for two-way hosts. | You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **Two-Way**. |
| Additional Text | Settings in the following fields allow you to define custom text to be displayed in the MMI CP screen. | |
| | **Line** - Determines where on the MMI CP screen the custom text appears | Enter the line number on the MMI CP screen where custom text appears, based on the following criteria:<br>▪ Options for this field are the numbers 0 to 16.<br>▪ Selecting 0 indicates that no custom text is to be displayed in the MMI CP screen.<br>▪ To display a blank line, assign a line number to a text field, but leave the text field empty.<br>**Note:** The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen. |
| | **Text** - Determines the custom text | Enter the custom text to be displayed in the MMI CP screen for the selected line number.<br>**Note:** Each line can contain a maximum of 32 |

| | |
|---|---|
| | characters, including marks of punctuation and blank spaces. For example, to display "In order to start service for this device, please call 1-800-555-1212." in the MMI CP screen, you would need to break the text up into a minimum of three lines because there are 70 characters in this sentence. |
| Default Values | The default values for lines 1 to 3:<br>▪ Line 1 - The default value is **In order to start service for**.<br>▪ Line 2 - The default value is **this device please call**.<br>▪ Line 3 - The default value is taken from the **Card Authorization Phone Number** value on the Configure CableCARD Server window. |

6. To see how the MMI CP screen would display using your configuration, click **Preview**. The Sample MMI Copy Protection Data window opens and shows an example of the text that appears for each of the 16 lines in the MMI CP screen. To close this window, click **Close Preview**.

7. Are you are satisfied with appearance of the MMI CP screen?

▪ If **yes**, click **Save** to save your configuration. When a message box appears to let you know that the save was successful, click **OK** to close the message box. Once you save the changes you have made, the data is saved in the file /dvs/dvsFiles/CCardServer/CPDefinition.tbl and is put on the BFS Client under podServer/POD_Data/0/CPDefinition.tblo.

▪ If **no**, repeat steps 6 and 7 to change the settings and preview your changes.

8. To close the Configure MMI Screen Data window, click **File > Exit**.

## Related Topics

▪ MMI Copy Protection Sample

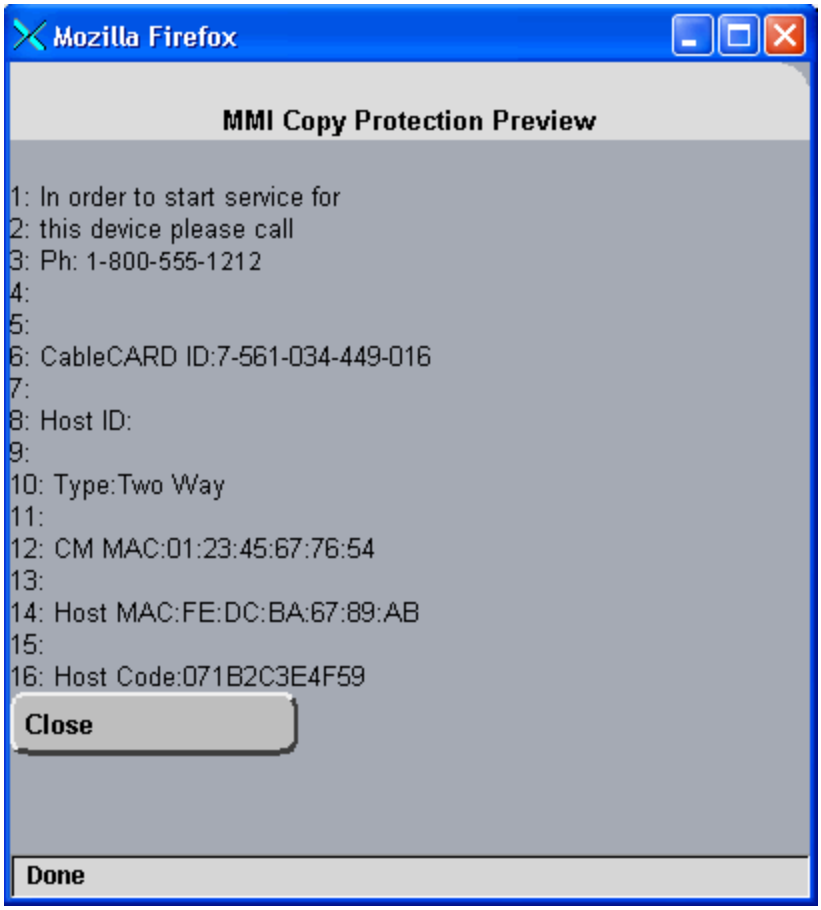
▪ Previewing the MMI CP Screen

### Previewing the MMI CP Screen

**Quick Path: DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > CableCARD > MMI Screen Format > Preview**

From the Set CableCARD MMI Copy Protection window, you can preview how the MMI CP screen appears on the screens of CableCARD hosts. Previewing the MMI CP screen is helpful when you are configuring the MMI CP screen and want to get an idea of how the screen appears to subscribers before you save the configuration. If you don't like what you see, you can make changes to the configuration and preview the screen again. When you are satisfied with the screen's appearance, save your configuration.

To preview the MMI CP screen, click **Preview** from the Configure MMI Screen Data window. The following shows an example of the preview screen.



## Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

### Authorizing a Set-Top or CableCARD Module for a Service

1. Make sure the test set-top is connected to a television, as well as to an RF feed into your network.
2. Make sure both the set-top and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the set-top or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected already when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the **Admin Status** field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the set-top or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each package.

- If your system uses a Brick mode package, the set-top or CableCARD module must be authorized for that package as well. This should have been done when the set-top or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the Selected field.

12. In the **Options** area, make the following selections as appropriate:

    - **IPPV Enable** - If this set-top or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
    - **DMS Enable** - Enable this option to allow the set-top or CableCARD module to receive secure services.
    - **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
    - **Analog Enable** - If this set-top needs to display secure analog services, enable this option.

      **Note:** Your system and the set-top must be designed to display secure analog services for this option to work properly. If necessary, refer to the Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see Printed Resources.

    - **Fast Refresh Enable** - This option is used to send EMMs to set-top or CableCARD modules during staging. For more information, refer to the Explorer Digital Home Communications Terminal Staging Guide (part number 734375).
    - **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this set-top or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service. Go to Verify a Successful Service Setup for more information.

## Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

### Authorizing a Set-Top or CableCARD Module for a Service

1. Make sure the test set-top is connected to a television, as well as to an RF feed into your network.
2. Make sure both the set-top and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the set-top or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected already when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the **Admin Status** field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the set-top or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each package.

- If your system uses a Brick mode package, the set-top or CableCARD module must be authorized for that package as well. This should have been done when the set-top or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the Selected field.

12. In the **Options** area, make the following selections as appropriate:

    - **IPPV Enable** - If this set-top or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
    - **DMS Enable** - Enable this option to allow the set-top or CableCARD module to receive secure services.
    - **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
    - **Analog Enable** - If this set-top needs to display secure analog services, enable this option.

      **Note:** Your system and the set-top must be designed to display secure analog services for this option to work properly. If necessary, refer to the Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see Printed Resources.

    - **Fast Refresh Enable** - This option is used to send EMMs to set-top or CableCARD modules during staging. For more information, refer to the Explorer Digital Home Communications Terminal Staging Guide (part number 734375).
    - **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this set-top or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service. Go to Verify a Successful Service Setup for more information.

## Identify Error-Handling Conditions

CableCARD module errors are set by the HOST-POD Interface Standard (ANSI-SCTE 28 2001), as written and approved by the Society of Cable Communications Engineers (SCTE). Please refer to the standards document located on the Internet for the most current error-handling conditions (http://www.scte.org/documents/pdf/ANSISCTE282004.pdf).

# Content Sources and Sessions

This section discusses defining sources and setting up sessions.

In the DBDS, a source is the actual program or data that is made available to the DHCT as a service to the subscriber. Sources can include: MPEG-2 digital broadcast services that are non-secure, non-encrypted, audio/video programs; Internet connections from an Internet service provider (ISP); Digital PPVs that are secure, encrypted, digital MPEG-2 programs; Digital music services; Analog programs that are modulated in the traditional format or converted into MPEG-2 format.

Sessions are the logical elements that define and allocate the resources that the network uses to deliver source content.

## What do you want to do?

- Add a content source
- Define a content source
- Define a third-party content source
- Add a partially encrypted session

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Define a Content Source

**Note:** These procedures do not apply to VOD services.

After you add a content source to the DNCS database for a clear, secure, or PPV service, define parameters for the source so that the system knows how to process the service content.

**Important:** If you are sending the same source through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same content source through six QAM modulators, you must define the source six times once for each modulator.

## Define an Analog Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Analog**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source in the DNCS. You do not need to define a source for a VOD service.

**Note:** You do not need to build a session for an analog source.

**Important:** If you are sending the same source content through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator.

### You Need to Know

Before You Begin

Before you define an **analog** service source, you must have the following information:

- Name of the source as you defined it when you added the content source
- If the service source is going to only one hub, name of that hub as defined in your network (refer to your network map)
- Number of the channel where the service will be displayed

**Important:** Before you set up a **secure analog service** in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

Time To Complete

Defining an analog source takes approximately 10 minutes to complete.

Performance Impact

Defining an analog source does not impact network performance. You can complete this procedure at any time.

### Analog Source Settings

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪**Default** - Distributes the source to all hubs.<br>▪**Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪**Now** - The service is available for viewing immediately.<br>▪**Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |

### Defining an Analog Source

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define.
5. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
6. Click **File > New Analog**. The Set Up Source Definition window opens.
7. Complete the fields on the screen as described in Analog Source Settings.

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪ **Default** - Distributes the source to all hubs.<br>▪ **Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪ **Now** - The service is available for viewing immediately.<br>▪ **Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source. |

You must type two digits for each value.

**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.

**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

This option is only activated if you select the **Custom** option in the Date/Time field.

8. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source Definition window. The Source Definition List window updates to include the new source information.

9. Do you need to define another analog source for this service?

- If **yes**, repeat this procedure from step 6.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

10. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

11. Click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 13.
- If **no**, your next step is to register the clear service. Go to Register a Service.

13. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

**Define a Digital Source and Session**

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Digital**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source. Then build a session from the source definition. You do not need to define a source and session for a VOD service.

**Important:**

- If you are sending the same source through more than one QAM, MQAM, GQAM, or GoQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator. This also applies to GQAM stat mux dejitter groups (SMDGs).
- If you are setting up a CF session as a **stat mux dejitter group (SMDG)** session, the session must use the same input port and output port that the SMDG uses. Otherwise, the session may fail. You can set up a maximum of 60 sessions on an SMDG. For assistance setting up an SMDG, see Setting Up Stat Mux Dejitter Groups.

**You Need to Know**

Before You Begin

Before you define a digital service source, you must have the following information:

- Name of the service source as you defined it when you added the content source
- Number of the channel where the service will be displayed
- Service source ID as you defined it when you added the content source
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)
- As part of defining a digital session, you will identify the bandwidth that the session requires and the QAM carrier that the session uses. When assigning sessions to a QAM carrier, use the following guidelines to ensure that the throughput is sized appropriately for the carrier.
  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

**Example:** Placing 10 video streams at 3.75 Mbps on a single QAM carrier would require 37.5 Mbps, plus an additional 0.375 Mbps (for overhead), resulting in a total of 37.875 Mbps bandwidth used. In this example, a 256-QAM modulator would have 0.936 Mbps of unused bandwidth on the QAM carrier, and no additional services could be placed on this carrier without resulting in a loss of quality.

Time To Complete

Defining a digital content source and building a session from the source definition takes approximately 20 minutes to complete.

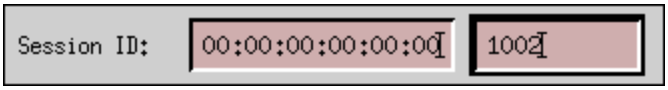
Performance Impact

Defining a digital content source and building a session from the source definition does not impact network

performance. You can complete this procedure at any time.

### Digital Source and Session Settings

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br><br>**Right Session ID field** - The source ID you used when you added the content source.<br><br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br><br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br><br>You must type two digits for the month and day, and four digits for the year.<br><br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br><br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br><br>You must type two digits for each value.<br><br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br><br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br><br>Select the **Broadcast programming** option because this source will provide broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br><br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.

| | | |
|---|---|---|
| | ▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. | |
| Wrap-up | See below for more information pertinent to the specific output device you selected. | |
| | ASI ports on a QAM, MQAM, or GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| | GbE ports on a GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 |

| | |
|---|---|
| | Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪**Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪**GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪**MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps |

for each QAM carrier.

○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

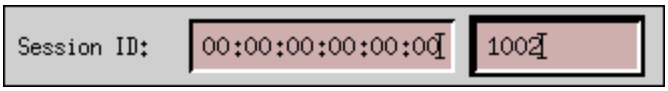
▪**Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.

▪**Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

### Defining a Digital Source and Session

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define and click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
5. Click **File > New Digital**. The Digital Source Set Up window opens.
6. Complete the fields on the screen as described in Digital Source and Session Settings.

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br>**Right Session ID field** - The source ID you used when you added the content source.<br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br>Select the **Broadcast programming** option because this source will provide |

| | |
|---|---|
| | broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
- Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
- For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

| | | |
|---|---|---|
| Wrap-up | See below for more information pertinent to the specific output device you selected. | |
| | ASI ports on a QAM, MQAM, or GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| | GbE ports on a GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program |

| | |
|---|---|
| | number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪ **Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪ **GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪ **MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪ **Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the |

UpConverter (if used).

- **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.

**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:

  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

- **Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.
- **Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

7. On the Save Source Definition window, click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

8. Do you need to define another digital source for this service?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

**Note:** You would define more than one digital service source if you have more than one MPEG source feeding the same content into different portions of your network.

9. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

10. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 11.
- If **no**, your next step is to register the clear service. Go to Register a Service.

11. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

## Define a Third-Party Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New non-SA Digital**

This procedure describes how to configure a system to carry clear (unencrypted) MPEG content that delivers unmodified Program and System Information Protocol (PSIP) in a bandwidth-efficient manner using a QAM configured on the DNCS as a third-party source. This configuration causes QAM frequencies to be included in the DHCT population's tuning table without the use of mirror QAMs.

If you are not using mirror QAM modulators to provide Program and System Information Protocol (PSIP) in the DHCT population's tuning table, define parameters for a third-party content source; otherwise, tuning information will not be included in the SI table for the sessions carried on clear QAM modulators.

**Note**: For more information refer to OBSOLETE

Program and System Information Protocol Configuration for System Releases 2.5, 3.5, and 4.0 (part number 4011319). To obtain a copy of this technical bulletin, go to Printed Resources.

## Before You Begin

Before you define a third-party content source, complete the following tasks:

- Contact Cisco Services to enable non-SA digital sources on the DNCS.
- If QAM modulators operate in a clear, pass-through mode, new QAM modulators must be configured using the front panel and through the serial port interface. In addition, you must add an entry into the /etc/bootptab file for each new QAM modulator that delivers clear MPEG content and aggregated PSIP. (If your system is already configure for PSIP, clear QAM modulators are already in the /etc/bootptab file.)

**Note**: For more information on the tasks listed above, refer to OBSOLETE

Program and System Information Protocol Configuration for System Releases 2.5, 3.5, and 4.0 (part number 4011319). To obtain a copy of this technical bulletin, go to Printed Resources.

- Also gather the following information:
  - Names of the hubs that will distribute the source.
  - MPEG program number for the content passed through the clear MQAM modulator (from your content provider)
  - Frequency of the channel being used to send data from the modulator to the hubs on your system
  - Modulation standard the modulator uses
  - Modulation method that the modulator uses

## Time To Complete

Defining a third-party service source takes approximately 10 minutes to complete.

## Performance Impact

If you need to tear down sessions on mirror QAM modulators, subscribers will not be able to view the service until you have completed this procedure.

### Third-Party Content Source Settings

Use the following fields when you manage a third-party content source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪**Default** - Distributes the source to all hubs.<br>▪**Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| MPEG Program Number | The MPEG program being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Channel Center Frequency | The channel frequency of the channel you will use to send data from this modulator to the hubs on your system.<br>You can enter a value in 6 MHz increments from 91 to 867.<br>Click for a table of recommended QAM frequencies. |
| Modulation Type | The type of modulation this modulator uses.<br>**Example:** If this modulator uses ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| Modulation | The modulation method this modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256-QAM**. |

### Defining a Third-Party Content Source

1. Is the Source List window open?
   - If **yes**, go to step 5.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **Source**. The Source List window opens.
5. Click once on the row containing the source you need to define.
6. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
7. Do you have existing source definitions?
   - If **yes**, in the Source Definition List window, locate and delete all previously configured source definitions for mirror QAM modulators.

     **Note**: When deleting these source definitions, you will be prompted to tear down the session associated with this source definition. Answer **Yes** to this prompt for each session you delete. This also tears down the session currently active on the mirror QAM modulator.

   - If **no**, go to step 8.
8. Read the following instruction before going to step 9:

**Important**: Before you create Source Definitions, determine how many source definitions you need. To determine this, identify how many unique configurations you have for carrying the services to the DHCTs in your system. If a service is configured with a unique frequency, MPEG number, or modulation scheme, it is a unique configuration. If any of these parameters are different, you must create a unique source definition.

**Example:** An off-air service is carried to most hubs by a single QAM modulator or by multiple QAM modulators at 573 MHz, but some hubs carry the service at 561 MHz. You will then create a source definition for 573 MHz and make it a default distribution. Then, for each hub that does not receive the service at 573 MHz, you will create a hub-specific source definition. In this example, at 561 MHz with "hub" distribution selected where the hub is the hub ID for any hub that carries the service at 561 MHz. This configuration parallels the configuration used for analog services that are carried at different frequencies in different parts of the system.

9. Click **File > New non-SA Digital**. The Set Up Non-SA Digital Source Definition window opens.
10. Complete the fields on the screen as described in Third-Party Content Source Settings.

Use the following fields when you manage a third-party content source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪ **Default** - Distributes the source to all hubs.<br>▪ **Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |

| | |
|---|---|
| MPEG Program Number | The MPEG program being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Channel Center Frequency | The channel frequency of the channel you will use to send data from this modulator to the hubs on your system.<br>You can enter a value in 6 MHz increments from 91 to 867.<br>Click for a table of recommended QAM frequencies. |
| Modulation Type | The type of modulation this modulator uses.<br>**Example:** If this modulator uses ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| Modulation | The modulation method this modulator uses.<br>**Example:** If this modulator uses 256 QAM, select **256-QAM**. |

11. Click **Save**. The system closes the Set Up Non-SA Digital Source Definition window and the Source Definition List window updates to include the new non SA source.

12. Repeat this procedure from step 5 for each QAM modulator from another manufacturer you are using to deliver broadcast services.

13. From the Source Definition List window, select **File > Close**.

14. From the Source List window, select **File > Close**.

15. Now that you have added source definitions for each QAM modulator from another manufacturer that you are using to deliver broadcast services, reboot the SI manager process to have these changes take effect. Go to Rebooting the SI Manager Process.

## Add a Partially Encrypted Session

**Important:** Follow this procedure only if your system uses Overlay technology and uses GoQAM modulators. Only GoQAM modulators produce partially encrypted sessions.

After you add a content source to the Source List, define the source and use it to build a partially encrypted session. A partially encrypted session can be delivered to DHCTs.

**Note:** Sessions define and allocate the resources that your network uses to deliver content. When you build a session, you identify the equipment where the content originates, such as an IRT. You also identify the GoQAM modulator that places the content onto the HFC network.

### You Need to Know

Before You Begin

Before you create a partially encrypted session, you must have the following information:

- Name and Source ID that you gave the source when you added the content source to the Source List
- Number of the channel where the service will be displayed
- MPEG program number from your content service provider
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)

Time To Complete

Building a partially encrypted session takes approximately 20 minutes to complete.

Performance Impact

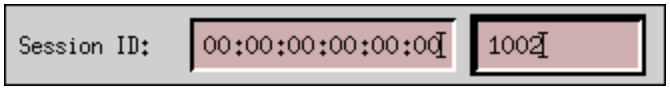
Building a partially encrypted session does not impact network performance. You can complete this procedure at any time.

### Related Topics

- Partially Encrypted Session Settings
- Adding a Partially Encrypted Session

### Partially Encrypted Session Settings

Use the following fields when you manage a partially encrypted session in the DNCS.

| Field | Description | |
|---|---|---|
| Session ID | **Left window** - The session MAC address. Type 12 zeros (the system inputs the colons for you). | |
| | **Right Session ID field** - The source ID you used when you added the content source. | |
| | Your final entry will look similar to the following example:<br>  | |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source. | |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year. **Example:** You would type July 4, 2007, as **07042007**. The system inputs the slashes for you and displays 07/04/2007.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. | |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** You would type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. | |
| Define Session | Define the session programming.<br>Select the **Broadcast** programming option because this source will provide broadcast (audio/video) programming rather than system information. | |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br>You defined the MPEG source when you set up your network. | |
| Select Outputs | The carrier that will receive content from this source. | |
| Wrap-up | **Input MPEG Program Number** | The MPEG program number of the clear stream that the GoQAM modulator receives. |
| | **Incumbent MPEG Program Number** | The MPEG program number of the non-SA encrypted stream that the GoQAM modulator receives. |
| | **Bandwidth** | The amount of bandwidth (in Mbps) that the system should allow for this service.<br>This value is usually defined by your content service provider. Requirements vary from |

| | |
|---|---|
| | system to system. |
| **Audio Encryption Percentage** | Leave the default value of **5** so that the modulator will use our encryption method to partially encrypt the audio portion of the clear stream. |
| **Video Encryption Percentage** | Leave the default value of **2** so that the modulator will use our encryption method to partially encrypt the video portion of the clear stream. |

### Adding a Partially Encrypted Session

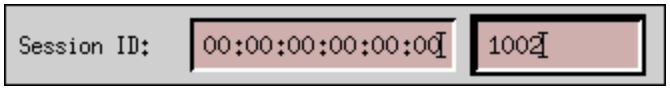
**Notes:**

- This procedure applies to systems that use Overlay technology and GoQAM modulators.
- If you are sending the same source content through more than one GoQAM modulator,you must define the source for each modulator.

**Example:** If you are sending the same source content through six GoQAM modulators, you must define the source six times once for each modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define.
5. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
6. Click **File > New Digital**. The Digital Source Set Up window opens.
7. Complete the fields on the screen as described in Partially Encrypted Session Settings. Be sure to click **Next** to move to the next screen in the sequence.

Use the following fields when you manage a partially encrypted session in the DNCS.

| Field | Description |
|---|---|
| Session ID | **Left window** - The session MAC address. Type 12 zeros (the system inputs the colons for you). |
| | **Right Session ID field** - The source ID you used when you added the content source. |
| | Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year. **Example:** You would type July 4, 2007, as **07042007**. The system inputs the slashes for you and displays 07/04/2007.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** You would type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. |

| | | |
|---|---|---|
| Define Session | Define the session programming.<br><br>Select the **Broadcast** programming option because this source will provide broadcast (audio/video) programming rather than system information. | |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br><br>You defined the MPEG source when you set up your network. | |
| Select Outputs | The carrier that will receive content from this source. | |
| Wrap-up | **Input MPEG Program Number** | The MPEG program number of the clear stream that the GoQAM modulator receives. |
| | **Incumbent MPEG Program Number** | The MPEG program number of the non-SA encrypted stream that the GoQAM modulator receives. |
| | **Bandwidth** | The amount of bandwidth (in Mbps) that the system should allow for this service.<br><br>This value is usually defined by your content service provider. Requirements vary from system to system. |
| | **Audio Encryption Percentage** | Leave the default value of **5** so that the modulator will use our encryption method to partially encrypt the audio portion of the clear stream. |
| | **Video Encryption Percentage** | Leave the default value of **2** so that the modulator will use our encryption method to partially encrypt the video portion of the clear stream. |

8. Click **Save** on the Save Source Definition window. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

9. Will other GoQAM modulators deliver this content to different portions of your network?

   - If **yes**, for each additional GoQAM modulator that carries this content, repeat this procedure from step 5 to build partially encrypted sessions on each modulator.
   - If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

10. Now that you have built a partially encrypted session, use this session to provide a secure or PPV service to subscribers:

    - To create a secure service from this partially encrypted session, go to step 4 of Setting Up Secure Services.
    - To create a PPV service from this partially encrypted session, go to step 4 of Setting Up PPV Services.

# Channel Maps and Channels

## Viewing Your Channel Plan

**Quick Path: DNCS Administrative Console > System Provisioning tab > DNCS System > Miscellaneous tab**

The DNCS supports three types of channel plans that are common to North America. When your system is upgraded or installed, the method that your DBDS uses is selected in the DNCS. When troubleshooting, you may want to verify the channel plan method your system uses, or confirm that this setting is correct in the DNCS.

Follow these steps to view the type of channel plan selected for your DBDS.

1. From the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **DNCS System**. The DNCS System Configuration window opens.
3. Click the **Miscellaneous** tab, and look for the setting that is selected for the Channel Plan option:
   - STD (Standard) channel plan
   - HRC (Harmonically Related Channel) plan
   - IRC (Incrementally Related Channel) plan
4. To close the DNCS System Configuration window without making any changes, click **Cancel**.

# Channel Maps and Channels

## Viewing Your Channel Plan

**Quick Path: DNCS Administrative Console > System Provisioning tab > DNCS System > Miscellaneous tab**

The DNCS supports three types of channel plans that are common to North America. When your system is upgraded or installed, the method that your DBDS uses is selected in the DNCS. When troubleshooting, you may want to verify the channel plan method your system uses, or confirm that this setting is correct in the DNCS.

Follow these steps to view the type of channel plan selected for your DBDS.

1. From the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **DNCS System**. The DNCS System Configuration window opens.
3. Click the **Miscellaneous** tab, and look for the setting that is selected for the Channel Plan option:
   - STD (Standard) channel plan
   - HRC (Harmonically Related Channel) plan
   - IRC (Incrementally Related Channel) plan
4. To close the DNCS System Configuration window without making any changes, click **Cancel**.

## Add a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > New**

The set of channels that subscribers can tune in through their DHCTs is called a "channel map." You must add a service to a channel map so that your subscribers can access it by tuning to a particular channel.

## Time To Complete

Adding a channel map takes approximately 15 minutes to complete.

## Performance Impact

Adding a channel map does not impact network performance. You can complete this procedure at any time.

### Adding a Channel Map

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click **File > New**. The Set Up Channel Map window opens.
4. Enter information as described in Channel Map Settings.

   Use the following fields when you manage channel maps in the ISDS.

| Field | Description |
|---|---|
| Name | Name of the channel map. You can use up to 20 alphanumeric characters. |
| VCT ID | Virtual channel table identifier. During set-top provisioning, each set-top is assigned a VCT ID. The set-top uses the VCT ID to retrieve its associated SI data among other sets of data that might be available on its hub. |
| Copy channel map from: | Copy an existing channel map.<br>Select the **Copy channel map from:** option.<br>Click the arrow to select the channel map you want to copy.<br>Click **Continue** to view and amend the channel setup for that channel map. |
| Channels | Assign services to channels.<br>Select a service in the Available Services column then click a Channel Slot.<br>Click **Add** to move that service to that Channel Slot. |

5. Click **Continue**. The Set Up Display Channel Map window opens.
6. Do you need to add a service to this channel map?
   - If **yes**, go to Add a Service to a Channel Map.
   - If **no**, click **Save**. The system saves the channel map information in the database, closes the Set Up Display Channel Map window, and returns you to the Display Channel Map List window.
7. Do you need to add another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

## Add a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > New**

The set of channels that subscribers can tune in through their DHCTs is called a "channel map." You must add a service to a channel map so that your subscribers can access it by tuning to a particular channel.

## Time To Complete

Adding a channel map takes approximately 15 minutes to complete.

## Performance Impact

Adding a channel map does not impact network performance. You can complete this procedure at any time.

### Adding a Channel Map

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click **File > New**. The Set Up Channel Map window opens.
4. Enter information as described in Channel Map Settings.

   Use the following fields when you manage channel maps in the ISDS.

| Field | Description |
|---|---|
| Name | Name of the channel map. You can use up to 20 alphanumeric characters. |
| VCT ID | Virtual channel table identifier. During set-top provisioning, each set-top is assigned a VCT ID. The set-top uses the VCT ID to retrieve its associated SI data among other sets of data that might be available on its hub. |
| Copy channel map from: | Copy an existing channel map.<br>Select the **Copy channel map from:** option.<br>Click the arrow to select the channel map you want to copy.<br>Click **Continue** to view and amend the channel setup for that channel map. |
| Channels | Assign services to channels.<br>Select a service in the Available Services column then click a Channel Slot.<br>Click **Add** to move that service to that Channel Slot. |

5. Click **Continue**. The Set Up Display Channel Map window opens.
6. Do you need to add a service to this channel map?
   - If **yes**, go to Add a Service to a Channel Map.
   - If **no**, click **Save**. The system saves the channel map information in the database, closes the Set Up Display Channel Map window, and returns you to the Display Channel Map List window.
7. Do you need to add another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

**Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?
   - If **yes**, go to Split a Channel.
   - If **no**, go to step 9.
9. Do you need to add another service to this channel map?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
10. Do you need to add a service to another channel map?
    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.
11. Do you need to include the service on your IPG?
    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.
12. Is this is a VOD service?
    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.
13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
1. Click **Channel Maps**. The Display Channel Map List window opens.
1. Click once on the row containing the channel map to which you want to add this service.

**Note:** If you select the Default channel map, this service will be available to all hubs.

1. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
1. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

1. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
1. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
1. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?
    - If **yes**, go to Split a Channel.
    - If **no**, go to step 9.
1. Do you need to add another service to this channel map?
    - If **yes**, repeat this procedure from step 5.
    - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
1. Do you need to add a service to another channel map?
    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.
1. Do you need to include the service on your IPG?
    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.
1. Is this is a VOD service?
    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.
1. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

# Delete a Service from a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > Delete**

When a service is no longer needed for a particular channel map, delete the service from the channel map.

### Time To Complete

Deleting a service from a channel map takes approximately 5 minutes to complete.

### Performance Impact

Deleting a service from a channel map does not impact network performance. You can complete this procedure at any time.

### Deleting a Service from a Channel Map

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select the service in channel slot.
6. Click **Remove**. The service is now listed under Available Services.
7. If you are removing this service from your system, your next step is to delete the service from the SAM.

## Delete a Service from a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > Delete**

When a service is no longer needed for a particular channel map, delete the service from the channel map.

### Time To Complete

Deleting a service from a channel map takes approximately 5 minutes to complete.

### Performance Impact

Deleting a service from a channel map does not impact network performance. You can complete this procedure at any time.

### Deleting a Service from a Channel Map

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select the service in channel slot.
6. Click **Remove**. The service is now listed under Available Services.
7. If you are removing this service from your system, your next step is to delete the service from the SAM.

## Split a Channel

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

If you need to use one channel to show one service during one period of the day and another service during the remainder of the day, you must split that channel so the system will know which service to implement and when.

## Before You Begin

Before you can set up a split channel, there must be at least two services listed in the **Available Services** field on the Set Up Display Channel Map window.

## Time To Complete

Splitting a channel takes approximately 20 minutes to complete, including the time it takes for the channel changes to appear on DHCTs.

## Performance Impact

Splitting a channel does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Splitting a Channel

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map that contains the channel you need to split.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. In the **Channel Slot** field, double-click on the channel you want to split. The Set Up Split Channel window opens.

**Important:** If a service is already assigned to the channel slot, a confirmation window will open to indicate that the service in that slot will be deleted if you continue. Make sure that you do not want to include that service as part of the split channel before you click **Yes** and continue.

6. Does the **Service A** field contain one of the services you want to include in this split channel?
   - If **yes**, go to step 7.
   - If **no**, click the **Service A** arrow and select the service that you want to appear first on this channel every day for seven days a week.
7. Click in the **Ends at** field to the right of the Service A field and type the exact time you want Service A to stop appearing on this channel. You must type two digits for each value.

**Example:** You would type six o'clock as **060000**. The system inputs the colons for you and displays 06:00:00.

**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

8. Click **AM/PM** to establish which portion of the day that Service A will stop appearing on this channel. This also establishes when Service B will start appearing on this channel.

9. Click the **Service B** arrow and select the service that you want to appear on this channel when Service A ends.

10. Click in the **Ends at** field to the right of the Service B field and type the exact time you want Service B to stop appearing on this channel. You must type two digits for each value.

**Example:** You would type ten o'clock as **100000**. The system inputs the colons for you and displays 10:00:00.

**Note:** You can also represent time in the 24-hour format. For example, 22:30:00 would represent 10:30 p.m.

11. Click **AM/PM** to establish which portion of the day that Service B will stop appearing on this channel. This also establishes when Service A will start appearing on this channel.

**Note:** The default time for Service A to start using a channel slot is midnight. However, when you select the ending time for Service B, you can reset this time to be any time you want. The actual time that Service A will begin using the channel slot is reflected in the bottom left corner of the Set Up Split Channel window after you select **AM** or **PM**.

12. Click **OK**. The system saves the split channel information in the DNCS database and closes the Set Up Split Channel window. The Set Up Display Channel Map window updates to include the new split channel.

13. Do you need to split another channel on this channel map?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns you to the Display Channel Map List window.

**Note:** It takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

14. Do you need to split another channel on another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

15. Do you need to include the service on your IPG?

- If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for more information. To obtain this guide, refer to Printed Resources.
- If **no**, go to step 17.

16. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

## Split a Channel

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

If you need to use one channel to show one service during one period of the day and another service during the remainder of the day, you must split that channel so the system will know which service to implement and when.

## Before You Begin

Before you can set up a split channel, there must be at least two services listed in the **Available Services** field on the Set Up Display Channel Map window.

## Time To Complete

Splitting a channel takes approximately 20 minutes to complete, including the time it takes for the channel changes to appear on DHCTs.

## Performance Impact

Splitting a channel does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Splitting a Channel

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map that contains the channel you need to split.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. In the **Channel Slot** field, double-click on the channel you want to split. The Set Up Split Channel window opens.

**Important:** If a service is already assigned to the channel slot, a confirmation window will open to indicate that the service in that slot will be deleted if you continue. Make sure that you do not want to include that service as part of the split channel before you click **Yes** and continue.

6. Does the **Service A** field contain one of the services you want to include in this split channel?
   - If **yes**, go to step 7.
   - If **no**, click the **Service A** arrow and select the service that you want to appear first on this channel every day for seven days a week.
7. Click in the **Ends at** field to the right of the Service A field and type the exact time you want Service A to stop appearing on this channel. You must type two digits for each value.

**Example:** You would type six o'clock as **060000**. The system inputs the colons for you and displays 06:00:00.

**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

8. Click **AM/PM** to establish which portion of the day that Service A will stop appearing on this channel. This also establishes when Service B will start appearing on this channel.

9. Click the **Service B** arrow and select the service that you want to appear on this channel when Service A ends.

10. Click in the **Ends at** field to the right of the Service B field and type the exact time you want Service B to stop appearing on this channel. You must type two digits for each value.

**Example:** You would type ten o'clock as **100000**. The system inputs the colons for you and displays 10:00:00.

**Note:** You can also represent time in the 24-hour format. For example, 22:30:00 would represent 10:30 p.m.

11. Click **AM/PM** to establish which portion of the day that Service B will stop appearing on this channel. This also establishes when Service A will start appearing on this channel.

**Note:** The default time for Service A to start using a channel slot is midnight. However, when you select the ending time for Service B, you can reset this time to be any time you want. The actual time that Service A will begin using the channel slot is reflected in the bottom left corner of the Set Up Split Channel window after you select **AM** or **PM**.

12. Click **OK**. The system saves the split channel information in the DNCS database and closes the Set Up Split Channel window. The Set Up Display Channel Map window updates to include the new split channel.

13. Do you need to split another channel on this channel map?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns you to the Display Channel Map List window.

**Note:** It takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

14. Do you need to split another channel on another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

15. Do you need to include the service on your IPG?

- If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for more information. To obtain this guide, refer to Printed Resources.
- If **no**, go to step 17.

16. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

# SARA Server

Buttons on the Server Applications tab of the DNCS Administrative Console are controlled by the SARA server.

Online Help is not available for the SARA server. If you have questions about the SARA server, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159). To obtain a copy of this document, see Printed Resources.

# Service Groups

From this window, you can create service groups, which are used to provide VOD and other interactive services. You can also modify or delete service groups from this window.

A service group is a set of QAM, MQAM, or GQAM modulator channels that provide narrowcast (VOD) services to a unique group of DHCTs. Service groups enable a DHCT to identify to the VOD server the VOD QAM resources to which the DHCT has access.

**Important:** If you are using Overlay technology, remember that GoQAM modulators cannot be used to provide VOD services. GoQAM modulators produce partially encrypted sessions, which are not necessary for providing VOD.

**In This Section**


Service Group Settings
Service Group Filter
Add a Service Group
Modify a Service Group
Delete a Service Group



From this window, you can create service groups, which are used to provide VOD and other interactive services. You can also modify or delete service groups from this window.

A service group is a set of QAM, MQAM, or GQAM modulator channels that provide narrowcast (VOD) services to a unique group of DHCTs. Service groups enable a DHCT to identify to the VOD server the VOD QAM resources to which the DHCT has access.

**Important:** If you are using Overlay technology, remember that GoQAM modulators cannot be used to provide VOD services. GoQAM modulators produce partially encrypted sessions, which are not necessary for providing VOD.


## What do you want to do?

- Learn about different kinds of service groups
- Review service group settings
- Use the Filter to display information about the service groups in your system
- Add a service group to the DNCS
- Modify an existing service group
- Delete existing service groups
- Display the latest data about service groups, by clicking **Reset**

### Types of Service Groups

A service group is a set of QAM, MQAM, or GQAM modulator channels that provide narrowcast services, most frequently VOD services, to a unique group of DHCTs. Service groups enable a VOD server to determine which VOD QAM modulator resources a DHCT can access.

You can add the following types of service groups to the DNCS:

- Parent service groups, which contain one or more child service groups
- **Child service groups**, which belong to a parent service group
- **Standalone service groups**, which are independent: they contain no child service groups nor do they belong to a parent service group

Allowing one service group to belong to another enables you to more effectively manage the different types of content that your VOD server provides.

Related Topics

- Why Use Different Types of Service Groups?
- Service Groups for VOD Services
- Add a Service Group

### Why Use Different Types of Service Groups?

Your ability to better manage content increases when using parent and child service groups because you can share the VOD QAM channels of a parent service group with those of its children. Sharing QAM channels gives you the ability to provide services without consuming a large portion of the available RF spectrum.

For example, because child service groups have access to all of the QAM modulator channels of their parent, a parent service group typically provides content that is infrequently accessed, such as classic films or documentaries. Low demand for this type of content means that it can be made available to a larger group of DHCTs (those fed by a child and its parent) without impacting the ability of subscribers to access the content. However, content that is in high demand, such as recent movie releases, is typically provided by child service groups. Child service groups better serve this purpose because they feed a smaller number of DHCTs than parent service groups.

**Note:** VOD providers often refer to low-demand content as "library content."

### Related Topics

- Types of Service Groups
- Service Groups for VOD Services
- Add a Service Group
- Modify a Service Group
- Delete a Service Group

### Service Groups for VOD Services

If you are going to provide VOD services, add a service group for each unique group of VOD QAM modulators. To provide low-demand (library) content, identify this service group as a parent service group and then add child service groups, which provide high-demand content, to the parent service group. If you do not want to manage content by distinguishing between content types, simply add a service group and do not identify it as a parent service group. (Standalone service groups contain no child service groups nor do they belong to parent service groups.)

### Related Topics

- Types of Service Groups
- Why Use Different Types of Service Groups
- Add a Service Group
- Modify a Service Group
- Delete a Service Group

## Service Group Settings

The following settings allow you to manage the service groups in your network:

- Add Service Group Settings
- Edit Service Group Settings

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

### Add Service Group Settings

Use the Add Service Group window on the DNCS Administrative Console to add service groups to the DNCS.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and that processes VOD data for Hub 1. |
| Parent Group | Allows this service group to function as a parent service group.<br><br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Groups/Selected Groups | Determines the child groups associated with this parent group. Select groups from this list only when adding a parent service group to the DNCS.<br><br>To add a child to this parent service group, select a service group in the Available Group list and click **Add**.<br><br>The selected service group moves from the Available Groups list to the Selected Groups list.<br><br>**Notes:**<br><br>▪If you make a mistake, you can remove ports from the Selected Groups list by clicking on the name of the group you want to remove in the Selected Groups list, and then clicking **Remove**. The selected group moves from the Selected Groups list into the Available Groups list.<br><br>▪These lists display only when you select the **Parent Group** setting. For more information on parent service groups, see Types of Service Groups. |
| Available Ports/Selected Ports | Determines the ports associated with the service group.<br><br>Select the port of the QAM, MQAM, or GQAM modulator that will provide VOD data for this service group and click **Add**.<br><br>The selected port moves from the Available Ports list into the Selected Ports list.<br><br>Repeat for each QAM, MQAM, or GQAM modulator that will provide VOD data for this service group.<br><br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

**Related Topics**

- Service Groups
- Edit Service Group Settings

### Edit Service Group Settings

Use the Edit Service Group window on the DNCS Administrative Console to modify the settings of a service groups.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| Service Group ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Service Group Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and that processes VOD data for Hub 1. |
| Parent ID | A 0 in this field indicates that this is a parent or standalone service group.<br><br>If this is a child service group, you can change it to a parent or standalone service group, by entering a 0 in this field.<br><br>If this is a child service group, you can change the Parent ID and make this service group the child of another parent service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable.<br><br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Children | If this is a parent service group, the child groups associated with this parent group are listed here. |
| Parent Group | Allows this service group to function as a parent service group.<br><br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Ports/Selected Ports | For a parent, standalone, or child service group, you can change the RF ports that the service group uses by adding or removing RF ports:<br><br>▪To add RF ports to the service group, select a port in the **Available Ports** and click **Add**. The selected port moves from the Available Ports list to the Selected Ports list.<br><br>▪To remove RF ports from the service group, select a port in the **Selected Ports** list and click **Remove**. The selected port moves from the Selected Ports list to the Available Ports list.<br><br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in |

| | |
|---|---|
| | the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

## Related Topics

- Service Groups
- Add Service Group Settings

## Service Group Filter

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

From the Filter area on the Service Group Data window, you can quickly retrieve information about the service groups in your system. The Filter allows you to select service group attributes, such as a service group name, and find the service groups in your system that meet your search criteria.

## What do you want to do?

- Learn about service group filter settings
- Use the Filter to search and display the service groups in your system
- Learn about the data that the filter displays

### Service Group Filter Settings

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

This section describes service group Filter options and provides examples to show how the Filter searches for service groups based on your selections.

**Notes:**

- To learn more about service group data the Filter displays in the Service Group Data window, see Service Group Data.
- To learn how to use the Filter to search for and display certain service groups, see Use the Filter to Display Service Group Data.

### Service Group Filter Options

The following table describes the Filter options for searching service groups.

| By Field | By Value | Examples |
|---|---|---|
| **ID** | Enter the service group ID in the By Value field to have the filter display service group data for the ID you entered.<br><br>Important: The filter searches for the service group with an ID that exactly matches the number you enter in the By Value field. | If you enter **38** in the By Value field, the Filter finds and displays only the service group with an ID of 38. The Filter would not search for service groups whose IDs contain the number 38.<br><br>For example, service groups with IDs of 3855 or 138 would not be found. |
| **Name** | Enter any part of a service group name in the By Value field to have the filter display service groups whose names match any portion of the text entered in this field.<br><br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **Se** in the By Value field, the Filter finds and displays service groups with any of the following names:<br><br>▪All**Se**rvice<br>▪LaGrange **Se**rvice Group<br>▪**Se**rvice Group 10 |
| **Parent ID** | Enter the Parent ID of the service group whose data you want in the By Value field to have the filter display parent service groups with IDs that match any portion of the text entered in this field.<br><br>**Important:** The filter searches for the service group with a Parent ID that exactly matches the number you enter in the By Value field. | If you enter **38** in the By Value field, the Filter finds and displays only the service group with a Parent ID of 38. The Filter would not search for service groups whose Parent ID contain the number 38.<br><br>For example, service groups with Parent IDs of 3855 or 138 would not be found. |

### Use the Filter to Display Service Group Data

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

This section provides instructions for using the Filter to search and display the service groups in your system.

### Before You Begin

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following service group parameters:

- Service group ID
- Service group name
- Parent ID

### Display Service Group Data

1. Click the **By Field** arrow and select one of the following options:
   - ID
   - Name
   - Parent ID

   **Note:** For a description of these options, see Service Group Filter Settings.

2. Click in the **By Value** field and enter data in this field.

   **Note:** For examples of how By Value data affects searches, see Service Group Filter Settings.

3. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Service Group Data window.

   **Notes:**

   - For information about the data displayed in the Service Group Data window, see Service Group Data.
   - You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: ID, Parent ID, Name. Clicking the same heading again displays the column in descending order.

**Before You Begin**

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following service group parameters:

- Service group ID
- Service group name
- Parent ID

### Use the Filter to Display Service Group Data

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

This section provides instructions for using the Filter to search and display the service groups in your system.

### Before You Begin

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following service group parameters:

- Service group ID
- Service group name
- Parent ID

### Display Service Group Data

1. Click the **By Field** arrow and select one of the following options:
   - ID
   - Name
   - Parent ID

**Note:** For a description of these options, see Service Group Filter Settings.

1. Click in the **By Value** field and enter data in this field.

**Note:** For examples of how By Value data affects searches, see Service Group Filter Settings.

1. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Service Group Data window.

**Notes:**

- For information about the data displayed in the Service Group Data window, see Service Group Data.
- You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: ID, Parent ID, Name. Clicking the same heading again displays the column in descending order.

### Service Group Data

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

When you use the Filter to search for and display service groups, search results are shown in the Service Group Data window, which lists the following information:

| Field | Description |
|---|---|
| Service Group ID | Shows the unique numerical identifier for the service group. This field accepts up to 10 digits.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Service Group Name | Shows the name used to identify this service group.<br><br>You can use numbers and letters. We recommend that you establish a naming scheme that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example**: A name of VOD_SG_Hub1_MQ43 could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and that processes VOD data for Hub 1. |
| Groups: Available and Selected | Shows the groups that can be assigned to the parent service group. |
| Ports: Available and Selected | Shows the ports of the QAM, MQAM, or GQAM modulators that will provide VOD data for the service group. |

## Add a Service Group

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

These instructions describe how to add a service group to the DNCS.

**Note:** For more information about service groups, see Types of Service Groups.

**Important:** If you are using Overlay technology, remember that GoQAM modulators cannot be used to provide VOD services. GoQAM modulators produce partially encrypted sessions, which are not necessary for providing VOD.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also know which QAM, MQAM, or GQAM modulator will provide data for each VOD service.

### Adding a Service Group

After you add the content QAM, MQAM modulator, or GQAM modulator that will be providing data for a particular VOD service, complete these steps to add a service group for that modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Click **Add**. The Add Service Group window opens.
5. Complete the fields on the screen as described in Service Group Settings.

Use the Add Service Group window on the DNCS Administrative Console to add service groups to the DNCS.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and |

| | |
|---|---|
| | that processes VOD data for Hub 1. |
| Parent Group | Allows this service group to function as a parent service group.<br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Groups/Selected Groups | Determines the child groups associated with this parent group. Select groups from this list only when adding a parent service group to the DNCS.<br>To add a child to this parent service group, select a service group in the Available Group list and click **Add**.<br>The selected service group moves from the Available Groups list to the Selected Groups list.<br>**Notes:**<br>▪ If you make a mistake, you can remove ports from the Selected Groups list by clicking on the name of the group you want to remove in the Selected Groups list, and then clicking **Remove**. The selected group moves from the Selected Groups list into the Available Groups list.<br>▪ These lists display only when you select the **Parent Group** setting. For more information on parent service groups, see Types of Service Groups. |
| Available Ports/Selected Ports | Determines the ports associated with the service group.<br>Select the port of the QAM, MQAM, or GQAM modulator that will provide VOD data for this service group and click **Add**.<br>The selected port moves from the Available Ports list into the Selected Ports list.<br>Repeat for each QAM, MQAM, or GQAM modulator that will provide VOD data for this service group.<br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

### Related Topics

- Service Groups
- Edit Service Group Settings

6. Click **Save**. The system closes the Add Service Group window and displays the Service Group Data window, which now lists the service group that you just added. The message "Service Group Saved Successfully" appears in the status area of the window.

7. Click **File > Close** to return to the DNCS Administrative Console.

## Related Topics

- Modify a Service Group
- Remove a Service Group
- Types of Service Groups

## Add a Service Group

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

These instructions describe how to add a service group to the DNCS.

**Note:** For more information about service groups, see Types of Service Groups.

**Important:** If you are using Overlay technology, remember that GoQAM modulators cannot be used to provide VOD services. GoQAM modulators produce partially encrypted sessions, which are not necessary for providing VOD.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also know which QAM, MQAM, or GQAM modulator will provide data for each VOD service.

### Adding a Service Group

After you add the content QAM, MQAM modulator, or GQAM modulator that will be providing data for a particular VOD service, complete these steps to add a service group for that modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Click **Add**. The Add Service Group window opens.
5. Complete the fields on the screen as described in Service Group Settings.

Use the Add Service Group window on the DNCS Administrative Console to add service groups to the DNCS.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and |

| | |
|---|---|
| | that processes VOD data for Hub 1. |
| Parent Group | Allows this service group to function as a parent service group.<br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Groups/Selected Groups | Determines the child groups associated with this parent group. Select groups from this list only when adding a parent service group to the DNCS.<br>To add a child to this parent service group, select a service group in the Available Group list and click **Add**.<br>The selected service group moves from the Available Groups list to the Selected Groups list.<br>**Notes:**<br>▪ If you make a mistake, you can remove ports from the Selected Groups list by clicking on the name of the group you want to remove in the Selected Groups list, and then clicking **Remove**. The selected group moves from the Selected Groups list into the Available Groups list.<br>▪ These lists display only when you select the **Parent Group** setting. For more information on parent service groups, see Types of Service Groups. |
| Available Ports/Selected Ports | Determines the ports associated with the service group.<br>Select the port of the QAM, MQAM, or GQAM modulator that will provide VOD data for this service group and click **Add**.<br>The selected port moves from the Available Ports list into the Selected Ports list.<br>Repeat for each QAM, MQAM, or GQAM modulator that will provide VOD data for this service group.<br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

### Related Topics

- Service Groups
- Edit Service Group Settings

6. Click **Save**. The system closes the Add Service Group window and displays the Service Group Data window, which now lists the service group that you just added. The message "Service Group Saved Successfully" appears in the status area of the window.

7. Click **File > Close** to return to the DNCS Administrative Console.

## Related Topics

- Modify a Service Group
- Remove a Service Group
- Types of Service Groups

## Modify a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Select Service Group Name] > Open Selected Service Group**

This section describes how to modify service groups, which are used to provide VOD and other interactive services to subscribers.

After a service group has been saved in the DNCS, you can modify many of its parameters. For example, you can add a QAM modulator to the service group by selecting the modulator's RF output ports the VOD service will use. If your site uses generic QAM modulators, you can use the same method to add generic QAM modulators to service groups. However, to change the name or identifier (ID) of a service group, delete the service group and then add the service group again. When you add the service group back to the DNCS, use a new name or ID for the service group.

### Modifying a Service Group

Complete these steps to modify a service group in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Use the Filter to display the service group that you want to modify.

   **Note:** For assistance using the Filter, see Service Group Filter.

5. Select the box next to the Service Group that you want to modify.
6. Click **Edit**. The Edit Service Group window opens for the service group you selected.
7. Make any of the following changes. For assistance with any of the fields, see Edit Service Group Settings.
   - If this is a child service group, you can change the Parent ID and make this service group the child of another parent service group. Or, you can enter a Parent ID of 0 to make this a standalone service group instead of a child service group.

     Important: Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable.

   - For a parent, standalone, or child service group, you can change the RF ports that the service group uses by adding or removing RF ports:
     - To add RF ports to the service group, select a port in the Available Ports and click **Add** . The selected port moves from the Available Ports list to the Selected Ports list.
     - To remove RF ports from the service group, select a port in the **Selected Ports** list and click **Remove**. The selected port moves from the Selected Ports list to the Available Ports list.
8. When you finish making changes, click **Save** . The system saves the new service group information in the DNCS database. The Service Group Data window updates to include the new service group information.
9. Update your network map to reflect these changes.

## Modify a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Select Service Group Name] > Open Selected Service Group**

This section describes how to modify service groups, which are used to provide VOD and other interactive services to subscribers.

After a service group has been saved in the DNCS, you can modify many of its parameters. For example, you can add a QAM modulator to the service group by selecting the modulator's RF output ports the VOD service will use. If your site uses generic QAM modulators, you can use the same method to add generic QAM modulators to service groups. However, to change the name or identifier (ID) of a service group, delete the service group and then add the service group again. When you add the service group back to the DNCS, use a new name or ID for the service group.

### Modifying a Service Group

Complete these steps to modify a service group in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Use the Filter to display the service group that you want to modify.

   **Note:** For assistance using the Filter, see Service Group Filter.

5. Select the box next to the Service Group that you want to modify.
6. Click **Edit**. The Edit Service Group window opens for the service group you selected.
7. Make any of the following changes. For assistance with any of the fields, see Edit Service Group Settings.
   - If this is a child service group, you can change the Parent ID and make this service group the child of another parent service group. Or, you can enter a Parent ID of 0 to make this a standalone service group instead of a child service group.

     Important: Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable.

   - For a parent, standalone, or child service group, you can change the RF ports that the service group uses by adding or removing RF ports:
     - To add RF ports to the service group, select a port in the Available Ports and click **Add** . The selected port moves from the Available Ports list to the Selected Ports list.
     - To remove RF ports from the service group, select a port in the **Selected Ports** list and click **Remove**. The selected port moves from the Selected Ports list to the Available Ports list.
8. When you finish making changes, click **Save** . The system saves the new service group information in the DNCS database. The Service Group Data window updates to include the new service group information.
9. Update your network map to reflect these changes.

# Delete a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Service Group Name] Delete Selected Service Group**

Use this procedure to delete a standalone, parent, or child service group from the DNCS.

**Important:** When you delete a parent service group, any child service groups that belong to the parent service group **are not** deleted. Child service groups remain until you delete each one individually, or change the child service group to a standalone service group by changing the Parent ID of the child service group to 0.

## You Need to Know

Before You Begin

Before you delete a service group, you must delete any associated QAM or MQAM modulators. In addition, you must have your network map available.

## Deleting a Service Group

1. Are there any QAM or MQAM modulators associated with this service group?
   - If **yes**, delete those modulators first. Go to Deleting a QAM, MQAM, GQAM, or GoQAM Modulator. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Service Group**. The Service Group Data window opens.
5. Use the Filter to display the service group that you want to delete.

   **Note:** For assistance using the Filter, see Service Group Filter Overview.
6. Select the box to the left of the service group that you want to delete.
7. Click **Delete**. A confirmation window opens and asks you to confirm the deletion.
8. Click **OK**. The system removes the service group from the Service Group Data window and a message appears in the Status area of the window to let you know that the deletion was successful.
9. Remove the service group from your network map.

## Delete a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Service Group Name] Delete Selected Service Group**

Use this procedure to delete a standalone, parent, or child service group from the DNCS.

**Important:** When you delete a parent service group, any child service groups that belong to the parent service group **are not** deleted. Child service groups remain until you delete each one individually, or change the child service group to a standalone service group by changing the Parent ID of the child service group to 0.

### You Need to Know

Before You Begin

Before you delete a service group, you must delete any associated QAM or MQAM modulators. In addition, you must have your network map available.

### Deleting a Service Group

1. Are there any QAM or MQAM modulators associated with this service group?
   - If **yes**, delete those modulators first. Go to Deleting a QAM, MQAM, GQAM, or GoQAM Modulator. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Service Group**. The Service Group Data window opens.
5. Use the Filter to display the service group that you want to delete.

   **Note:** For assistance using the Filter, see Service Group Filter Overview.
6. Select the box to the left of the service group that you want to delete.
7. Click **Delete**. A confirmation window opens and asks you to confirm the deletion.
8. Click **OK**. The system removes the service group from the Service Group Data window and a message appears in the Status area of the window to let you know that the deletion was successful.
9. Remove the service group from your network map.

# Manage Network Features

## Introduction

This section describes how to manage the following network features:

- Content protection
- Daylight Saving Time
- Direct ASI
- DOCSIS set-top gateway support
- Enhanced channel maps
- GQAM redundancy
- InstaStaging
- Multiple bootloader carousels
- OpenCable compliance
- Overlay
- PowerKEY Conditional Access
- Stat mux dejitter groups
- SONET networks
- Two-way communication
- Video-on-demand

# Content Protection

We provide end-to-end solutions for content protection to prevent the unauthorized copying and distribution of program content. Encrypted program content is protected by Copy Control Information (CCI) data embedded in Entitlement Control Messages (ECMs). DHCT outputs are protected in different ways depending on content type and output method.

For more information on protecting content, refer to Enabling Content Protection for Broadcast Programming Configuration Guide (part number 4005893). To obtain a copy of this publication, see Printed Resources.

**Important:** Content-protection features for our DHCTs are being phased in with newer versions of application platform software. The activation or implementation of content- protection features is dependent on specific versions of SARA and PowerTV OS software, some of which are in development. For the most recent information on software versions that support content-protection features, contact Cisco Services.

## What do you want to do?

- Protect encrypted broadcasts from unauthorized copying
- Protect on-demand content from unauthorized copying (Protect On-Demand Content From Unauthorized Copying, Removing the no_vod_cci File Flag)
- Delete a _DVI SAM Service to ensure that content-protection methods do not conflict
- Learn how CCI impacts subscribers
- Find out who determines if program content can be copied
- Learn the types of content protection supported by our DHCTs and CableCARD modules
- Review the levels of CCI embedded in encrypted programs
- Review a list of common methods of content protection
- Review how CCI-enabled DHCTs respond to various content-protection methods

## Delete the _DVI SAM Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > Short Description tab > [Select _DVI service] > File > Delete**

You might have previously set up a _DVI SAM service to turn off HDCP on a DVI port. However, starting with Service Pack 2 for SR 2.2 and SR 3.2 software, support for content protection policy settings was added. Because the _DVI SAM service cannot be used in conjunction with the software that supports content protection policy settings, you are required to delete this service.

Complete these steps to make certain that your system does not use a _DVI SAM service and to delete an existing _DVI SAM service, if necessary.

### Deleting the _DVI SAM Service

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service** to open the SAM Service List window.
3. Click the **Short Description** tab. If you click the Short Description tab again, the services in that column are reordered.
4. Do you have a _DVI service listed in the Short Description column?
   - If **yes**, highlight the _DVI service.
   - If **no**, go to step 6.
5. Click **File > Delete** to delete the service. Then, click **Yes** to confirm that you want to delete the file.
6. Click **File > Close** to close the SAM Service List window.
7. Do you have a package already built to control only the DVI port or the HDCP function?

**Important:** Before you delete any _DVI SAM package be certain that the package is used specifically for the _DVI SAM service. Do not delete a package if it is also used for other functions.

   - If **yes**, delete that package and have billing stop assigning that package to DHCTs.
   - If **no**, you have successfully deleted the existing _DVI SAM service.

## Delete the _DVI SAM Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > Short Description tab > [Select _DVI service] > File > Delete**

You might have previously set up a _DVI SAM service to turn off HDCP on a DVI port. However, starting with Service Pack 2 for SR 2.2 and SR 3.2 software, support for content protection policy settings was added. Because the _DVI SAM service cannot be used in conjunction with the software that supports content protection policy settings, you are required to delete this service.

Complete these steps to make certain that your system does not use a _DVI SAM service and to delete an existing _DVI SAM service, if necessary.

### Deleting the _DVI SAM Service

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service** to open the SAM Service List window.
3. Click the **Short Description** tab. If you click the Short Description tab again, the services in that column are reordered.
4. Do you have a _DVI service listed in the Short Description column?
   - If **yes**, highlight the _DVI service.
   - If **no**, go to step 6.
5. Click **File > Delete** to delete the service. Then, click **Yes** to confirm that you want to delete the file.
6. Click **File > Close** to close the SAM Service List window.
7. Do you have a package already built to control only the DVI port or the HDCP function?

**Important:** Before you delete any _DVI SAM package be certain that the package is used specifically for the _DVI SAM service. Do not delete a package if it is also used for other functions.

   - If **yes**, delete that package and have billing stop assigning that package to DHCTs.
   - If **no**, you have successfully deleted the existing _DVI SAM service.

## Content Protection Settings

Use the following fields when you manage content protection for existing segments.

| Field | Description |
|---|---|
| Digital Copy Rights | Defines the option appropriate for your system to set content protection for 1394 ports that receive this segment.<br>▪**Copy Never** - Prevent subscribers from making a digital copy of any program or event associated with this segment.<br>**Important:** The FCC does not permit a segment to be marked "Copy Never" unless that segment is being used for pay-per-view (PPV).<br>▪**Copy One Generation** - Allow subscribers to make a single digital copy of any program or event associated with this segment.<br>▪**Copy Freely** - Allow subscribers to make as many copies as they would like of any program or event associated with this segment. |
| Macrovision | Defines the option appropriate for your system to set content protection of PPV or VOD on analog composite output ports that receive this segment.<br>▪**Enabled** - Use the Macrovision content-protection process to prevent subscribers from copying all events or programming that this segment provides. Selecting this option prevents unauthorized copying by significantly distorting a recording of the event or programming this segment provides.<br>**Note:** Clicking enable causes an informational window to open that describes the license restrictions of the Macrovision content-protection process. When this window opens, click **OK**.<br>▪**Disabled** - You do not want to use the Macrovision content-protection process to prevent subscribers from copying all events or programming that this segment provides. Selecting this option allows subscribers to record a viewable copy of the event or programming this segment provides.<br>▪**Follow Package Definition** - Not currently supported. |
| CIT flag<br>(Constrained Image Trigger) | Defines the option appropriate for your system to set content protection on YPbPr component (HD analog) output ports that receive this segment.<br>▪**Clear** - Allow high-definition analog outputs to display video at full HD resolution.<br>▪**Set** - Cause high-definition analog outputs to reduce the effective image resolution to less than 520,000 pixels. |

## Protect Encrypted Broadcasts From Unauthorized Copying

**Quick Path: DNCS Administrative Console > DNCS tab > Source > File > All Segments > [Select Segment] > File > Open**

To protect the content of an encrypted broadcast source, assign CCI to each segment that provides a service from this source. This procedure describes how to configure the Set Up Segment window to assign a level of CCI to an existing segment. To determine the level of security required for each encrypted service you offer to subscribers, contact your corporate office or the content provider.

**Notes:**

- CCI settings are effective immediately.
- In a system where PowerKEY is not used, the provider of the primary conditional access (CA) system is responsible for delivering CCI data to the DHCT.
- A content-protection method is not enforced on OpenCable Host devices that are not running the PowerTV OS. For example, you may require the HDCP to be always on, but the OpenCable Host may disable HDCP for Copy Freely content.

**Important:** If more than one segment has been created from the same source, all segments must have the same levels of content-protection. Otherwise, content-protection may not work as expected for those segments.

## You Need to Know

Additional Information

For details on these content-protection settings, including the content-protection methods used by output ports on our DHCTs, see Enabling Content Protection for Broadcast Programming Configuration Guide (part number 4005893). To obtain a copy of this publication, see Printed Resources.

Before You Begin

Before you begin, contact your corporate office or your content provider to determine the level of security required for each encrypted service you offer subscribers.

**Important:** CCI is delivered in the ECM for a program. As a result, it may be applied to any **encrypted** source. However, it cannot be applied to a **clear** source because clear sources do not require ECMs.

Time to Complete

Adding security to one segment takes about a minute.

### Assigning Content Protection to Existing Segments

To embed CCI in segments associated with an encrypted broadcast source, complete the following steps.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Select the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > All Segments**. The Segment List window opens.
5. Select a segment in the list, and click **File > Open**. The Set Up Segment window opens.
6. Complete the content-protection fields as described in Content Protection Settings.

Use the following fields when you manage content protection for existing segments.

| Field | Description |
|---|---|
| Digital Copy Rights | Defines the option appropriate for your system to set content protection for 1394 ports that receive this segment.<br>▪ **Copy Never** - Prevent subscribers from making a digital copy of any program or event associated with this segment.<br>**Important:** The FCC does not permit a segment to be marked "Copy Never" unless that segment is being used for pay-per-view (PPV).<br>▪ **Copy One Generation** - Allow subscribers to make a single digital copy of any program or event associated with this segment.<br>▪ **Copy Freely** - Allow subscribers to make as many copies as they would like of any program or event associated with this segment. |
| Macrovision | Defines the option appropriate for your system to set content protection of PPV or VOD on analog composite output ports that receive this segment.<br>▪ **Enabled** - Use the Macrovision content-protection process to prevent subscribers from copying all events or programming that this segment provides. Selecting this option prevents unauthorized copying by significantly distorting a recording of the event or programming this segment provides.<br>**Note:** Clicking enable causes an informational window to open that describes the license restrictions of the Macrovision content-protection process. When this window opens, click **OK**.<br>▪ **Disabled** - You do not want to use the Macrovision content-protection process to prevent subscribers from copying all events or programming that this segment provides. Selecting this option allows subscribers to record a viewable copy of the event or programming this segment provides.<br>▪ **Follow Package Definition** - Not currently supported. |
| CIT flag<br>(Constrained Image Trigger) | Defines the option appropriate for your system to set content protection on YPbPr component (HD analog) output ports that receive this segment.<br>▪ **Clear** - Allow high-definition analog outputs to display video at full HD resolution.<br>▪ **Set** - Cause high-definition analog outputs to reduce the effective image resolution to less than 520,000 pixels. |

7. Do you need to add content-protection to another segment?

**Important:** When creating other segments from the same source, make certain that all segments have the same levels of content-protection; otherwise, the content protection may not work as expected for these segments.

- If **yes**, repeat this procedure from step 5.
- If **no**, you have successfully added content protection information to appropriate segments. Click **File > Close** to close the Segment List window and return to the Source List window.

8. To close the Source List window, click **File > Close**.

## Protect On-Demand Content From Unauthorized Copying

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules > BFS Client > [Expand the OSM File Cabinet] > File > Delete**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules > Please select a site > [Select Site] > BFS Client > [Expand the OSM File Cabinet] > File > Delete**

To protect the content of an encrypted on-demand source, assign CCI to each segment that provides a service from this source. This procedure describes how to configure the Set Up Segment window to assign a level of CCI to an existing segment. To determine the level of security required for each encrypted service you offer to subscribers, contact your corporate office or the content provider.

**Notes:**

- CCI settings are effective immediately.
- In a system where PowerKEY is not used, the provider of the primary conditional access (CA) system is responsible for delivering CCI data to the DHCT.
- A content-protection method is not enforced on OpenCable Host devices that are not running the PowerTV OS. For example, you may require the HDCP to be always on, but the OpenCable Host may disable HDCP for Copy Freely content.

**Important:** If more than one segment has been created from the same source, all segments must have the same levels of content-protection. Otherwise, content-protection may not work as expected for those segments.

**You Need to Know**

Additional Information

For details on these content-protection settings, including the content-protection methods used by output ports on our DHCTs, see Enabling Content Protection for Broadcast Programming Configuration Guide (part number 4005893). To obtain a copy of this publication, see Printed Resources.

Before You Begin

Before you begin, contact your corporate office or your content provider to determine the level of security required for each encrypted service you offer subscribers.

**Important:** CCI is delivered in the ECM for a program. As a result, it may be applied to any **encrypted** source. However, it cannot be applied to a **clear** source because clear sources do not require ECMs.

Time to Complete

Adding security to one segment takes about a minute.

### Removing the no_vod_cci File Flag

If the no_vod_cci file is present on the BFS, DHCTs automatically activate content protection on the 1394 output for any VOD or xOD sessions. For this reason, you should remove the no_vod_cci flag from the BFS if you want DHCTs to protect content based on the settings provided by the VOD or xOD application.

To remove the no_vod_cci file from the BFS, complete the following procedure.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **OS**. The DHCT OS List window opens.
4. Scroll through the OS list. Is the no_vod_cci file present in the list?
   - If **yes**, select the file and click **File > Delete**. The file is removed from the BFS. All VOD or xOD sessions built from this point forward use the content- protection settings specified in the session setup request.
   - If **no**, go to step 5.
5. Click **File > Close** to close the OS list.
6. Select the **Applications Interface Modules** tab.
7. Are you using our RCS Solution?
   - If **yes**, click **BFS Client**. The Please select a site window opens. Go to step 8.
   - If **no**, click **BFS Client**. The Broadcast File Server List window opens. Go to step 9.
8. Select **DNCS** from the list of sites. Then select **File > Select**. The Broadcast File Server List window opens for the site you selected.
9. Scroll down and double-click the **OSM** cabinet.
10. Is the no_vod_cci file present in the OSM cabinet?
    - If **yes**, select the file.
    - If **no**, go to step 12.
11. Click **File > Delete** to delete the file.
12. Click **File > Close** to close the Broadcast File Server List window.
13. Are you using our RCS Solution?
    - If **no**, you have successfully removed the no_vod_cci file flag.
    - If **yes**, go to step 14.
14. Do you want to remove the no_vod_cci file flag from other sites in your system?
    - If **yes**, from the Please select a site window, select the site whose no_vod_cci flag you want to remove. Then repeat this procedure from step 8 to remove the no_vod_cci flag file from this site.
    - If **no**, you have successfully removed the no_vod_cci file flag from all sites in your system. Select **File > Close** to close the Please select a site window.

### Creating the no_vod_cci File Flag

If your provider is not able to set up content protection for your server, complete the following instructions to set up a VOD file flag (no_vod_cci) to set all content to "copy never."

1. Open an xterm window.
2. At the dncs user prompt, type **pwd** and press **Enter**. The system displays the working directory.
3. Did the system display **/export/home/dncs** as the working directory?
   - If **yes**, go to step 4.
   - If **no**, type **cd /export/home/dncs** and press **Enter**. The system makes /export/home/dncs the working directory.
4. Type **touch no_vod_cci** and press **Enter**. The system creates an empty file in the directory /export/home/dncs and labels the file no_vod_cci.
5. Type **exit** and press **Enter**. The xterm window closes.
6. From the DNCS Administrative Console, select the **DNCS** tab.
7. Select the **Home Element Provisioning** tab.
8. Click **OS**. The DHCT OS List window opens.
9. Click **File > New**. The Set Up DHCT OS window opens.
10. Click **Browse**. The Select OS File window opens.
11. Click in the **Filter** field and type **/export/home/dncs/***. The files in the /export/home/dncs directory appear in the Files list.
12. Scroll down the Files list to find and select the file no_vod_cci that you created. The Selection field updates and displays the path to the no_vod_cci file.
13. Click **OK**. The Select OS File window closes and /export/home/dncs/no_vod_cci appears in the Source File field on the Set Up DHCT OS window.
14. In the **Destination File Name** field, type **bfs:///osm/no_vod_cci**.
15. In the **Description** field, type **File to Activate Content Protection on VOD**.
16. For **Format**, select **Out-of-Band File**.
17. Click **Save**. The system places the no_vod_cci file the BFS carousel and, as a result, DHCTs automatically activate content protection on 1394 outputs for any VOD or xOD sessions.

## CCI Impact on Subscribers

CCI is a bit-encoded value associated with specific media content. It is delivered in the ECM for a program and describes the level of protection that should be applied to the content. Because CCI provides only the **level of protection** that should be applied, it is up to the various software components that receive CCI to implement an appropriate content-protection method based on the CCI level they receive.

The software components responsible for implementing content protection have some control over the output devices on various consumer equipment (VCRs and digital recording devices) and on service provider equipment (DHCTs, CableCARD modules, or tru2way™ hosts). Because each output device, or **output port**, performs a unique function and resides on equipment manufactured by diverse vendors, the industry uses a variety of content-protection methods to meet the specifications of a particular output port.

**Note:** To determine the versions of client software and PowerTV® OS that support content protection, contact Cisco Services.

As the following broad examples show, user impact varies according to the output port to which a subscriber connects when attempting to record content and how the program content is protected:

- **Analog recording:** When subscribers attempt to view a content-protected program that was sent from an analog composite port to an analog VCR, Macrovision® technology will distort the program so that it will be unviewable.
- **Digital recording:** When subscribers attempt to view a content-protected program that was sent from a digital output port, the digital recording device that receives the content will behave as required based on the content-protection methods that the port uses.

**Important:** CCI is delivered in the ECM for a program. As a result, it may be applied to any **encrypted** source. However, it cannot be applied to a **clear** source because clear sources do not require ECMs.

## Who Determines If Program Content Can Be Copied?

Content providers determine the extent to which their program can be copied, subject in the United States to the Federal Communications Commission (FCC) Encoding Rules. Service providers can then configure the CCI data for each source, based on contractual agreements with content owners and applicable FCC rules.

## What Limitations Are Placed On Content Protection?

In the United States, the FCC sets the policy for protecting program content. Outside the United States, service providers should consult with content providers and local regulatory agencies. To change the protection settings, contact Cisco Services.

## Do Content Providers Have Other Protection Setting Options?

Yes, a content provider has the option of using a less restrictive protection setting. The content provider and service provider usually work together to determine the protection setting for specific program content.

## Content Protection for Our DHCTs and CableCard Modules

The following tables give an overview of the types of content protection supported by our DHCTs and CableCARD modules.

**Important:** These tables do not address the specific client and OS software versions required to activate or enable content protection features. For the most recent information on software versions that support content-protection features, contact Cisco Services.

### Digital Output Content Protection

| Description | Support |
|---|---|
| **DTCP** (Digital Transmission Content Protection) - Protects compressed MPEG content transmitted over the 1394 port | DHCTs with 1394 ports |
| **HDCP** (High-bandwidth Digital Content Protection) - Protects uncompressed digital content transmitted through DVI or HDMI™ ports. | DHCTs with DVI or HDMI ports |
| **DFAST** (Dynamic Feedback Arrangement Scrambling Technique) - Protects the physical data interface between a CableCARD module and its host. The CableCARD module performs conditional access (CA) decryption and then re-encrypts the stream using DFAST. | CableCARD modules |

### Analog Output Content Protection

| Description | Support |
|---|---|
| **Macrovision** - Discourages VCR recording of composite and RF analog outputs by changing information in the vertical and horizontal blanking intervals. When Macrovision-encoded outputs are recorded, the recording is distorted on playback. | DHCTs with analog outputs |
| **CIT** (Constrained Image Trigger) - Reduces the effective resolution that is less than 520k pixels. This is accomplished by band-limiting the video, rather than shrinking the image.<br>Cable service providers may enable image constraint by asserting the CIT bit (in CCI). This reduces the quality of recordings made on the component analog output. | HD DHCTs |

### Removable Media Content Protection

| Description | Support |
|---|---|
| **CPRM** (Content Protection for Recordable Media) - Securely binds the recording to the media so that copies are rendered unplayable. Used for DVD mass distribution and manufacture. | DHCTs with DVD drives |
| **CPPM** (Content Protection for Pre-recorded Media) - Essentially the same as CPRM, but CPRM is for DVD mass distribution and manufacture. | |
| **CSS** (Content Scrambling System) - Scrambling method currently used for most commercial DVDs. | |

### Digital Output Content Protection

| Description | Support |
|---|---|
| **DTCP** (Digital Transmission Content Protection) - Protects compressed MPEG content transmitted over the 1394 port | DHCTs with 1394 ports |
| **HDCP** (High-bandwidth Digital Content Protection) - Protects uncompressed digital content transmitted through DVI or HDMI™ ports. | DHCTs with DVI or HDMI ports |
| **DFAST** (Dynamic Feedback Arrangement Scrambling Technique) - Protects the physical data interface between a CableCARD module and its host. The CableCARD module performs conditional access (CA) decryption and then re-encrypts the stream using DFAST. | CableCARD modules |

### Analog Output Content Protection

| Description | Support |
|---|---|
| **Macrovision** - Discourages VCR recording of composite and RF analog outputs by changing information in the vertical and horizontal blanking intervals. When Macrovision-encoded outputs are recorded, the recording is distorted on playback. | DHCTs with analog outputs |
| **CIT** (Constrained Image Trigger) - Reduces the effective resolution that is less than 520k pixels. This is accomplished by band-limiting the video, rather than shrinking the image.<br><br>Cable service providers may enable image constraint by asserting the CIT bit (in CCI). This reduces the quality of recordings made on the component analog output. | HD DHCTs |

## Content Protection for Our DHCTs and CableCard Modules

The following tables give an overview of the types of content protection supported by our DHCTs and CableCARD modules.

**Important:** These tables do not address the specific client and OS software versions required to activate or enable content protection features. For the most recent information on software versions that support content-protection features, contact Cisco Services.

### Digital Output Content Protection

| Description | Support |
|---|---|
| **DTCP** (Digital Transmission Content Protection) - Protects compressed MPEG content transmitted over the 1394 port | DHCTs with 1394 ports |
| **HDCP** (High-bandwidth Digital Content Protection) - Protects uncompressed digital content transmitted through DVI or HDMI™ ports. | DHCTs with DVI or HDMI ports |
| **DFAST** (Dynamic Feedback Arrangement Scrambling Technique) - Protects the physical data interface between a CableCARD module and its host. The CableCARD module performs conditional access (CA) decryption and then re-encrypts the stream using DFAST. | CableCARD modules |

### Analog Output Content Protection

| Description | Support |
|---|---|
| **Macrovision** - Discourages VCR recording of composite and RF analog outputs by changing information in the vertical and horizontal blanking intervals. When Macrovision-encoded outputs are recorded, the recording is distorted on playback. | DHCTs with analog outputs |
| **CIT** (Constrained Image Trigger) - Reduces the effective resolution that is less than 520k pixels. This is accomplished by band-limiting the video, rather than shrinking the image.<br>Cable service providers may enable image constraint by asserting the CIT bit (in CCI). This reduces the quality of recordings made on the component analog output. | HD DHCTs |

### Removable Media Content Protection

| Description | Support |
|---|---|
| **CPRM** (Content Protection for Recordable Media) - Securely binds the recording to the media so that copies are rendered unplayable. Used for DVD mass distribution and manufacture. | DHCTs with DVD drives |
| **CPPM** (Content Protection for Pre-recorded Media) - Essentially the same as CPRM, but CPRM is for DVD mass distribution and manufacture. | |
| **CSS** (Content Scrambling System) - Scrambling method currently used for most commercial DVDs. | |

## CCI Levels

CCI is delivered in the Entitlement Control Message (ECM) for a program and describes the level of content protection that should be applied to the content. Based on the level that is indicated, software components that have some control over output devices on audiovisual equipment implement a content-protection method that meets the specifications of a particular output device.

**Note:** For a more complete discussion of CCI, see Enabling Content Protection for Broadcast Programming Configuration Guide (part number 4005893). To obtain a copy of this publication, see Printed Resources.

CCI data consists of 8 bits, each with the following specific functions:

- **2 EMI bits**. The Encryption Mode Indicator (EMI) digital copy control bits affect the DTCP content-protection method for the 1394 port and, depending on policy settings, may affect the HDCP content- protection method for the DVI/HDMI port. The EMI bits mark encrypted digital content as one of the following:
  - Do Not Copy
  - Copy Once
  - Copy Freely
- **2 APS bits**. The Analog Protection System (APS) bits affect composite analog outputs. The APS bits indicate how the circuit providing Macrovision content-protection is to be driven:
  - Macrovision circuit disabled
  - Macrovision circuit enabled (Automatic Gain Control Process On, 2 Line Split Burst On)
- **1 CIT bit**. The Constrained Image Trigger (CIT) bit affects only the high-definition (HD) YPbPr (component) analog output. The CIT bit determines how the HD YPbPr (component) analog output may function:
  - Output at full HD resolution
  - Reduce effective resolution to less than 520,000 pixels (image constraint)
- **3 reserved bits**

## Content Protection Methods

Because each output device, or output port, on a DHCT or other audiovisual device performs a unique function and resides on equipment manufactured by diverse vendors, the industry uses a variety of content-protection methods to meet the specifications of a particular output port.

### Protection From Unauthorized Copying of Content

DHCTs, CableCARD modules, and OpenCable hosts use the CCI in the content as well as data embedded in the vertical blanking interval (VBI) and Extended Data Services (XDS) to determine how and when to apply the following forms of content protection:

- **Macrovision** is used to protect content that is output on analog composite ports. Macrovision modifies the NTSC signal that is output on analog composite ports to inhibit recording onto a VCR. DBDS components and subsystems are capable of activating the Macrovision content-protection system on digital sources. This capability enables cable system providers to inhibit copying of digital PPV and digital VOD content through the analog outputs (RF, S-Video, or composite) of a DHCT. Note that this method does not affect analog YPbPr component outputs, but only analog composite ports.
- **Digital Transmission Content Protection (DTCP)** protects content that is output on the 1394 port from being recorded, although its use is not restricted to 1394. Unless content is marked "Copy Freely," the stream is encrypted on this port and content is marked with the appropriate content-protection setting (either "Copy One Generation" or "Copy Never.") Content can be encrypted and be set to "Copy Freely."
- **Copy Generation Management System/Analog (CGMS/A)** protects analog outputs from being recorded to devices such as DVD recorders and digital VCRs. The DHCT may receive CGMS/A in analog content as VBI data. The DHCT may also receive CGMS/A in digital content as embedded XDS data. The DHCT has the capability to output CGMS/A information on the composite and component analog outputs. CGMS/A data is copied from the source content to the appropriate VBI line. When analog content is encoded and recorded, CGMS/A settings are restored in a secure manner along with the content and restored on playback.

### Protection From Content Snooping

In addition to the content-protection methods listed above, which protect against unauthorized copying of content, the following methods are used to protect unauthorized devices from trying to obtain information ( **snooping**).

- **High-bandwidth Digital Content Protection (HDCP)** protects content that is output on the Digital Visual Interface/High-Definition Multimedia Interface™ (DVI/HDMI™) port. HDCP encrypts the high-value content, which audiovisual devices output through a DVI/HDMI port.
- **CableCARD modules** provide content protection for decrypted content. To prevent devices from "snooping" on the CableCARD/Host interface (PCMCIA bus), the content is re-encrypted using Dynamic Feedback Arrangement Scrambling Technique (DFAST). This technique "re-scrambles" the bits of a program for hand-off to a host device, such as a TV. You can revoke recording privileges for a host if you believe the host has been compromised.

**Note:** The camPsm process uses Global Broadcast Authorization Messages (GBAMs) to control various types of content protection. If the environment variable CC_DATA_FILE is not set when camPsm starts, the system creates the file copyControlParams.inf for you with the default values. If the variable is set to point to a specific file, the configuration values in that file will be used. For more information on the CC_DATA_FILE, see Default Behavior of DHCTs That Support CCI.

### Protection From Unauthorized Copying of Content

DHCTs, CableCARD modules, and OpenCable hosts use the CCI in the content as well as data embedded in the vertical blanking interval (VBI) and Extended Data Services (XDS) to determine how and when to apply the following forms of content protection:

- **Macrovision** is used to protect content that is output on analog composite ports. Macrovision modifies the NTSC signal that is output on analog composite ports to inhibit recording onto a VCR. DBDS components and subsystems are capable of activating the Macrovision content-protection system on digital sources. This capability enables cable system providers to inhibit copying of digital PPV and digital VOD content through the analog outputs (RF, S-Video, or composite) of a DHCT. Note that this method does not affect analog YPbPr component outputs, but only analog composite ports.
- **Digital Transmission Content Protection (DTCP)** protects content that is output on the 1394 port from being recorded, although its use is not restricted to 1394. Unless content is marked "Copy Freely," the stream is encrypted on this port and content is marked with the appropriate content-protection setting (either "Copy One Generation" or "Copy Never.") Content can be encrypted and be set to "Copy Freely."
- **Copy Generation Management System/Analog (CGMS/A)** protects analog outputs from being recorded to devices such as DVD recorders and digital VCRs. The DHCT may receive CGMS/A in analog content as VBI data. The DHCT may also receive CGMS/A in digital content as embedded XDS data. The DHCT has the capability to output CGMS/A information on the composite and component analog outputs. CGMS/A data is copied from the source content to the appropriate VBI line. When analog content is encoded and recorded, CGMS/A settings are restored in a secure manner along with the content and restored on playback.

## Content Protection Methods

Because each output device, or output port, on a DHCT or other audiovisual device performs a unique function and resides on equipment manufactured by diverse vendors, the industry uses a variety of content-protection methods to meet the specifications of a particular output port.

### Protection From Unauthorized Copying of Content

DHCTs, CableCARD modules, and OpenCable hosts use the CCI in the content as well as data embedded in the vertical blanking interval (VBI) and Extended Data Services (XDS) to determine how and when to apply the following forms of content protection:

- **Macrovision** is used to protect content that is output on analog composite ports. Macrovision modifies the NTSC signal that is output on analog composite ports to inhibit recording onto a VCR. DBDS components and subsystems are capable of activating the Macrovision content-protection system on digital sources. This capability enables cable system providers to inhibit copying of digital PPV and digital VOD content through the analog outputs (RF, S-Video, or composite) of a DHCT. Note that this method does not affect analog YPbPr component outputs, but only analog composite ports.
- **Digital Transmission Content Protection (DTCP)** protects content that is output on the 1394 port from being recorded, although its use is not restricted to 1394. Unless content is marked "Copy Freely," the stream is encrypted on this port and content is marked with the appropriate content-protection setting (either "Copy One Generation" or "Copy Never.") Content can be encrypted and be set to "Copy Freely."
- **Copy Generation Management System/Analog (CGMS/A)** protects analog outputs from being recorded to devices such as DVD recorders and digital VCRs. The DHCT may receive CGMS/A in analog content as VBI data. The DHCT may also receive CGMS/A in digital content as embedded XDS data. The DHCT has the capability to output CGMS/A information on the composite and component analog outputs. CGMS/A data is copied from the source content to the appropriate VBI line. When analog content is encoded and recorded, CGMS/A settings are restored in a secure manner along with the content and restored on playback.

### Protection From Content Snooping

In addition to the content-protection methods listed above, which protect against unauthorized copying of content, the following methods are used to protect unauthorized devices from trying to obtain information ( **snooping**).

- **High-bandwidth Digital Content Protection (HDCP)** protects content that is output on the Digital Visual Interface/High-Definition Multimedia Interface™ (DVI/HDMI™) port. HDCP encrypts the high-value content, which audiovisual devices output through a DVI/HDMI port.
- **CableCARD modules** provide content protection for decrypted content. To prevent devices from "snooping" on the CableCARD/Host interface (PCMCIA bus), the content is re-encrypted using Dynamic Feedback Arrangement Scrambling Technique (DFAST). This technique "re-scrambles" the bits of a program for hand-off to a host device, such as a TV. You can revoke recording privileges for a host if you believe the host has been compromised.

**Note:** The camPsm process uses Global Broadcast Authorization Messages (GBAMs) to control various types of content protection. If the environment variable CC_DATA_FILE is not set when camPsm starts, the system creates the file copyControlParams.inf for you with the default values. If the variable is set to point to a specific file, the configuration values in that file will be used. For more information on the CC_DATA_FILE, see Default Behavior of DHCTs That Support CCI.

## Default Behavior of DHCTs That Support CCI

The camPSM process uses Global Broadcast Authorization Messages (GBAMs) to control various types of content protection. If the environment variable CC_DATA_FILE is not set when camPsm starts, the system will create the copyControlParams.inf file for you with default values. On the other hand, if the environmental variable is set to point to a specific file, the configuration values in that file is used.

The system-created copyControlParams.inf file contains the following default configurations:

- The DVI/HDMI default configuration always uses HDCP authentication and encryption for the DVI/HDMI port and blocks the port when authentication fails.
- The YPbPr default configuration constrains the image sent to the YPbPr output when the CIT bit is set.
- The 1394 port is enabled by default if the connected device supports DTCP; otherwise, the 1394 port is blocked.
- Composite outputs use Macrovision according to the setting indicated in APS bits for encrypted digital content.

### Do the Default Settings Fit Your System Requirements?

A provision in the software allows for changes to the system-created default configuration. If the default settings are not adequate for your system's requirements, Contact Cisco Services for information regarding other support configurations. Cisco Services can provide you with instructions on how to enable alternate configurations that are suitable for your system.

### Previous Content-Control Methods

Depending on your system configuration, you may need to change some of the following settings so that they do not conflict with software that supports content-protection policy settings.

## _DVI SAM Service

Prior to the release of Service Pack 2 for SR 2.2 and SR 3.2, you may have set up a _DVI SAM service and package to turn off HDCP on a DVI port. Because the _DVI SAM service cannot be used in conjunction with the software that supports content-protection policy settings, you are required to delete this service.

After the installation of Service Pack 2 for SR 2.2 and SR 3.2, the HDCP setting will be controlled globally based on the settings in the copyControlParams.inf file. If subscribers connect a monitor that does not support HDCP to the DVI port, they will see an HDCP barker.

Because you will no longer be using a package to control the DVI port or the HDCP function, delete the package that was used for this purpose. However, if the package is used to control other DHCT functions or services, it should not be deleted.

**Note:** For instructions on deleting the _DVI SAM Service, see Delete the _DVI SAM Service.

## no_vod_cci File Flag

To accommodate earlier versions of VOD or xOD that did not support setting the content-protection flag, you could enable content protection for all VOD or xOD services by adding a file called no_vod_cci to the BFS. If this file is on the BFS, the DHCT automatically activates content protection on the 1394 output for any VOD or xOD sessions. If you want the DHCT to protect content based on the settings provided by the VOD or xOD application, you must remove this file from the BFS. For assistance, see Protect On-Demand Content From Unauthorized Copying.

However, if your VOD provider is not able to set the content protection settings as required, you can globally enable content-protection for VOD by adding the no_vod_cci file to the BFS. For assistance, see Protect On-Demand Content From Unauthorized Copying.

### Do the Default Settings Fit Your System Requirements?

A provision in the software allows for changes to the system-created default configuration. If the default settings are not adequate for your system's requirements, Contact Cisco Services for information regarding other support configurations. Cisco Services can provide you with instructions on how to enable alternate configurations that are suitable for your system.

## Default Behavior of DHCTs That Support CCI

The camPSM process uses Global Broadcast Authorization Messages (GBAMs) to control various types of content protection. If the environment variable CC_DATA_FILE is not set when camPsm starts, the system will create the copyControlParams.inf file for you with default values. On the other hand, if the environmental variable is set to point to a specific file, the configuration values in that file is used.

The system-created copyControlParams.inf file contains the following default configurations:

- The DVI/HDMI default configuration always uses HDCP authentication and encryption for the DVI/HDMI port and blocks the port when authentication fails.
- The YPbPr default configuration constrains the image sent to the YPbPr output when the CIT bit is set.
- The 1394 port is enabled by default if the connected device supports DTCP; otherwise, the 1394 port is blocked.
- Composite outputs use Macrovision according to the setting indicated in APS bits for encrypted digital content.

### Do the Default Settings Fit Your System Requirements?

A provision in the software allows for changes to the system-created default configuration. If the default settings are not adequate for your system's requirements, Contact Cisco Services for information regarding other support configurations. Cisco Services can provide you with instructions on how to enable alternate configurations that are suitable for your system.

### Previous Content-Control Methods

Depending on your system configuration, you may need to change some of the following settings so that they do not conflict with software that supports content-protection policy settings.

## _DVI SAM Service

Prior to the release of Service Pack 2 for SR 2.2 and SR 3.2, you may have set up a _DVI SAM service and package to turn off HDCP on a DVI port. Because the _DVI SAM service cannot be used in conjunction with the software that supports content-protection policy settings, you are required to delete this service.

After the installation of Service Pack 2 for SR 2.2 and SR 3.2, the HDCP setting will be controlled globally based on the settings in the copyControlParams.inf file. If subscribers connect a monitor that does not support HDCP to the DVI port, they will see an HDCP barker.

Because you will no longer be using a package to control the DVI port or the HDCP function, delete the package that was used for this purpose. However, if the package is used to control other DHCT functions or services, it should not be deleted.

**Note:** For instructions on deleting the _DVI SAM Service, see Delete the _DVI SAM Service.

## no_vod_cci File Flag

To accommodate earlier versions of VOD or xOD that did not support setting the content-protection flag, you could enable content protection for all VOD or xOD services by adding a file called no_vod_cci to the BFS. If this file is on the BFS, the DHCT automatically activates content protection on the 1394 output for any VOD or xOD sessions. If you want the DHCT to protect content based on the settings provided by the VOD or xOD application, you must remove this file from the BFS. For assistance, see Protect On-Demand Content From Unauthorized Copying.

However, if your VOD provider is not able to set the content protection settings as required, you can globally enable content-protection for VOD by adding the no_vod_cci file to the BFS. For assistance, see Protect On-Demand Content From Unauthorized Copying.

# Daylight Saving Time Rules

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST**

From the Configure Daylight Saving Time Rules window, you can create, change, and delete daylight saving time (DST) rules that can be used by DHCTs in different DST zones. Setting up the right DST rules enables the DHCTs in your system to automatically adjust to changes in DST observance. After creating a rule for a particular zone, apply the rule to one or more hubs. DHCTs will then use the rule of the hub to which they belong.

**Important:**

- To enable the DHCTs in your system to adjust for DST, you must first create a DST rule for a particular zone and then you must apply the correct rule to each hub; otherwise, unexpected results can occur.
- We strongly recommend that you configure the DST Rules more than 30 days before the time change. The DNCS will broadcast the DST rules to the DHCTs within 30 days of the DST start and end times that you specify in the DST Rules window. However, you can add DST rules as necessary at any time. If you add DST rules within the 30-day window, the DNCS will broadcast the rules to the set-tops immediately.

**Note:** If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to Modify a Hub.

For additional information on this feature, including the DHCT software versions that support this feature, refer to the Daylight Saving Time Configuration Guide for an RF Network (part number 749233). To obtain a copy of this publication, see Printed Resources.

## What do you want to do?

- Learn about the Default DST Rules
- View a description of the fields in this window
- View a DST rule
- Create a DST rule
- Change a DST rule
- Delete a DST rule
- Close the Configure Daylight Saving Time Rules window by clicking **Exit**
- Display help for DST rules tasks by clicking **Help**

## Default DST Rules

When you open the Set Daylight Savings Time Rules window for the first time, it will be blank. If no data appears in the fields, a DST rule has not been created and DHCTs use their default DST rules (the time moves forward 1 hour on the first Sunday in April, and back 1 hour on the last Sunday in October).

## Daylight Saving Time Rules Settings

Use the following fields when you manage DST rule in the DNCS.

| Field | Description |
|---|---|
| **Note:** Settings in the first area of the window define how DST is observed in a particular DST Zone ID. | |
| Daylight Saving Time Zone ID | The IDs of the DST zones that the DNCS uses:<br>▪**US** - United States of America.<br>▪**UK** - United Kingdom of Great Britain and Northern Ireland.<br>▪**Europe** - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland.<br>▪**Australia** - All states and territories in the Commonwealth of Australia.<br>▪**Local DST Zone** - Used for all other countries and territories, except as noted below. |
| **What if my country or territory isn't listed?**<br><br>If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK ), select that territory from the DST Zone ID list. For example, if you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province.<br><br>If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID. | |
| Daylight Saving Time Offset (minutes) | The time shift (in minutes) relative to standard time.<br>**Example:** If daylight saving time is one hour ahead, you would enter **60** in this field. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID.<br>This field accepts any positive number from 0 to 1439. |
| Effective Year | The year the DST rule becomes effective |
| Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied in that DST Zone ID.<br><br>**Important:** All DST rules except those created for the Australia Zone ID and Local Zone ID must be applied to the same year. | |
| Start: Month | The month the DST rule becomes effective |
| Start: Day | The day the DST rule becomes effective |
| Start: Day Rank in Month | The day of the month that the DST rule becomes effective.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Start: Hour | The hour the DST rule becomes effective. |
| Start: Minute | The number of minutes after the Start Hour that the DST rule becomes effective. |
| End: Month | The month the DST rule ends. |
| End: Day | The day the DST rule ends. |

| | |
|---|---|
| End: Day Rank in Month | The day of the month that the DST rule ends.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| End: Hour | The hour the DST rule ends. |
| End: Minute | The number of minutes after the End Hour that the DST rule ends. |
| Settings in the **Broadcast Start** area of the window define when the DNCS broadcasts this rule to DHCTs that reside in the DST Zone ID.<br>**Important:** Broadcast Start Time can begin no more than 30 days before the start of the DST rule. | |
| Year | The year that the DNCS begins broadcasting this rule to DHCTs. |
| Month | The month that the DNCS begins broadcasting this rule to DHCTs. |
| Day | The day that the DNCS begins broadcasting this rule to DHCTs. |
| Day Rank in Month | The day of the month that the DNCS begins broadcasting this rule to DHCTs.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Hour | The hour that the DNCS begins broadcasting this rule to DHCTs |
| Minute | The number of minutes after the Start Hour that the DNCS begins broadcasting this rule to DHCTs |

## View a DST Rule

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST > [Select DST Zone ID]**

By displaying a DST rule in the Configure Daylight Saving Time Rules window, you can quickly verify that the settings are correct.

**Note:** If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to Modify a Hub.

Complete these steps to view the settings for a DST rule.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Configure Daylight Saving Time Rules window opens.
4. Click the **Daylight Saving Time Zone ID** arrow and select the ID of the zone whose settings you wish to view. The window updates and displays the settings of the DST Zone ID that you selected.

   **Note:** If no data appears in the fields, a rule has not been created for this DST Zone ID, and DHCTs in this zone use their default DST rules. To create a rule for this DST Zone ID, go to Create a DST Rule.

5. To view the settings of another DST rule, repeat step 4. For an explanation of the DST fields, see Daylight Saving Time Rules Settings.

Use the following fields when you manage DST rule in the DNCS.

| Field | Description |
|---|---|
| **Note:** Settings in the first area of the window define how DST is observed in a particular DST Zone ID. | |
| Daylight Saving Time Zone ID | The IDs of the DST zones that the DNCS uses:<br>▪ **US** - United States of America.<br>▪ **UK** - United Kingdom of Great Britain and Northern Ireland.<br>▪ **Europe** - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland.<br>▪ **Australia** - All states and territories in the Commonwealth of Australia.<br>▪ **Local DST Zone** - Used for all other countries and territories, except as noted below. |

**What if my country or territory isn't listed?**

If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK ), select that territory from the DST Zone ID list. For example, if you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province.

If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID.

| | |
|---|---|
| Daylight Saving Time Offset (minutes) | The time shift (in minutes) relative to standard time.<br>**Example:** If daylight saving time is one hour ahead, you would enter **60** in this field. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID.<br>This field accepts any positive number from 0 to 1439. |
| Effective Year | The year the DST rule becomes effective |
| Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied in that DST Zone ID.<br>**Important:** All DST rules except those created for the Australia Zone ID and Local Zone ID must be applied to the same year. | |
| Start: Month | The month the DST rule becomes effective |
| Start: Day | The day the DST rule becomes effective |
| Start: Day Rank in Month | The day of the month that the DST rule becomes effective.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Start: Hour | The hour the DST rule becomes effective. |
| Start: Minute | The number of minutes after the Start Hour that the DST rule becomes effective. |
| End: Month | The month the DST rule ends. |
| End: Day | The day the DST rule ends. |
| End: Day Rank in Month | The day of the month that the DST rule ends.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| End: Hour | The hour the DST rule ends. |
| End: Minute | The number of minutes after the End Hour that the DST rule ends. |
| Settings in the **Broadcast Start** area of the window define when the DNCS broadcasts this rule to DHCTs that reside in the DST Zone ID.<br>**Important:** Broadcast Start Time can begin no more than 30 days before the start of the DST rule. | |
| Year | The year that the DNCS begins broadcasting this rule to DHCTs. |
| Month | The month that the DNCS begins broadcasting this rule to DHCTs. |
| Day | The day that the DNCS begins broadcasting this rule to DHCTs. |
| Day Rank in Month | The day of the month that the DNCS begins broadcasting this rule to DHCTs.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Hour | The hour that the DNCS begins broadcasting this rule to DHCTs |
| Minute | The number of minutes after the Start Hour that the DNCS begins broadcasting this rule to DHCTs |

6. To close the Configure Daylight Saving Time Rules window, click **Exit**.

## Create a DST Rule

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST > [Configure Settings] > Save**

DST rules are typically created during a system upgrade or installation. However, as your system changes you may need to create new rules. The instructions on this page describe how create a DST rule and ensure that it is used by the appropriate hubs.

**Note:** If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to Modifying a Hub.

**Important:** Make sure that Time Zone and DST Zone ID settings are set correctly in the Hub Summary window. These settings must be correct because the DNCS uses them to broadcast DST data to DHCTs in hubs.

### Creating a DST Rule

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Configure Daylight Saving Time Rules window opens.
4. Click the **Daylight Saving Time Zone ID** arrow and select the Zone ID for the rule that you want to create.

   **Note:** You must select one of the predefined Zone IDs (US, Europe, Australia, UK, or Local DST Zone) to create a DST Rule.

5. Complete the fields on the screen as described in Daylight Saving Time Rules Settings.

   Use the following fields when you manage DST rule in the DNCS.

| Field | Description |
|---|---|
| **Note:** Settings in the first area of the window define how DST is observed in a particular DST Zone ID. | |
| Daylight Saving Time Zone ID | The IDs of the DST zones that the DNCS uses:<br>▪ **US** - United States of America.<br>▪ **UK** - United Kingdom of Great Britain and Northern Ireland.<br>▪ **Europe** - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland.<br>▪ **Australia** - All states and territories in the Commonwealth of Australia.<br>▪ **Local DST Zone** - Used for all other countries and territories, except as noted below. |

**What if my country or territory isn't listed?**

If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK ), select that territory from the DST Zone ID list. For example, if you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province.

| | |
|---|---|
| If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID. | |
| Daylight Saving Time Offset (minutes) | The time shift (in minutes) relative to standard time.<br>**Example:** If daylight saving time is one hour ahead, you would enter **60** in this field. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID.<br>This field accepts any positive number from 0 to 1439. |
| Effective Year | The year the DST rule becomes effective |
| Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied in that DST Zone ID.<br>**Important:** All DST rules except those created for the Australia Zone ID and Local Zone ID must be applied to the same year. | |
| Start: Month | The month the DST rule becomes effective |
| Start: Day | The day the DST rule becomes effective |
| Start: Day Rank in Month | The day of the month that the DST rule becomes effective.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Start: Hour | The hour the DST rule becomes effective. |
| Start: Minute | The number of minutes after the Start Hour that the DST rule becomes effective. |
| End: Month | The month the DST rule ends. |
| End: Day | The day the DST rule ends. |
| End: Day Rank in Month | The day of the month that the DST rule ends.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| End: Hour | The hour the DST rule ends. |
| End: Minute | The number of minutes after the End Hour that the DST rule ends. |
| Settings in the **Broadcast Start** area of the window define when the DNCS broadcasts this rule to DHCTs that reside in the DST Zone ID.<br>**Important:** Broadcast Start Time can begin no more than 30 days before the start of the DST rule. | |
| Year | The year that the DNCS begins broadcasting this rule to DHCTs. |
| Month | The month that the DNCS begins broadcasting this rule to DHCTs. |
| Day | The day that the DNCS begins broadcasting this rule to DHCTs. |
| Day Rank in Month | The day of the month that the DNCS begins broadcasting this rule to DHCTs.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Hour | The hour that the DNCS begins broadcasting this rule to DHCTs |
| Minute | The number of minutes after the Start Hour that the DNCS begins broadcasting this rule to DHCTs |

**Important:** The Broadcast Start Time can begin no more than 30 days before the start of the DST rule.

6. Click **Save**. A message window opens and informs you that the DNCS database will be updated with the DST data you have selected.

7. Click **OK**. The message window closes and the DNCS database is updated with your changes. DHCTs receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a DHCT causes it to update immediately with DST data.

8. Display the Hub Summary window (**DNCS tab > Network Element Provisioning tab > Hub)** and confirm that the correct settings are selected for **Time Zone** and **DST Zone ID** fields. If necessary, change these settings. For assistance, go to Modifying a Hub.

9. Do you need to create another DST rule?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **Exit** to close the Configure Daylight Saving Time Rules window.

## Create a DST Rule

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST > [Configure Settings] > Save**

DST rules are typically created during a system upgrade or installation. However, as your system changes you may need to create new rules. The instructions on this page describe how create a DST rule and ensure that it is used by the appropriate hubs.

**Note:** If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to Modifying a Hub.

**Important:** Make sure that Time Zone and DST Zone ID settings are set correctly in the Hub Summary window. These settings must be correct because the DNCS uses them to broadcast DST data to DHCTs in hubs.

### Creating a DST Rule

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Configure Daylight Saving Time Rules window opens.
4. Click the **Daylight Saving Time Zone ID** arrow and select the Zone ID for the rule that you want to create.

   **Note:** You must select one of the predefined Zone IDs (US, Europe, Australia, UK, or Local DST Zone) to create a DST Rule.

5. Complete the fields on the screen as described in Daylight Saving Time Rules Settings.

   Use the following fields when you manage DST rule in the DNCS.

| Field | Description |
|---|---|
| **Note:** Settings in the first area of the window define how DST is observed in a particular DST Zone ID. | |
| Daylight Saving Time Zone ID | The IDs of the DST zones that the DNCS uses:<br>▪ **US** - United States of America.<br>▪ **UK** - United Kingdom of Great Britain and Northern Ireland.<br>▪ **Europe** - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland.<br>▪ **Australia** - All states and territories in the Commonwealth of Australia.<br>▪ **Local DST Zone** - Used for all other countries and territories, except as noted below. |

**What if my country or territory isn't listed?**

If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK ), select that territory from the DST Zone ID list. For example, if you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province.

| | |
|---|---|
| If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID. | |
| Daylight Saving Time Offset (minutes) | The time shift (in minutes) relative to standard time.<br>**Example:** If daylight saving time is one hour ahead, you would enter **60** in this field. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID.<br>This field accepts any positive number from 0 to 1439. |
| Effective Year | The year the DST rule becomes effective |
| Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied in that DST Zone ID.<br>**Important:** All DST rules except those created for the Australia Zone ID and Local Zone ID must be applied to the same year. | |
| Start: Month | The month the DST rule becomes effective |
| Start: Day | The day the DST rule becomes effective |
| Start: Day Rank in Month | The day of the month that the DST rule becomes effective.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Start: Hour | The hour the DST rule becomes effective. |
| Start: Minute | The number of minutes after the Start Hour that the DST rule becomes effective. |
| End: Month | The month the DST rule ends. |
| End: Day | The day the DST rule ends. |
| End: Day Rank in Month | The day of the month that the DST rule ends.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| End: Hour | The hour the DST rule ends. |
| End: Minute | The number of minutes after the End Hour that the DST rule ends. |
| Settings in the **Broadcast Start** area of the window define when the DNCS broadcasts this rule to DHCTs that reside in the DST Zone ID.<br>**Important:** Broadcast Start Time can begin no more than 30 days before the start of the DST rule. | |
| Year | The year that the DNCS begins broadcasting this rule to DHCTs. |
| Month | The month that the DNCS begins broadcasting this rule to DHCTs. |
| Day | The day that the DNCS begins broadcasting this rule to DHCTs. |
| Day Rank in Month | The day of the month that the DNCS begins broadcasting this rule to DHCTs.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Hour | The hour that the DNCS begins broadcasting this rule to DHCTs |
| Minute | The number of minutes after the Start Hour that the DNCS begins broadcasting this rule to DHCTs |

**Important:** The Broadcast Start Time can begin no more than 30 days before the start of the DST rule.

6. Click **Save**. A message window opens and informs you that the DNCS database will be updated with the DST data you have selected.

7. Click **OK**. The message window closes and the DNCS database is updated with your changes. DHCTs receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a DHCT causes it to update immediately with DST data.

8. Display the Hub Summary window (**DNCS tab > Network Element Provisioning tab > Hub)** and confirm that the correct settings are selected for **Time Zone** and **DST Zone ID** fields. If necessary, change these settings. For assistance, go to Modifying a Hub.

9. Do you need to create another DST rule?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **Exit** to close the Configure Daylight Saving Time Rules window.

## Change a DST Rule

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST > [Select Daylight Saving Time Zone ID] > [Change Desired Fields] > Save**

As your system changes, you may need to change a DST rule. Complete these steps to change a DST rule and ensure that it is used by the appropriate hubs.

**Important:** Make certain that Time Zone and DST Zone ID settings are set correctly in the Hub Summary window (**DNCS tab > Network Element Provisioning tab > Hub**). These settings must be correct because the DNCS uses them to broadcast DST data to DHCTs in hubs.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Configure Daylight Saving Time Rules window opens.
4. Is the rule that you want to change shown in the Configure Daylight Saving Time Rules window?
   - If **yes**, change the settings as described in Daylight Saving Time Rules Settings.

   Use the following fields when you manage DST rule in the DNCS.

| Field | Description |
|---|---|
| **Note:** Settings in the first area of the window define how DST is observed in a particular DST Zone ID. | |
| Daylight Saving Time Zone ID | The IDs of the DST zones that the DNCS uses:<br>▪ **US** - United States of America.<br>▪ **UK** - United Kingdom of Great Britain and Northern Ireland.<br>▪ **Europe** - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland.<br>▪ **Australia** - All states and territories in the Commonwealth of Australia.<br>▪ **Local DST Zone** - Used for all other countries and territories, except as noted below. |
| **What if my country or territory isn't listed?**<br><br>If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK ), select that territory from the DST Zone ID list. For example, if you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province.<br><br>If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID. | |
| Daylight Saving Time Offset (minutes) | The time shift (in minutes) relative to standard time.<br><br>**Example:** If daylight saving time is one hour ahead, you would enter **60** in this field. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID.<br><br>This field accepts any positive number from 0 to 1439. |

| | |
|---|---|
| Effective Year | The year the DST rule becomes effective |
| Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied in that DST Zone ID.<br>**Important:** All DST rules except those created for the Australia Zone ID and Local Zone ID must be applied to the same year. | |
| Start: Month | The month the DST rule becomes effective |
| Start: Day | The day the DST rule becomes effective |
| Start: Day Rank in Month | The day of the month that the DST rule becomes effective.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Start: Hour | The hour the DST rule becomes effective. |
| Start: Minute | The number of minutes after the Start Hour that the DST rule becomes effective. |
| End: Month | The month the DST rule ends. |
| End: Day | The day the DST rule ends. |
| End: Day Rank in Month | The day of the month that the DST rule ends.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| End: Hour | The hour the DST rule ends. |
| End: Minute | The number of minutes after the End Hour that the DST rule ends. |
| Settings in the **Broadcast Start** area of the window define when the DNCS broadcasts this rule to DHCTs that reside in the DST Zone ID.<br>**Important:** Broadcast Start Time can begin no more than 30 days before the start of the DST rule. | |
| Year | The year that the DNCS begins broadcasting this rule to DHCTs. |
| Month | The month that the DNCS begins broadcasting this rule to DHCTs. |
| Day | The day that the DNCS begins broadcasting this rule to DHCTs. |
| Day Rank in Month | The day of the month that the DNCS begins broadcasting this rule to DHCTs.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Hour | The hour that the DNCS begins broadcasting this rule to DHCTs |
| Minute | The number of minutes after the Start Hour that the DNCS begins broadcasting this rule to DHCTs |

**Important:** The Broadcast Start Time can begin no more than 30 days before the start of the DST rule.

- If **no**, display the rule whose settings you want to change. For help displaying a rule, go to View a DST Rule.

5. Click **Save**. A message window opens and informs you that the DNCS database will be updated with the DST data you have selected.

6. Click **OK**. The message window closes and the DNCS database is updated with your changes. DHCTs receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a DHCT causes it to update immediately with DST data.

7. Display the Hub Summary window and confirm that the correct settings are selected for **Time Zone** and **DST Zone ID** fields. For assistance, go to Modify a Hub.

8. Do you need to change the settings for another DST rule?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **Exit** to close the Configure Daylight Saving Time Rules window.

## Delete a DST Rule

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DST > [Select DST Zone ID] > Delete**

As your system changes, you may need to delete a DST rule.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Configure Daylight Saving Time Rules window opens.
4. Is the rule that you want to delete shown in the Configure Daylight Saving Time Rules window?
   - If **yes**, click **Delete**. A confirmation window opens.
   - If **no**, display the DST rule that you want to delete and then click **Delete**. A confirmation window opens.

   **Note:** Go to View a DST Rule for assistance displaying a rule.
5. Click **OK**. The DNCS removes the rule from the database and removes all settings from the fields in the window. DHCTs receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a DHCT causes it to update immediately with DST data.
6. Display the Hub Summary window and confirm that the correct settings are selected for **Time Zone** and **DST Zone ID** fields. For assistance, go to Modify a Hub.
7. Do you need to delete another DST rule?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Exit** to close the Configure Daylight Saving Time Rules window.

# Direct ASI

With Direct ASI, you have the ability to send Broadcast File System (BFS) data directly from the DNCS to your BFS QAM modulator. Or, if you are using a Regional Control System (RCS) you can send BFS data directly from an RNCS/LIONN at a remote site to the BFS QAM modulator at the remote site. Direct ASI simplifies your network by eliminating the need for a BFS BIG or for asynchronous transfer mode (ATM) permanent virtual circuits (PVCs).

## What do you want to do?

- View the requirements for supporting Direct ASI
- Learn about the settings for direct ASI

## Direct ASI Requirements

Support for Direct ASI requires the following:

- Installation of either SR 2.5 (or later) or SR 3.5 (or later)
- Installation of an ASI card on your DNCS.

**Note:** If you are using an RCS, each RNCS/LIONN leaves the factory with an ASI card. For this reason, an ASI card does not need to be installed in an RNCS/LIONN.

If your DBDS uses Direct ASI, Cisco Services engineers install the products listed above during the upgrade process and then configure your DNCS to support Direct ASI. Because engineers perform these tasks for you, you should not need to configure your DNCS for Direct ASI. However, the procedures in Set Up Direct ASI can help you gain an understanding of how the DNCS is configured to support Direct ASI. This knowledge may be helpful in monitoring and managing your DBDS.

## Direct ASI Settings

Use the following fields when you manage direct ASI in the DNCS:

- ASI Card Basic Parameter Settings
- ASI Card Connection Settings

### ASI Card Basic Parameter Settings

Use the following fields when you manage ASI cards in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend associated with the ASI card. |
| MPEG Source Name | The name of this MPEG source.<br>**Example: DNCS_ASI**, or, for a remote site, **RNCS1_ASI** or **LIONN1_AS**.<br>You can use up to 20 alphanumeric characters. |
| Device Type | The type of MPEG source you are adding.<br>Select **ASI** as the type of MPEG source you are adding.<br>If ASI does not appear in the list of device types, click in the **Device Type** field and enter **ASI**. |
| IP Address | The IP address for the ASI card.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address of the ASI card.<br>Type a dummy value (such as 12 zeros) for the MAC address of the ASI card. |

### ASI Card Connection Settings

Use the following fields when you manage connections for ASI cards.

| Field | Description |
|---|---|
| Port Number | The output port on the ASI card that is physically connected to the input port on the BFS QAM modulator.<br><br>We recommend that you start with zero (0). |
| Transport Stream ID | The transport stream of the MPEG source to the BFS QAM modulator.<br><br>**Important:** You will need this number when you set up the BFS QAM modulator. |
| Transport Protocol | The type of output that feeds the BFS QAM modulator.<br><br>Select **ASI** as the type of output that feeds the BFS QAM modulator. |

**Note:** When you set up the BFS QAM modulator that the ASI card connects to, the system will automatically complete the Connect To fields on this window.

## Set Up Direct ASI

The Direct ASI option allows you to send BFS data directly from the DNCS to a BFS QAM modulator. This simplifies your network by eliminating the need for a BFS BIG or for asynchronous transfer mode (ATM) permanent virtual circuits (PVCs).

Direct ASI allows a Regional Control System (RCS) to send BFS data directly from an RNCS/LIONN at a remote site to the BFS QAM modulator at the remote site.

## You Need to Know

Before You Begin

Before you begin, you must have your network map.

Also verify that your system meets the requirements for supporting Direct ASI. If you are unsure, view the Direct ASI Requirements.

Process Overview

The following steps describe how to configure a DNCS to support Direct ASI.

**Note:** Cisco Services engineers configure your DNCS to support Direct ASI when they upgrade your system. Because engineers perform these tasks for you, you should not need to configure your DNCS for Direct ASI. However, the procedures given here can help you understand how a DNCS is configured to support Direct ASI. This knowledge may be helpful in monitoring and managing your DBDS.

1. Add an MPEG BFS source for the ASI card in the DNCS.

**Note:** If you use an RCS, add an MPEG BFS source for the ASI card of each RNCS/LIONN in your system.

2. Add a BFS QAM modulator to receive the output of the ASI card, using the following procedure appropriate to your system:
   - If using an RCS, add a BFS QAM modulator to an RCS.
   - For systems other than RCS, add a BFS QAM modulator.

## Add an MPEG BFS Source

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > File > New**

**Important:** Follow this procedure only if your system uses the Direct ASI or RCS option. Direct ASI is required in an RCS.

If your network uses Direct ASI to send BFS data to DHCTs, the first step in setting up the elements that process system data for your network is to add an MPEG BFS source. This source represents the ASI card installed in the DNCS or RNCS/LIONN. In addition, if you are using the RCS option, you will also need to add an MPEG BFS source for each RNCS/LIONN in your network.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information, which should be noted on your network map:

- Name of the headend containing the ASI card
- A name that will identify each MPEG source as one that is used for the ASI card (We recommend that you use the name BFS_ASI.)
- The IP address for the ASI card installed in the DNCS (from your system administrator)
- Physical (MAC) address for the Ethernet port on the ASI control card that is being used to receive data from the DNCS
- Number identifying the output port on the ASI card that is physically connected to the input port on the BFS QAM modulator
- Number identifying the transport stream going from the MPEG source to the BFS QAM modulator

**Note:** If you are using an **RCS network**, you will need the information listed above for the ASI card on the DNCS and the ASI card on each RNCS/LIONN.

Process Overview

To add an MPEG BFS source for an ASI card, complete the following tasks.

1. Set up the basic parameters for the ASI card.
2. Set up the connection from the ASI card to the BFS QAM modulator.

### Related Topics

- Setting Up ASI Card Basic Parameters
- Setting Up ASI Card Connections

### Setting Up ASI Card Basic Parameters

The first step in adding an MPEG source for an ASI card is to set up the basic parameters for the card as described in the following steps.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click **File > New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in ASI Card Basic Parameter Settings.

   Use the following fields when you manage ASI cards in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend associated with the ASI card. |
| MPEG Source Name | The name of this MPEG source.<br>**Example: DNCS_ASI**, or, for a remote site, **RNCS1_ASI** or **LIONN1_AS**.<br>You can use up to 20 alphanumeric characters. |
| Device Type | The type of MPEG source you are adding.<br>Select **ASI** as the type of MPEG source you are adding.<br>If ASI does not appear in the list of device types, click in the **Device Type** field and enter **ASI**. |
| IP Address | The IP address for the ASI card.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address of the ASI card.<br>Type a dummy value (such as 12 zeros) for the MAC address of the ASI card. |

6. Click **Apply**. The system saves the basic parameters for this MPEG source in the DNCS database. The previously disabled Connectivity tab becomes available.
7. Your next step is to set up the connection from the MPEG source to the BFS modulator. Go to Setting Up ASI Card Connections.

### Setting Up ASI Card Connections

After you set up the basic parameters for the ASI card, complete these steps to set up the connections from the ASI card to the BFS QAM modulator.

1. On the Set Up MPEG source window, click the **Connectivity** tab. The Connectivity window opens.

   **Note:** Because no devices are connected yet, the illustration field is empty.

2. Click **Create Port**. The Port Number Prompt window opens.
3. Complete the fields on the screen as described in ASI Card Connection Settings.

   Use the following fields when you manage connections for ASI cards.

| Field | Description |
|---|---|
| Port Number | The output port on the ASI card that is physically connected to the input port on the BFS QAM modulator.<br>We recommend that you start with zero (0). |
| Transport Stream ID | The transport stream of the MPEG source to the BFS QAM modulator.<br>**Important:** You will need this number when you set up the BFS QAM modulator. |
| Transport Protocol | The type of output that feeds the BFS QAM modulator.<br>Select **ASI** as the type of output that feeds the BFS QAM modulator. |
| **Note:** When you set up the BFS QAM modulator that the ASI card connects to, the system will automatically complete the Connect To fields on this window. | |

4. Click **Apply**. The system saves the MPEG source information in the DNCS database and updates the Connectivity illustration to include the new port information.
5. Do you need to add an MPEG BFS source for another ASI card, for example an ASI card on an RNCS/LIONN?
   - If **yes**, set up the parameters for the other ASI card. Go to Setting Up ASI Card Basic Parameters.
   - If **no**, click **Save**. The system saves the MPEG source information in the DNCS database and closes the Set Up MPEG Source window. The MPEG Source List window updates to include the new MPEG source.
6. Add the new MPEG BFS source to your network map.
7. Your next step is to add the BFS QAM modulator that will be receiving BFS data from this ASI card. Go to Add a BFS QAM Modulator to the DNCS.

## Add a BFS QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used for all systems except those that use the RCS option. If your system uses the RCS option, follow a different procedure to set up a BFS QAM modulator for an RCS. A different procedure is required because the RCS option requires system information (SI) to be delivered out-of-band by a QPSK modulator. Other systems typically deliver SI out-of-band and inband by the BFS QAM modulator. See Manage Regional Control System for more information.

A BFS QAM modulator receives BFS data, modulates the data onto an RF carrier, and then sends it downstream on the inband data path to all DHCTs in the headend.

In addition to providing BFS data to DHCTs, your system must also deliver SI data to DHCTs. Systems that do not use the RCS option deliver SI both inband (by a QAM modulator) and out-of-band (by a QPSK modulator). To deliver SI data to all DHCTs, you must establish (distinguish) one QAM modulator per headend to carry inband SI data to all the DHCTs on that headend. This QAM modulator is called the Distinguished QAM. Any QAM modulator that is online (active) and not assigned to a specific hub is a candidate for a Distinguished QAM modulator.

We recommend that you set up your BFS QAM modulator to also be the Distinguished QAM. However, if you are using an MQAM modulator to carry BFS data, you will need to distinguish a QAM modulator to carry SI data. Only a QAM modulator can become a Distinguished QAM modulator.

**Important:**

- **For systems without Direct ASI**, each headend in your network must have a BFS QAM modulator associated with a BFS BIG. In addition, each headend in your network must also have a Distinguished QAM modulator. Otherwise, some DHCTs in your network will not receive BFS and SI data for that headend.
- **For systems using Direct ASI**, each headend in your network must have a BFS QAM modulator associated with an ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

**You Need to Know**

Before You Begin

Before adding a BFS QAM modulator, make sure that you have first added one of the following elements to the DNCS:

- Systems without Direct ASI: First add a BFS BIG to the DNCS.
- Systems with Direct ASI: First add an MPEG BFS source to the DNCS.

**Important:** Before you begin, you must have your network map.

You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- If connecting to a BFS BIG, obtain the following information:
    - Output transport stream ID used by the BFS BIG

- Slot number where the MSYNC control card is installed on the corresponding BFS BIG (usually, slot 3)
- Port number on the MSYNC control card or SWIF transmit card that is connected to this QAM modulator (usually, port 1)

- If connecting directly to the ASI card on the DNCS, the output transport stream ID used by the DNCS

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the BFS QAM modulator basic parameters.
2. Set up the BFS QAM modulator connection to the BFS BIG or DNCS.
3. Activate the BFS QAM modulator.

### You Need to Know

Before You Begin

Before adding a BFS QAM modulator, make sure that you have first added one of the following elements to the DNCS:

- Systems without Direct ASI: First add a BFS BIG to the DNCS.
- Systems with Direct ASI: First add an MPEG BFS source to the DNCS.

**Important:** Before you begin, you must have your network map.

You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- If connecting to a BFS BIG, obtain the following information:
  - Output transport stream ID used by the BFS BIG
  - Slot number where the MSYNC control card is installed on the corresponding BFS BIG (usually, slot 3)
  - Port number on the MSYNC control card or SWIF transmit card that is connected to this QAM modulator (usually, port 1)
- If connecting directly to the ASI card on the DNCS, the output transport stream ID used by the DNCS

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Related Topics

- BFS and Distinguished QAM Modulator Recommendations
- BFS QAM Settings

### BFS and Distinguished QAM Modulator Recommendations

We recommend the following regarding BFS and Distinguished QAM modulators:

- Because all DHCTs on a headend need both BFS and SI data, set up your BFS QAM modulator to also be the Distinguished QAM modulator. However, if you are using an MQAM modulator to carry BFS data, you will need to set up another QAM modulator as the Distinguished QAM modulator to carry SI data. Only a QAM modulator can become a Distinguished QAM modulator.
- Make sure the BFS/Distinguished QAM modulator is not assigned to a specific hub, but that it sends BFS and SI data to all hubs in the headend.
- When you activate the BFS/Distinguished QAM modulator, make sure you select the **Allow SI** option to allow the modulator to process SI data, as well as other types of data.
- Make sure you define only one Distinguished QAM modulator per headend.

**Important:** If more than one Distinguished QAM candidate exists in a headend, the DNCS automatically selects one of those QAM modulators to be the Distinguished QAM. Depending on the other data you need to transmit through that QAM modulator, this may or may not be desirable.

### Related Topics

- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters
- Setting Up BFS QAM Modulator Connections
- Activating a BFS QAM Modulator

### BFS QAM Settings

Use the Set Up QAM page to manage the BFS QAM modulators in your network. The following tabs in this window provide settings for the BFS QAM:

- Basic Parameters Settings
- Connection Settings
- Advanced Parameters settings - The system automatically sets up advanced parameters. As a result, you do not need to complete any fields on the Advanced Parameters tab.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

### Basic Parameter Settings - BFS QAM Modulator

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪If the BFS QAM Modulator connects to a BFS BIG, click the **SWIF** option to select the type of card sending BFS data from the BFS BIG to this QAM modulator.<br>▪If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator<br>Select the type of modulation this QAM modulator uses. For example, if this modulator |

| | |
|---|---|
| uses | uses 256 QAM, you would select **256 QAM**. |
| **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

## Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

### Connections Settings - BFS QAM Modulator

Use the following fields when you manage the connections for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives from the BFS QAM resides. |
| Device Type | Determines the device type that feeds this QAM:<br>▪If a BFS BIG feeds the BFS QAM, select **BIG**.<br>▪If an ASI card on the DNCS feeds this BFS QAM, select **ASI**. Select this option if you are using the QAM modulator with an RCS.<br>The option you select determines which parameters display for setup, as described below. |
| Device Name | The name of the device. Valid for either BFS BIG or ASI QAMs. |
| Card Type | The type of card in the BFS BIG.<br>Select **MSYNC SWIF**. |
| Slot Number | The slot number where the MSYNC control card is installed on the BFS BIG (usually, slot 3).<br>Valid for BFS BIG only. |
| Port Number | The port number for the various cards:<br>▪**For BFS BIG** - control card that is connected to this QAM modulator (usually port 1).<br>▪**For ASI** - Select the port number on the ASI card that is connected to this BFS QAM modulator. |

### Related Topics

- Add a BFS QAM
- Setting Up BFS QAM Modulator Connections in an RCS
- BFS QAM Modulator
- BFS QAM Settings

### Setting Up BFS QAM Modulator Basic Parameters

The first step in adding a BFS QAM modulator is to set up the BFS QAM modulator basic parameters. Complete these steps to set up the basic parameters for a BFS QAM modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > QAM**. The Set Up QAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameter Settings - BFS QAM Modulator.

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪ Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪ Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪ If the BFS QAM Modulator connects to a BFS BIG, click the |

| | | |
|---|---|---|
| | **SWIF** option to select the type of card sending BFS data from the BFS BIG to this QAM modulator.<br>▪ If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. | |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. | |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| | **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| | **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| | **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| | **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| | **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

### Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

6.Click **Apply**. The system saves the QAM modulator information you have entered thus far into the DNCS database and enables the Port To Hubs button.

7. Click **Port to Hubs**. The RF Output Port window opens. The Basic Parameters area of this window shows the data that you entered for key RF output fields. The Associated Hubs area shows the hubs that are available to receive content data from this QAM modulator.

8. Make sure the **Selected Hubs** field shows no hub names so that this QAM modulator sends BFS and SI data (DNCS BFS QAM only) to all hubs in the headend.

**Note:** To remove a hub name from the Selected Hubs field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field.

9. Click **Save**. The system saves this information into the DNCS database and closes the RF Output Port window.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

10. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to select one of the following options:

- Set up the connections between the BFS QAM modulator and the BFS BIG (for a DNCS BFS QAM installation)
- Set up the connections for a BFS QAM in an RCS (for an RNCS/LIONN BFS QAM installation)

### Setting Up BFS QAM Modulator Connections

After you set up the basic parameters for a BFS QAM modulator, complete these steps to set up the connections between the BFS QAM modulator and the BFS BIG or the ASI card on the DNCS.

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this QAM modulator.
2. If not already selected, click to select the **Input Port** option in the **QAM Name** area.
3. Complete the fields on the screen as described in Connections Settings - BFS QAM Modulator.

Use the following fields when you manage the connections for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives from the BFS QAM resides. |
| Device Type | Determines the device type that feeds this QAM:<br>▪ If a BFS BIG feeds the BFS QAM, select **BIG**.<br>▪ If an ASI card on the DNCS feeds this BFS QAM, select **ASI**. Select this option if you are using the QAM modulator with an RCS.<br>The option you select determines which parameters display for setup, as described below. |
| Device Name | The name of the device. Valid for either BFS BIG or ASI QAMs. |
| Card Type | The type of card in the BFS BIG.<br>Select **MSYNC SWIF**. |
| Slot Number | The slot number where the MSYNC control card is installed on the BFS BIG (usually, slot 3).<br>Valid for BFS BIG only. |
| Port Number | The port number for the various cards:<br>▪ **For BFS BIG** - control card that is connected to this QAM modulator (usually port 1).<br>▪ **For ASI** - Select the port number on the ASI card that is connected to this BFS QAM modulator. |

#### Related Topics

- Add a BFS QAM
- Setting Up BFS QAM Modulator Connections in an RCS
- BFS QAM Modulator
- BFS QAM Settings

4. Click **Apply**. The system saves this information into the DNCS database.
5. Your next step is to activate the BFS QAM modulator.

### Activating a BFS QAM Modulator

After you set up the connections between the BFS QAM modulator and the device that feeds it, complete these steps to activate the BFS QAM modulator.

**Note:** You can activate a QAM modulator only after all parameters for the QAM modulator have been saved to the DNCS database, and only after the QAM modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
2. At the **Administrative State** field, click the **Online** option.
3. If this BFS QAM modulator will also function as a Distinguished QAM modulator, verify that **Allow SI** is set to **Yes**. If it is not, click and select **Yes**.
4. Click **Save**. The system saves the QAM modulator information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new QAM modulator.
5. Add the new BFS QAM modulator to your network map.
6. Do you need to add another BFS QAM modulator?
   - If **yes**, go back to Setting Up BFS QAM Modulator Basic Parameters.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console. Go to Verifying Your VASP Configuration.

## Add a BFS QAM Modulator to Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow another procedure to add a BFS QAM modulator to the DNCS.

Before adding a BFS QAM modulator to your RCS, make sure that you have first added an MPEG BFS source for the central DNCS site and for each remote site in your system.

A BFS QAM modulator receives BFS data, modulates the data onto an RF carrier, and then sends it downstream to all DHCTs on the headend. Each headend in your network must have a BFS QAM modulator associated with ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- The output transport stream ID of the ASI card on the DNCS or RNCS/LIONN

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the basic parameters of a BFS QAM modulator in an RCS.
2. Set up connections for a BFS QAM modulator in an RCS.
3. Activate a BFS QAM modulator in an RCS.

### Related Topics

- Recommendations for BFS QAM Modulators in an RCS
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

### Recommendations for BFS QAM Modulators in an RCS

We recommend the following regarding BFS QAM modulators:

- Make sure the BFS QAM modulator is **not** assigned to a specific hub, but that it sends BFS data to all hubs in the headend.
- When you activate the BFS QAM modulator, make sure that the **Allow SI** option is set to **No**. In an RCS, system information (SI) is carried on the out-of-band data path through a QPSK modulator.

## Add a BFS QAM Modulator to Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow another procedure to add a BFS QAM modulator to the DNCS.

Before adding a BFS QAM modulator to your RCS, make sure that you have first added an MPEG BFS source for the central DNCS site and for each remote site in your system.

A BFS QAM modulator receives BFS data, modulates the data onto an RF carrier, and then sends it downstream to all DHCTs on the headend. Each headend in your network must have a BFS QAM modulator associated with ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- The output transport stream ID of the ASI card on the DNCS or RNCS/LIONN

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the basic parameters of a BFS QAM modulator in an RCS.
2. Set up connections for a BFS QAM modulator in an RCS.
3. Activate a BFS QAM modulator in an RCS.

### Related Topics

- Recommendations for BFS QAM Modulators in an RCS
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

### Recommendations for BFS QAM Modulators in an RCS

We recommend the following regarding BFS QAM modulators:

- Make sure the BFS QAM modulator is **not** assigned to a specific hub, but that it sends BFS data to all hubs in the headend.
- When you activate the BFS QAM modulator, make sure that the **Allow SI** option is set to **No**. In an RCS, system information (SI) is carried on the out-of-band data path through a QPSK modulator.

### BFS QAM Settings

Use the Set Up QAM page to manage the BFS QAM modulators in your network. The following tabs in this window provide settings for the BFS QAM:

- Basic Parameters Settings
- Connection Settings
- Advanced Parameters settings - The system automatically sets up advanced parameters. As a result, you do not need to complete any fields on the Advanced Parameters tab.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

### Basic Parameter Settings - BFS QAM Modulator

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪If the BFS QAM Modulator connects to a BFS BIG, click the **SWIF** option to select the type of card sending BFS data from the BFS BIG to this QAM modulator.<br>▪If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator<br>Select the type of modulation this QAM modulator uses. For example, if this modulator |

| | |
|---|---|
| uses | uses 256 QAM, you would select **256 QAM**. |
| **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

## Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

## Connections Settings - BFS QAM Modulator

Use the following fields when you manage the connections for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives from the BFS QAM resides. |
| Device Type | Determines the device type that feeds this QAM:<br>▪If a BFS BIG feeds the BFS QAM, select **BIG**.<br>▪If an ASI card on the DNCS feeds this BFS QAM, select **ASI**. Select this option if you are using the QAM modulator with an RCS.<br>The option you select determines which parameters display for setup, as described below. |
| Device Name | The name of the device. Valid for either BFS BIG or ASI QAMs. |
| Card Type | The type of card in the BFS BIG.<br>Select **MSYNC SWIF**. |
| Slot Number | The slot number where the MSYNC control card is installed on the BFS BIG (usually, slot 3).<br>Valid for BFS BIG only. |
| Port Number | The port number for the various cards:<br>▪**For BFS BIG** - control card that is connected to this QAM modulator (usually port 1).<br>▪**For ASI** - Select the port number on the ASI card that is connected to this BFS QAM modulator. |

### Related Topics

- Add a BFS QAM
- Setting Up BFS QAM Modulator Connections in an RCS
- BFS QAM Modulator
- BFS QAM Settings

### Setting Up BFS QAM Modulator Basic Parameters in an RCS

Complete these steps to set up the basic parameters for a BFS QAM modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > QAM**. The Set Up QAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameters - BFS QAM Modulator.

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪ Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪ Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪ If the BFS QAM Modulator connects to a BFS BIG, click the **SWIF** option to select the type of card sending BFS data from the BFS |

| | | |
|---|---|---|
| | BIG to this QAM modulator.<br>▪ If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. | |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. | |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| | **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| | **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| | **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| | **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| | **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

### Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

6. Click **Save**. The system saves this data and closes the Output Port window.

**Important:** You should not need to use the Advanced Parameters tab because the system automatically

configures these settings for you. These settings tell a modulator which version of software to use. Do **not** change information in the Advanced Parameters tab without first consulting contact Cisco Services. Changing this data without direction from Cisco Services can degrade system performance.

7. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to set up the connections between the BFS QAM modulator and the ASI card. Go to Setting Up Connections for a BFS QAM Modulator in an RCS.

### Setting Up BFS QAM Modulator Connections in an RCS

After you set up the basic parameters for a BFS QAM modulator, complete these steps to set up the connections between the BFS QAM modulator and the ASI card on the DNCS or RNCS/LIONN.

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this QAM modulator.
2. If not already selected, click to select the **Input Port** option in the **QAM Name** area.
3. In the **Connect To** area, click the **Headend Name** arrow and select the headend in which the device that feeds the BFS QAM resides.
4. Click the **Device Type** arrow and select **ASI**.
5. Continue defining connections to the ASI card by entering the following information in any order.
   - Click the **Device Name** arrow and select the name you gave the ASI card when you defined it earlier as an MPEG source.
   - Click the **Port Number** arrow and select the port number on the ASI card that is connected to this BFS QAM modulator.
6. Click **Apply**. The system saves this information into the DNCS database.
7. Your next step is to activate the BFS QAM modulator. Go to Activating a BFS QAM Modulator in an RCS.

### Activating a BFS QAM Modulator in an RCS

After you set up the connections between the BFS QAM modulator and the device that feeds it, complete these steps to activate the BFS QAM modulator.

**Note:** You can activate a QAM modulator only after all parameters for the QAM modulator have been saved to the DNCS database, and only after the QAM modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
2. At the **Administrative State** field, click the **Online** option.
3. If this BFS QAM modulator will also function as a Distinguished QAM modulator, verify that **Allow SI** is set to **No**. If it is not, click and select **No**.
4. Click **Save**. The system saves the QAM modulator information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new QAM modulator.
5. Add the new BFS QAM modulator to your network map.
6. Do you need to add another BFS QAM modulator to your RCS?
   - If **yes**, go back to Setting Up BFS QAM Modulator Basic Parameters in an RCS.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console. Go to Verify the VASP Configuration in an RCS.

**Modify**

### Modify an MPEG BFS Source

**Important:** Do not attempt to modify or delete an MPEG BFS source without assistance from us. Certain BFS modifications may degrade system performance. For this reason, always consult us before making changes to an MPEG BFS source.

### Modify a BFS QAM Modulator

**Important:** Do not attempt to modify or delete a BFS QAM modulator without assistance from Cisco Services. Certain BFS modifications may degrade system performance. For this reason, always consult Cisco Services before making changes to a BFS QAM modulator.

**Delete**

**Delete an MPEG BFS Source**

**Important:** Do not attempt to modify or delete an MPEG BFS source without assistance from us. Certain BFS modifications may degrade system performance. For this reason, always consult us before making changes to an MPEG BFS source.

**Delete**

**Delete an MPEG BFS Source**

**Important:** Do not attempt to modify or delete an MPEG BFS source without assistance from us. Certain BFS modifications may degrade system performance. For this reason, always consult us before making changes to an MPEG BFS source.

### Delete a BFS QAM Modulator

**Important:** Do not attempt to modify or delete a BFS QAM modulator without assistance from Cisco Services. Certain BFS modifications may degrade system performance. For this reason, always consult Cisco Services before making changes to a BFS QAM modulator.

# DOCSIS Set-top Gateway Support

With DOCSIS Set-top Gateway (DSG) support you can deploy DSG-capable DHCTs. These DHCTs contain a cable modem that operates with a CableLabs-qualified DOCSIS 1.0 and 1.1 and DSG Cable Modem Termination System (CMTS). As a result, you can support IP-based, real-time, two-way communication between these DHCTs and your headend and provide a faster out-of-band path for two-way services.

For example, the **Explorer 8300** can operate with any CMTS qualified by CableLabs for DSG operation. When part of a CMTS, the Explorer 8300 operates in either of the following modes:

- **Mixed DOCSIS/DAVIC communication mode** - These DHCTs receive out-of-band data on a DAVIC channel and unicast data on a two-way DOCSIS channel.
- **DOCSIS communication mode** - Unique code allows the DHCT to interpret the mode Mixed DOCSIS/DAVIC and the mode DOCSIS as DOCSIS. When in DOCSIS mode, these DHCTs receive both out-of-band data and unicast data on a DOCSIS channel.
- **Note:** DOCSIS is a CableLabs standard that enables data services to be provided over a two-way cable system. DSG is a CableLabs standard that enables video signaling to be provided over a one-way or two-way cable system.

## What do you want to do?

- Review the requirements your DBDS must meet to support DSG- capable DHCTs
- Examine a simplified network view of the DHCT communication modes that support DOCSIS
- View a list of DSG-capable DHCTs
- Learn how to prepare the DNCS to support DSG-capable DHCTs

## DSG Support Requirements

Your DBDS must meet the following requirements to support DSG-capable DHCTs:

- Hardware and software requirements
- Network element requirements

### Hardware and Software Requirements

The following hardware and software are required to support DSG-capable DHCTs:

- Installation of SR 3.5 (or later) and enabling the software license
- Cable Modem Termination System supporting DSG for CableLabs
- DHCTs as listed in DOCSIS-Capable DHCTs
- SARA Client Release 1.41 or later (or similar)
- PowerTV Home Gateway Edition 1.0
- DHCP Server
- Trivial File Transfer Protocol (TFTP) Server
- Time Of Day (TOD) Server (optional)
- Domain Name System (DNS) Server (optional)

**Note:** For information on installing and configuring these elements in a DOCSIS system, refer to DOCSIS in a DBDS Environment (part number 4000358). To obtain a copy of this document, see Printed Resources.

### Network Element Requirements

The network elements in your DBDS must meet the following requirements to operate DOCSIS-capable DHCTs.

**Important:** If you are unsure of your system's ability to meet the following requirements, contact your network administrator or Cisco Services to arrange for a network analysis.

- CMTS units used must adhere to the specifications detailed in the following publications:
  - Advanced DOCSIS Set-Top Gateway Application Guide For System Release 3.5 and 4.0 (part number 4004619)
  - Advanced DOCSIS® Set-Top Gateway Application Guide For System Releases 3.7 and 4.2 (part number 4012166)
  - DOCSIS Set-Top Gateway (DSG) Interface Specification
  - Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification
  - Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification
  - Data-Over-Cable Service Interface Specifications Operations Support System Interface Specification

  **Note:** To obtain a copy of any of the documents listed above, see Printed Resources.

- The DHCP servers used must adhere to the specifications detailed in the **Dynamic Host Control Protocol**.
- DHCTs booting in DAVIC mode must receive an IP address from a private address pool managed by the DNCS.
- DHCTs booting in DOCSIS or Mixed DOCSIS/DAVIC mode must receive cable modem and DHCT CPE IP addresses from address pools managed by the DHCP server.

**Related Topics**

- Network View of DHCT Communications
- DOCSIS-Capable DHCTs
- Prepare the DNCS for DSG
- DSG Timers and Filters

### Hardware and Software Requirements

The following hardware and software are required to support DSG-capable DHCTs:

- Installation of SR 3.5 (or later) and enabling the software license
- Cable Modem Termination System supporting DSG for CableLabs
- DHCTs as listed in DOCSIS-Capable DHCTs
- SARA Client Release 1.41 or later (or similar)
- PowerTV Home Gateway Edition 1.0
- DHCP Server
- Trivial File Transfer Protocol (TFTP) Server
- Time Of Day (TOD) Server (optional)
- Domain Name System (DNS) Server (optional)

**Note:** For information on installing and configuring these elements in a DOCSIS system, refer to DOCSIS in a DBDS Environment (part number 4000358). To obtain a copy of this document, see Printed Resources.

## DSG Support Requirements

Your DBDS must meet the following requirements to support DSG-capable DHCTs:

- Hardware and software requirements
- Network element requirements

### Hardware and Software Requirements

The following hardware and software are required to support DSG-capable DHCTs:

- Installation of SR 3.5 (or later) and enabling the software license
- Cable Modem Termination System supporting DSG for CableLabs
- DHCTs as listed in DOCSIS-Capable DHCTs
- SARA Client Release 1.41 or later (or similar)
- PowerTV Home Gateway Edition 1.0
- DHCP Server
- Trivial File Transfer Protocol (TFTP) Server
- Time Of Day (TOD) Server (optional)
- Domain Name System (DNS) Server (optional)

**Note:** For information on installing and configuring these elements in a DOCSIS system, refer to DOCSIS in a DBDS Environment (part number 4000358). To obtain a copy of this document, see Printed Resources.

### Network Element Requirements

The network elements in your DBDS must meet the following requirements to operate DOCSIS-capable DHCTs.

**Important:** If you are unsure of your system's ability to meet the following requirements, contact your network administrator or Cisco Services to arrange for a network analysis.

- CMTS units used must adhere to the specifications detailed in the following publications:
  - Advanced DOCSIS Set-Top Gateway Application Guide For System Release 3.5 and 4.0 (part number 4004619)
  - Advanced DOCSIS® Set-Top Gateway Application Guide For System Releases 3.7 and 4.2 (part number 4012166)
  - DOCSIS Set-Top Gateway (DSG) Interface Specification
  - Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification
  - Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification
  - Data-Over-Cable Service Interface Specifications Operations Support System Interface Specification

  **Note:** To obtain a copy of any of the documents listed above, see Printed Resources.

- The DHCP servers used must adhere to the specifications detailed in the **Dynamic Host Control Protocol**.
- DHCTs booting in DAVIC mode must receive an IP address from a private address pool managed by the DNCS.
- DHCTs booting in DOCSIS or Mixed DOCSIS/DAVIC mode must receive cable modem and DHCT CPE IP addresses from address pools managed by the DHCP server.

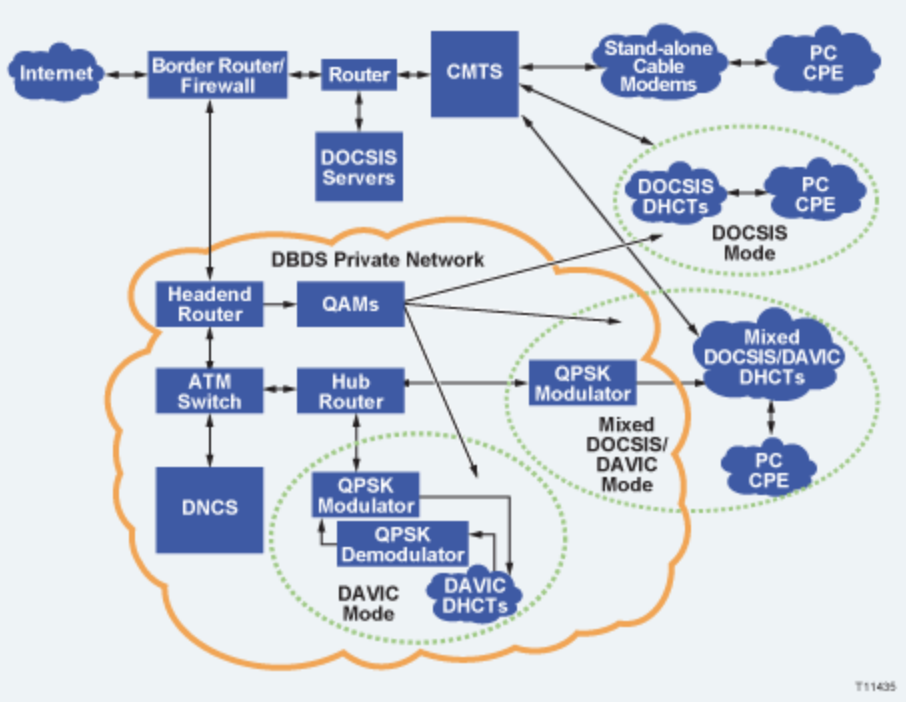
### Related Topics

- Network View of DHCT Communications
- DOCSIS-Capable DHCTs
- Prepare the DNCS for DSG
- DSG Timers and Filters

## Network View of DHCT Communications

The following diagram shows the layout of a network that can support DHCTs operating in the various communication modes.

**Note:** To support DSG-capable DHCTs, you must configure a CMTS bridge on the DNCS. A bridge is either a QPSK or a collection of CMTS elements. Any CMTS that joins a multicast group defined for a CMTS bridge becomes part of the hub for 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 that bridge.




### Related Topics

- DOCSIS-Capable DHCTs
- Prepare the DNCS for DSG
- DSG Timers and Filters

## DOCSIS-Capable DHCTs

The **Explorer 4200, Explorer 4240, Explorer 8240, and Explorer 8300** can operate with any Cable Modem Termination System (CMTS) qualified by CableLabs for DSG operation. These DHCTs offer video and data through a single device using hybrid fiber/coax network. These DHCTs deliver digital broadcast video and support real-time, two-way interactive applications, such as electronic program guides, enhanced TV, video-on-demand (VOD), and subscription VOD to the television. The Explorer 8300 also includes a digital video recorder (DVR) with picture-in-picture (PIP) control, giving subscribers control, convenience, and choice in their TV viewing experience.

The **Explorer 4200, Explorer 4250, Explorer 8250, and Explorer 8300** can use either a DOCSIS or DAVIC channel depending upon their communication mode. They receive both out-of-band data and unicast data on a DOCSIS channel when operating in DOCSIS mode.

### Related Topics

- Prepare the DNCS for DSG
- DSG Timers and Filters

# Prepare the DNCS for DSG

### Set Up the DNCS to Support DOCSIS-Capable DHCTs

The following topics summarize the steps you need to take to prepare the DNCS to support DSG-capable DHCTs. We recommend that you read all of the information in this section before attempting to prepare the DNCS.

## You Need to Know

Before You Begin

Time to Complete

Preparing the DNCS to support DSG-capable DHCTs takes approximately 2 hours and depends on the number of QPSK and CMTS bridges you need to configure with a new DCM.

Before you begin, make sure that you have completed the following tasks:

- Configured your DBDS to meet the requirements listed in DSG Support Requirements.
- Obtained a list from your system administrator of all the hubs defined in your network. In addition to new QPSK or CMTS bridges, this list should also contain the QPSKs whose DHCT communication modes (DCMs) will change from DAVIC to DOCSIS.

**Note:** To support DSG-capable DHCTs, you must configure CMTS **bridges** on the DNCS. A bridge is either a QPSK or a collection of CMTS elements. CMTS bridges support DOCSIS operation. Any CMTS that joins a multicast group defined for a CMTS bridge becomes part of the hub for 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 that bridge.

- Planned and managed the distribution of IP addresses to the DHCTs. Careful planning can prevent conflicts of IP addresses between existing DAVIC and DSG- capable DHCTs on the DBDS network. To review the guidelines that can help you assign IP addresses, refer to DOCSIS in a DBDS Environment (part number 4000358). To obtain a copy of this guide, refer to Printed Resources.

Performance Impact

These procedures do not impact the network and can be performed at any time.

### Setting Up the DNCS to Support DSG-Capable DHCTs

The following information provides an overview of the process you must follow to prepare the DNCS to support DSG-capable DHCTs. Click any link to display step-by-step instructions for the procedures summarized here.

Follow these steps to configure the DNCS to support the ability of Explorer 8300 DHCTs to multicast out-of-band data to DHCTs:

1. Add a CMTS Bridge to the DNCS. A CMTS bridge is a logical entity that serves DHCTs in the same hub. Create one CMTS bridge for every hub that serves DSG-capable DHCTs.
2. Add a QPSK Modulator. Adding a QPSK modulator for every hub that serves DSG-capable DHCTs ensures that a bridge resolution file (BRF) is sent to DHCTs. These DHCTs need this file so that they can determine which CMTS bridge to use for DOCSIS communication. When adding QPSK modulators to send the BRF to hubs, make sure to add one QPSK modulator for every hub that serves DSG-capable DHCTs, and to set the DCM of each modulator to DOCSIS.

3. Register the BRF Server With the BFS Client. The BRF contains a mapping of hub assignments to multicast MAC addresses. BRF data is automatically generated from the information you enter when adding a CMTS bridge for multicasting from the DNCS. To ensure that the BFS broadcasts the BRF over the DAVIC/QPSK path, register the BRF server with the BFS client. After the BRF server has registered with the BFS client, the BFS sends the BRF to DHCTs over the DAVIC/QPSK path. When DHCTs first boot, they use the DAVIC path to retrieve the BRF and acquire their hub assignments and multicast MAC addresses. Unique code running on the Explorer 8300 DHCTs allows them to complete the boot cycle by interpreting a DCM of Mixed DOCSIS/DAVIC as DOCSIS and establish a two-way connection using the DOCSIS/CMTS path.

4. Update the BFS. After a reboot, DHCTs check the BFS for new or revised information, and DHCTs that require the BRF will download it. Updating the BFS ensures that the BFS broadcasts the new file to DHCTs after the DHCTs reboot.

### Set Up the DNCS to Support DOCSIS-Capable DHCTs

The following topics summarize the steps you need to take to prepare the DNCS to support DSG-capable DHCTs. We recommend that you read all of the information in this section before attempting to prepare the DNCS.

## You Need to Know

- Before You Begin
- Time to Complete

Preparing the DNCS to support DSG-capable DHCTs takes approximately 2 hours and depends on the number of QPSK and CMTS bridges you need to configure with a new DCM.

Before you begin, make sure that you have completed the following tasks:

- Configured your DBDS to meet the requirements listed in DSG Support Requirements.
- Obtained a list from your system administrator of all the hubs defined in your network. In addition to new QPSK or CMTS bridges, this list should also contain the QPSKs whose DHCT communication modes (DCMs) will change from DAVIC to DOCSIS.

  **Note:** To support DSG-capable DHCTs, you must configure CMTS **bridges** on the DNCS. A bridge is either a QPSK or a collection of CMTS elements. CMTS bridges support DOCSIS operation. Any CMTS that joins a multicast group defined for a CMTS bridge becomes part of the hub for 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 that bridge.

- Planned and managed the distribution of IP addresses to the DHCTs. Careful planning can prevent conflicts of IP addresses between existing DAVIC and DSG- capable DHCTs on the DBDS network. To review the guidelines that can help you assign IP addresses, refer to DOCSIS in a DBDS Environment (part number 4000358). To obtain a copy of this guide, refer to Printed Resources.

- Performance Impact

These procedures do not impact the network and can be performed at any time.

# Prepare the DNCS for DSG

## Set Up the DNCS to Support DOCSIS-Capable DHCTs

The following topics summarize the steps you need to take to prepare the DNCS to support DSG-capable DHCTs. We recommend that you read all of the information in this section before attempting to prepare the DNCS.

## You Need to Know

Before You Begin

Time to Complete

Preparing the DNCS to support DSG-capable DHCTs takes approximately 2 hours and depends on the number of QPSK and CMTS bridges you need to configure with a new DCM.

Before you begin, make sure that you have completed the following tasks:

- Configured your DBDS to meet the requirements listed in DSG Support Requirements.
- Obtained a list from your system administrator of all the hubs defined in your network. In addition to new QPSK or CMTS bridges, this list should also contain the QPSKs whose DHCT communication modes (DCMs) will change from DAVIC to DOCSIS.

  **Note:** To support DSG-capable DHCTs, you must configure CMTS **bridges** on the DNCS. A bridge is either a QPSK or a collection of CMTS elements. CMTS bridges support DOCSIS operation. Any CMTS that joins a multicast group defined for a CMTS bridge becomes part of the hub for 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 that bridge.

- Planned and managed the distribution of IP addresses to the DHCTs. Careful planning can prevent conflicts of IP addresses between existing DAVIC and DSG- capable DHCTs on the DBDS network. To review the guidelines that can help you assign IP addresses, refer to DOCSIS in a DBDS Environment (part number 4000358). To obtain a copy of this guide, refer to Printed Resources.

Performance Impact

These procedures do not impact the network and can be performed at any time.

## Setting Up the DNCS to Support DSG-Capable DHCTs

The following information provides an overview of the process you must follow to prepare the DNCS to support DSG-capable DHCTs. Click any link to display step-by-step instructions for the procedures summarized here.

Follow these steps to configure the DNCS to support the ability of Explorer 8300 DHCTs to multicast out-of-band data to DHCTs:

1. Add a CMTS Bridge to the DNCS. A CMTS bridge is a logical entity that serves DHCTs in the same hub. Create one CMTS bridge for every hub that serves DSG-capable DHCTs.
1. Add a QPSK Modulator. Adding a QPSK modulator for every hub that serves DSG-capable DHCTs ensures that a bridge resolution file (BRF) is sent to DHCTs. These DHCTs need this file so that they can determine which CMTS bridge to use for DOCSIS communication. When adding QPSK modulators to send the BRF to hubs, make sure to add one QPSK modulator for every hub that serves DSG-capable DHCTs, and to set the DCM of each modulator to DOCSIS.

1. Register the BRF Server With the BFS Client. The BRF contains a mapping of hub assignments to multicast MAC addresses. BRF data is automatically generated from the information you enter when adding a CMTS bridge for multicasting from the DNCS. To ensure that the BFS broadcasts the BRF over the DAVIC/QPSK path, register the BRF server with the BFS client. After the BRF server has registered with the BFS client, the BFS sends the BRF to DHCTs over the DAVIC/QPSK path. When DHCTs first boot, they use the DAVIC path to retrieve the BRF and acquire their hub assignments and multicast MAC addresses. Unique code running on the Explorer 8300 DHCTs allows them to complete the boot cycle by interpreting a DCM of Mixed DOCSIS/DAVIC as DOCSIS and establish a two-way connection using the DOCSIS/CMTS path.

1. Update the BFS. After a reboot, DHCTs check the BFS for new or revised information, and DHCTs that require the BRF will download it. Updating the BFS ensures that the BFS broadcasts the new file to DHCTs after the DHCTs reboot.

**Explorer 4200-Series Home Gateway DHCTs**

**Change the DCM of Existing QPSK Modulators**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select QPSK Modulator] > File > Open**

When you change the DHCT Communication Mode (DCM) of an existing QPSK modulator to DOCSIS, you create a QPSK bridge. A QPSK bridge serves DHCTs in the same hub. For this reason, create one QPSK bridge for every hub that serves Explorer 8300 DHCTs. After changing the DCMs of the existing QPSK modulators, send a DCM update message to all of the affected DHCT types so the previously booted DHCTs can operate in DOCSIS Mode. This procedure describes how to change the DCMs of existing QPSK modulators to DOCSIS mode, and provides a link to instructions on sending a DCM update message.

## You Need to Know

Time to Complete

Changing the DCM of an existing QPSK modulator takes about one minute.

Performance Impact

Changing the DCM of an existing QPSK modulator does not impact network performance. You can complete this procedure at any time.

### Changing the DCM of Existing QPSK Modulators

Complete the following steps to change the DCM of an existing QPSK modulator.

1. On the DNCS tab of the DNCS Administrative Console, click the **Network Element Provisioning** tab.
2. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
3. Select the row with the bridge name associated with the QPSK whose DCM you want to change.
4. Click **File > Open**. The Set Up QPSK Modulator window opens and shows the Basic Parameters tab.
5. Click **DCM > DOCSIS**.
6. Click **Save**. A warning appears and states that you must send a DCM Updated Message for the new DCM to take effect.
7. Click **OK**. The system returns to the Set Up QPSK Modulator window and the Cancel button changes to Close. The DHCTs can now boot in DOCSIS mode at startup.
8. Do you need to change the DCM of another QPSK modulator?
   - If **yes**, repeat steps 3 through 7 for to create another QPSK bridge.
   - If **no**, go to step 9.
9. Click **Close** to return to the QPSK/CMTS List window.
10. Leave the QPSK/CMTS List window open.
11. You are ready to send a DCM Updated message to the selected DHCT types and bridges to enable the DHCTs to boot in the DOCSIS mode. Go to Send a DCM Updated Message.

**Change the DCM of Existing QPSK Modulators**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select QPSK Modulator] > File > Open**

When you change the DHCT Communication Mode (DCM) of an existing QPSK modulator to DOCSIS, you create a QPSK bridge. A QPSK bridge serves DHCTs in the same hub. For this reason, create one QPSK bridge for every hub that serves Explorer 8300 DHCTs. After changing the DCMs of the existing QPSK modulators, send a DCM update message to all of the affected DHCT types so the previously booted DHCTs can operate in DOCSIS Mode. This procedure describes how to change the DCMs of existing QPSK modulators to DOCSIS mode, and provides a link to instructions on sending a DCM update message.

## You Need to Know

Time to Complete

Changing the DCM of an existing QPSK modulator takes about one minute.

Performance Impact

Changing the DCM of an existing QPSK modulator does not impact network performance. You can complete this procedure at any time.

**Explorer 4200-Series Home Gateway DHCTs**

**Change the DCM of Existing QPSK Modulators**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select QPSK Modulator] > File > Open**

When you change the DHCT Communication Mode (DCM) of an existing QPSK modulator to DOCSIS, you create a QPSK bridge. A QPSK bridge serves DHCTs in the same hub. For this reason, create one QPSK bridge for every hub that serves Explorer 8300 DHCTs. After changing the DCMs of the existing QPSK modulators, send a DCM update message to all of the affected DHCT types so the previously booted DHCTs can operate in DOCSIS Mode. This procedure describes how to change the DCMs of existing QPSK modulators to DOCSIS mode, and provides a link to instructions on sending a DCM update message.

## You Need to Know

Time to Complete

Changing the DCM of an existing QPSK modulator takes about one minute.

Performance Impact

Changing the DCM of an existing QPSK modulator does not impact network performance. You can complete this procedure at any time.

### Changing the DCM of Existing QPSK Modulators

Complete the following steps to change the DCM of an existing QPSK modulator.

1. On the DNCS tab of the DNCS Administrative Console, click the **Network Element Provisioning** tab.
1. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
1. Select the row with the bridge name associated with the QPSK whose DCM you want to change.
1. Click **File > Open**. The Set Up QPSK Modulator window opens and shows the Basic Parameters tab.
1. Click **DCM > DOCSIS**.
1. Click **Save**. A warning appears and states that you must send a DCM Updated Message for the new DCM to take effect.
1. Click **OK**. The system returns to the Set Up QPSK Modulator window and the Cancel button changes to Close. The DHCTs can now boot in DOCSIS mode at startup.
1. Do you need to change the DCM of another QPSK modulator?
    - If **yes**, repeat steps 3 through 7 for to create another QPSK bridge.
    - If **no**, go to step 9.
1. Click **Close** to return to the QPSK/CMTS List window.
1. Leave the QPSK/CMTS List window open.
1. You are ready to send a DCM Updated message to the selected DHCT types and bridges to enable the DHCTs to boot in the DOCSIS mode. Go to Send a DCM Updated Message.

**Send a DCM Updated Message**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > DCM Update**

After changing the DCMs of the existing QPSK modulators, send a DCM update message to all of the affected DHCT types so the previously booted DHCTs can operate in DOCSIS Mode.

## You Need to Know

Time to Complete

Sending a DCM updated message takes about 5 to 20 minutes, depending on the number of DHCTs and QPSK bridges that must be updated.

Performance Impact

Sending a DCM updated message does not impact network performance. You can complete this procedure at any time.

### Sending a DCM Updated Message

Complete the following steps to send a DCM Updated message for the affected bridges.

1. On the QPSK/CMTS list window, click **File > DCM Updated Message**. The DCM Updated Message window opens.
2. In the Available DHCT Types column, select the DHCT type(s) that you want to operate in Mixed DOCSIS/DAVIC mode, and then click **Add**. The selected DHCT type(s) move to the Selected DHCT Types column.

   **Notes:**

   - To select a continuous group of DHCTs, click the first DHCT, press and hold the **Shift** key, and then click the last DHCT.
   - To select DHCTs that are not next to each other, press and hold the **Ctrl** key while you click each DHCT.
3. In the Available Bridges column, scroll through the list and select the bridge(s) whose DCM(s) you want to update, and then click **Add**. The bridge name(s) move to the Selected Bridges column. (You can also use the methods describe above to select a group of bridges or individual bridges.)
4. Click **Send**. The system sends the DCM Updated message to cause the affected DHCTs to reboot and obtain the new DCM. When the update is complete, the message Done appears in the status field.
5. Click **Cancel** to close the DCM Updated Message window.
6. Click **File > Close** to close the QPSK/CMTS list window.

**Send a DCM Updated Message**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > DCM Update**

After changing the DCMs of the existing QPSK modulators, send a DCM update message to all of the affected DHCT types so the previously booted DHCTs can operate in DOCSIS Mode.

## You Need to Know

Time to Complete

Sending a DCM updated message takes about 5 to 20 minutes, depending on the number of DHCTs and QPSK bridges that must be updated.

Performance Impact

Sending a DCM updated message does not impact network performance. You can complete this procedure at any time.

### Sending a DCM Updated Message

Complete the following steps to send a DCM Updated message for the affected bridges.

1. On the QPSK/CMTS list window, click **File > DCM Updated Message**. The DCM Updated Message window opens.
2. In the Available DHCT Types column, select the DHCT type(s) that you want to operate in Mixed DOCSIS/DAVIC mode, and then click **Add**. The selected DHCT type(s) move to the Selected DHCT Types column.

   **Notes:**

   - To select a continuous group of DHCTs, click the first DHCT, press and hold the **Shift** key, and then click the last DHCT.
   - To select DHCTs that are not next to each other, press and hold the **Ctrl** key while you click each DHCT.
3. In the Available Bridges column, scroll through the list and select the bridge(s) whose DCM(s) you want to update, and then click **Add**. The bridge name(s) move to the Selected Bridges column. (You can also use the methods describe above to select a group of bridges or individual bridges.)
4. Click **Send**. The system sends the DCM Updated message to cause the affected DHCTs to reboot and obtain the new DCM. When the update is complete, the message Done appears in the status field.
5. Click **Cancel** to close the DCM Updated Message window.
6. Click **File > Close** to close the QPSK/CMTS list window.

### Add a QPSK Bridge to the DNCS

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

A QPSK bridge uses a DOCSIS DCM to serve DSG-capable DHCTs in the same hub. For this reason, create one QPSK bridge for every hub that serves DSG-capable DHCTs.

You can create a QPSK bridge from existing QPSK modulators by changing the DCM of a modulator to Mixed DOCSIS/DAVIC. For assistance, see Change the DCM of Existing QPSK Modulators.

However, if no QPSK modulators feed a hub that contains DSG-capable DHCTs, create a new QPSK bridge for the DHCTs by following this procedure.

**Note:** To support Explorer 8300 DHCTs with a DCM of Mixed DOCSIS/DAVIC, a **CMTS** bridge must be set up. Unique code running on the Explorer 8300 DHCTs allows them to complete their boot cycle by interpreting a DCM of Mixed DOCSIS/DAVIC as DOCSIS-only and establish a two-way connection using the DOCSIS/CMTS path. For assistance setting up a CMTS bridge, see Add a CMTS Bridge to the DNCS.

#### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QPSK modulator
- MAC address for the QPSK modulator (click here for the procedure to locate)
- Subnet mask for the QPSK modulator
- IP address of the default router associated with the modulator
- Base IP address for all DHCTs within the domain of the modulator
- Subnet mask for all DHCTs within the domain of the modulator
- RF output frequency assigned to this modulator

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Time to Complete

Adding a QPSK bridge to the DNCS takes about 10 minutes.

Performance Impact

Adding a QPSK bridge to the DNCS does not impact network performance. You can complete this procedure at any time.

#### Related Topics

- QPSK Bridge Settings
- Adding a QPSK Bridge to the DNCS
- Setting Up QPSK Bridge Advanced Parameters

### QPSK Bridge Settings

Use the following fields when you manage a QPSK bridge in the DNCS.

| Field | Description |
|---|---|
| Hub Name | The hub associated with this content QPSK (if you have more than one defined). |
| Name | The name of this QPSK.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that allows you to easily identify the QPSK modulator and where it resides. |
| IP Address | The IP address for this QPSK.<br>Be careful to properly place the dots (.) between numbers. |
| Physical Address | The MAC address for the QPSK. |
| Subnet Mask | The subnet mask where this QPSK modulator resides. |
| Default Router | The IP address for the router associated with this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| DHCT Base IP Address | The base IP address for all DHCTs within the domain of this modulator. |
| DHCT Subnet Mask | The subnet mask for all DHCTs within the domain of this modulator. |
| Frequency | The RF output frequency assigned to this modulator.<br>This value can be from 70 MHz to 130 MHz in increments of 0.25 MHz. |
| DCM (DHCT Communications Mode) | Determines the DCM for the QPSK.<br>**Important:** Currently all DSG-capable DHCTs use a Mixed DOCSIS/DAVIC DCM. Unique code on Explorer 8300 DHCTs enables them to recognized a DCM of Mixed DOCSIS/DAVIC as DOCSIS. QPSK modulators that provide the BRF to hubs with Explorer 8300 DHCTs use a DCM of Mixed DOCSIS/DAVIC.<br>Select the appropriate DCM from one of the following choices:<br>▪**DAVIC** - Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel.<br>▪**Mixed DOCSIS/DAVIC** - Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel.<br>▪**DOCSIS** - Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.) |
| Options | **Continuous Wave Mode -** Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK. |

| | |
|---|---|
| | **Front Panel Lock -** Determines whether changes can be made from the front panel. |
| | **Broadcast Only Mode -** Determines whether the QPSK sends priority broadcast transmissions. |
| | **Database Persistence -** Determines whether the QPSK stores the IP addresses of DHCTs in RAM.<br><br>**Note:** Occasionally, you may need to clear the IP addresses that DHCTs are currently using and replace them with new IP addresses. To accomplish this, use the Reset and Clear DB selection on the QPSK File menu. For more information, see Reset the QPSK Modulator Persistent Database. |

## Related Topics

- Adding a QPSK Bridge to the DNCS
- Setting Up QPSK Bridge Advanced Parameters

### Adding a QPSK Bridge to the DNCS

The first step in adding a QPSK bridge to the DNCS is to complete these steps to set up the QPSK bridge basic parameters.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click **File > New > QPSK**. The Set Up QPSK Modulator window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in QPSK Bridge Settings.

Use the following fields when you manage a QPSK bridge in the DNCS.

| Field | Description |
|---|---|
| Hub Name | The hub associated with this content QPSK (if you have more than one defined). |
| Name | The name of this QPSK.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that allows you to easily identify the QPSK modulator and where it resides. |
| IP Address | The IP address for this QPSK.<br>Be careful to properly place the dots (.) between numbers. |
| Physical Address | The MAC address for the QPSK. |
| Subnet Mask | The subnet mask where this QPSK modulator resides. |
| Default Router | The IP address for the router associated with this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| DHCT Base IP Address | The base IP address for all DHCTs within the domain of this modulator. |
| DHCT Subnet Mask | The subnet mask for all DHCTs within the domain of this modulator. |
| Frequency | The RF output frequency assigned to this modulator.<br>This value can be from 70 MHz to 130 MHz in increments of 0.25 MHz. |
| DCM (DHCT Communications Mode) | Determines the DCM for the QPSK.<br>**Important:** Currently all DSG-capable DHCTs use a Mixed DOCSIS/DAVIC DCM. Unique code on Explorer 8300 DHCTs enables them to recognized a DCM of Mixed DOCSIS/DAVIC as DOCSIS. QPSK modulators that provide the BRF to hubs with Explorer 8300 DHCTs use a DCM of Mixed DOCSIS/DAVIC.<br>Select the appropriate DCM from one of the following choices:<br>▪ **DAVIC** - Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel. |

| | |
|---|---|
| | ▪ **Mixed DOCSIS/DAVIC** - Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel.<br>▪ **DOCSIS** - Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.) |
| Options | **Continuous Wave Mode -** Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK. |
| | **Front Panel Lock -** Determines whether changes can be made from the front panel. |
| | **Broadcast Only Mode -** Determines whether the QPSK sends priority broadcast transmissions. |
| | **Database Persistence -** Determines whether the QPSK stores the IP addresses of DHCTs in RAM.<br>**Note:** Occasionally, you may need to clear the IP addresses that DHCTs are currently using and replace them with new IP addresses. To accomplish this, use the Reset and Clear DB selection on the QPSK File menu. For more information, see Reset the QPSK Modulator Persistent Database. |

### Related Topics

- Adding a QPSK Bridge to the DNCS
- Setting Up QPSK Bridge Advanced Parameters

6. Your next step is to set up the advanced parameters for this QPSK bridge. Go to Setting Up QPSK Bridge Advanced Parameters.

### Setting Up QPSK Bridge Advanced Parameters

In general, the system sets up the QPSK bridge advanced parameters automatically, and you should not change them. However, if you need to change any advanced parameters after you have set up the basic parameters, keep in mind the following guidelines and contact Cisco Services if you need further assistance:

If you change any of the default parameters, you must stay within the signal capacity of your plant design. Otherwise, the DHCTs may not be able to communicate with the DBDS. In addition, you must reboot the QPSK bridge and wait for all corresponding DHCTs to sign on again before any changes will take effect.

1. Do not change the **Configuration File Name** parameter without first consulting Cisco Services.

2. For the **Service Channel Frequency** parameter, enter a value from 8 MHz to 26.5 MHz based on your plant design.

   **Note:** This parameter establishes the frequency that the DHCTs use to broadcast to the demodulators on this hub.

3. If you are **not** using a backup service channel, enter the same value for the **Backup Service Channel Frequency** parameter that you entered for the Service Channel Frequency parameter. Otherwise, enter a value from 8 to 26.5 MHz based on your plant design.

   **Note:** We recommend that you **not** use a backup service channel. The backup service channel is used when the service channel fails. All reverse channel messaging is sent over the channel on which the DHCT achieves initial sign-on. If a backup service channel is in use, the DHCT may not be able to achieve initial sign-on.

4. For the **Tuner Input Attenuator** parameter, select the DHCT calibration setting based on the design targets of your RF plant and the combining networks. If you need assistance, contact Cisco Services.

   **Note:** The system will not connect to any levels that are in the fail range.

After you set up the basic parameters for the QPSK bridge, complete these steps to set up the QPSK bridge advanced parameters.

1. On the Set Up QPSK Modulator window, click the **Advanced Parameters** tab. The Advanced Parameters window opens.

2. In general, the system sets up the QPSK bridge advanced parameters automatically, and you should not change them. However, if you need to change any of these parameters, refer to the guidelines listed at the beginning of this procedure.

3. Click **Save**. The system saves the advanced parameters for this QPSK bridge in the DNCS database and closes the Set Up QPSK Modulator window. The QPSK List window updates to include the new QPSK bridge.

4. Add the new QPSK bridge to your network map.

5. Do you need to add another QPSK bridge?
   - If **yes**, go back to Add a QPSK Bridge to the DNCS.
   - If **no**, select **File > Close** to close the QPSK/CMTS List.

**Explorer 8300-Series DHCTs**

## Add a CMTS Bridge to the DNCS

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

A CMTS bridge is a logical entity that serves DHCTs in the same hub. For this reason, create one CMTS bridge for every hub that serves Explorer 8300 DHCTs.

### You Need to Know

Before You Begin

Obtain a copy of your network map to ensure you can easily reference the information you need to enable each CMTS in your system for multicasting. You must also have the following information:

- Multicast IP address for each CMTS bridge

**Important:** A unique IP address that is within the range of addresses reserved for multicasting is required.

- IP address of your Session Resource Manager (SRM)
- UDP port number that the DHCT uses to communicate with the SRM

Time to Complete

Adding a CMTS bridge takes about 5 minutes.

Performance Impact

Adding a CMTS bridge to the DNCS does not impact network performance. You can complete this procedure at any time.

### Related Topics

- CMTS Bridge Settings
- Adding a CMTS Bridge to the DNCS

**Explorer 8300-Series DHCTs**

## Add a CMTS Bridge to the DNCS

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

A CMTS bridge is a logical entity that serves DHCTs in the same hub. For this reason, create one CMTS bridge for every hub that serves Explorer 8300 DHCTs.

### You Need to Know

Before You Begin

Obtain a copy of your network map to ensure you can easily reference the information you need to enable each CMTS in your system for multicasting. You must also have the following information:

- Multicast IP address for each CMTS bridge

  **Important:** A unique IP address that is within the range of addresses reserved for multicasting is required.

- IP address of your Session Resource Manager (SRM)
- UDP port number that the DHCT uses to communicate with the SRM

Time to Complete

Adding a CMTS bridge takes about 5 minutes.

Performance Impact

Adding a CMTS bridge to the DNCS does not impact network performance. You can complete this procedure at any time.

### Related Topics

- CMTS Bridge Settings
- Adding a CMTS Bridge to the DNCS

### CMTS Bridge Settings

Use the following fields when you manage a CMTS bridge in the DNCS.

| Field | Description |
|---|---|
| Hub | The hub to which the CMTS bridge is connected.<br>**Note:** If needed, you can assign a different hub to each CMTS bridge. |
| Bridge Name | The name for the bridge. |
| IP Flow | The type of IP flow this bridge will use.<br>Select **SFM** (Single Flow Multicast). |
| IP Address | A unique IP address for this bridge.<br>This IP address must be within the range of IP addresses reserved for multicasting (225.0.0.0 to 239.255.255.255).<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| DCM | The DHCT communications mode.<br>Select **DOCSIS**. |
| SRM IP | The IP address of your Session Resource Manager. |
| Disable EMM Generation | Determines whether we or another vendor provides your conditional access system.<br>Click to disable EMM generation only if a vendor other than us provides your conditional access system.<br>**Note:** When you disable PowerKEY EMMs, no DHCTs that have signed on and reported the ID for the CMTS bridge will receive PowerKEY EMMs.<br>In addition, new EMMs will not be generated for any DHCTs associated with the CMTS bridge. |

### Related Topics

- Adding a CMTS Bridge to the DNCS

### Adding a CMTS Bridge to the DNCS

Complete these steps to add a CMTS bridge to the DNCS.

1. From the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront.
2. Click the **Network Element Provisioning** tab. The Element Provisioning tab moves to the forefront.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Select **File > New > CMTS**. The Set Up CMTS Bridge window opens.
5. Complete the fields on the screen as described in CMTS Bridge Settings.

Use the following fields when you manage a CMTS bridge in the DNCS.

| Field | Description |
|---|---|
| Hub | The hub to which the CMTS bridge is connected.<br>**Note:** If needed, you can assign a different hub to each CMTS bridge. |
| Bridge Name | The name for the bridge. |
| IP Flow | The type of IP flow this bridge will use.<br>Select **SFM** (Single Flow Multicast). |
| IP Address | A unique IP address for this bridge.<br>This IP address must be within the range of IP addresses reserved for multicasting (225.0.0.0 to 239.255.255.255).<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| DCM | The DHCT communications mode.<br>Select **DOCSIS**. |
| SRM IP | The IP address of your Session Resource Manager. |
| Disable EMM Generation | Determines whether we or another vendor provides your conditional access system.<br>Click to disable EMM generation only if a vendor other than us provides your conditional access system.<br>**Note:** When you disable PowerKEY EMMs, no DHCTs that have signed on and reported the ID for the CMTS bridge will receive PowerKEY EMMs.<br>In addition, new EMMs will not be generated for any DHCTs associated with the CMTS bridge. |

**Related Topics**

- Adding a CMTS Bridge to the DNCS

6. Click **Save**. The Set Up CMTS Bridge window closes and the CMTS bridge is listed in the QPSK/CMTS List window.
7. Do you need to set up another CMTS bridge?

**Important:** When configuring single flow multicasting on the DNCS, a single multicast address is

entered for each logical CMTS bridge. Only one logical CMTS bridge is typically required for each hub; however, the system operator should carefully take into consideration the Federal Information Processing Standards (FIPS) code area when defining bridges. This may result in more than one logical bridge per hub. Because the DBDS associates channel lineups with hubs, unique hubs with at least one logical CMTS bridge and their associated multicasts must be defined for each unique channel lineup desired. The system operator must identify the physical CMTSs that are associated with each logical bridge.

- If **yes**, for each new bridge that you want to add to the DNCS, repeat this procedure from step 4.
- If **no**, you have successfully set up all the CMTS bridges for this CMTS chassis. Select **File > Close** to close the QPSK/CMTS List window.

8. Now that you have set up all of the CMTS bridges, you are ready to add a QPSK modulator to any hubs that need them. A QPSK modulator is required to feed each hub that contains Explorer 8300 DHCTs. The modulator provides the hub's Explorer 8300 DHCTs with the BRF so that these DHCTs can determine which CMTS bridge to use for DOCSIS communication. To add a QPSK modulator to any hubs that need them, see Add a QPSK Modulator.

### Register the BRF With the BFS Client

**Quick Path: DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Client > File > New Server**

Now that you have added a CMTS bridge and QPSK modulator for each hub that contains Explorer 8300 DHCTs, register the BRF server with the BFS client. When the BRF server is registered, it is able to send the BRF to DHCTs over a DAVIC/QPSK path. When DHCTs first boot, they retrieve the BRF, which contains a file mapping of hub assignments to multicast MAC addresses. Data for this file was generated from the information you entered earlier when setting up each CMTS bridge.

## You Need to Know

Time to Complete

Registering the BRF server with the BFS client takes about 10 minutes.

Performance Impact

Registering the BRF server with the BFS client does not impact network performance. You can complete this procedure at any time.

### Registering the BRF With the BFS Client

Complete these steps to register the BRF server with the BFS client.

1. From the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront.
2. Click the **Application Interface Modules** tab. The Application Interface Modules tab moves to the forefront.
3. Click **BFS Client**. The Broadcast File Server List window opens.
4. Select **File > New Server**. The Set Up Server window opens.
5. Click the **Server Name** arrow and select **brf** from the list.

   **Important:** If brf does not appear in the Server Name list, contact Cisco Services for assistance.

6. If One-Way is not enabled, click **One-Way** to enable this mode.
7. In the **Available Sources** list, click **Out of Band**. The Out of Band source is highlighted.
8. Click **Add**. The Out of Band source moves from the Available Sources list to the Selected Sources list.
9. Click **Save**. The Set Up Server window closes and the brf server icon appears in the Broadcast File Server List window.
10. In the Broadcast File Server List window, find the **brf Server** icon and select it. The brf Server icon is highlighted.
11. Select **File > New Link**. The Set Up Link window opens.
12. Click in the **Link Name** field and type **brf.cfg**.
13. Ensure that the **Source Name** field displays **Out of Band**.
14. Click in the **Linked Path** field and type **/dvs/dvsFiles/brf/brf.cfg**.
15. Click **Save**. The Set Up Link window closes, and the Broadcast File Server List window is visible. The brf.cfg link icon appears in the Broadcast File Server List window, just beneath the bfs server icon.

16. Now that you have registered the BRF server with the BFS client, update the BFS. Updating the BFS ensures that the BFS broadcasts the new file to DHCTs so the DHCTs that require the file can download it after a reboot. Go to Update the BFS.

### Register the BRF With the BFS Client

**Quick Path: DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Client > File > New Server**

Now that you have added a CMTS bridge and QPSK modulator for each hub that contains Explorer 8300 DHCTs, register the BRF server with the BFS client. When the BRF server is registered, it is able to send the BRF to DHCTs over a DAVIC/QPSK path. When DHCTs first boot, they retrieve the BRF, which contains a file mapping of hub assignments to multicast MAC addresses. Data for this file was generated from the information you entered earlier when setting up each CMTS bridge.

## You Need to Know

Time to Complete

Registering the BRF server with the BFS client takes about 10 minutes.

Performance Impact

Registering the BRF server with the BFS client does not impact network performance. You can complete this procedure at any time.

### Registering the BRF With the BFS Client

Complete these steps to register the BRF server with the BFS client.

1. From the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront.
2. Click the **Application Interface Modules** tab. The Application Interface Modules tab moves to the forefront.
3. Click **BFS Client**. The Broadcast File Server List window opens.
4. Select **File > New Server**. The Set Up Server window opens.
5. Click the **Server Name** arrow and select **brf** from the list.

   **Important:** If brf does not appear in the Server Name list, contact Cisco Services for assistance.

6. If One-Way is not enabled, click **One-Way** to enable this mode.
7. In the **Available Sources** list, click **Out of Band**. The Out of Band source is highlighted.
8. Click **Add**. The Out of Band source moves from the Available Sources list to the Selected Sources list.
9. Click **Save**. The Set Up Server window closes and the brf server icon appears in the Broadcast File Server List window.
10. In the Broadcast File Server List window, find the **brf Server** icon and select it. The brf Server icon is highlighted.
11. Select **File > New Link**. The Set Up Link window opens.
12. Click in the **Link Name** field and type **brf.cfg**.
13. Ensure that the **Source Name** field displays **Out of Band**.
14. Click in the **Linked Path** field and type **/dvs/dvsFiles/brf/brf.cfg**.
15. Click **Save**. The Set Up Link window closes, and the Broadcast File Server List window is visible. The brf.cfg link icon appears in the Broadcast File Server List window, just beneath the bfs server icon.

16. Now that you have registered the BRF server with the BFS client, update the BFS. Updating the BFS ensures that the BFS broadcasts the new file to DHCTs so the DHCTs that require the file can download it after a reboot. Go to Update the BFS.

### Update the BFS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > Open > [Select CMTS Bridge] > File > Open > Save**

Now that you have registered the BRF server with the BFS client, update the BFS. Updating the BFS ensures that the BFS broadcasts the new file to DHCTs. As a result, DHCTs check the BFS for new or revised information after a reboot, and DHCTs that require the BRF will download it.

If you do not update the BFS, Explorer 8300 DHCTs will not receive the BRF and will be unable to run in DOCSIS mode.

### You Need to Know

Time to Complete

Updating the BFS takes about one minute.

Performance Impact

Updating the BFS does not impact network performance. You can complete this procedure at any time.

### Updating the BFS

An easy way to update the BFS is to re-save an existing CMTS bridge. For assistance re-saving a CMTS bridge that you have created, follow these steps.

1. From the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront
2. Click the **Network Element Provisioning** tab. The Element Provisioning tab moves to the forefront.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Select a CMTS and click **File > Open**. The Set Up CMTS List Bridge window opens for the CMTS you selected.
5. Click **Save**. The DNCS updates the CMTS bridge and closes the Set UP CMTS Bridge window. You have successfully set up the DNCS to send the BRF to Explorer 8300 DHCTs. To close the Set Up CMTS window, click **Cancel**.
6. To close the QPSK/CMTS List window, click **File > Close**.

### Update the BFS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > Open > [Select CMTS Bridge] > File > Open > Save**

Now that you have registered the BRF server with the BFS client, update the BFS. Updating the BFS ensures that the BFS broadcasts the new file to DHCTs. As a result, DHCTs check the BFS for new or revised information after a reboot, and DHCTs that require the BRF will download it.

If you do not update the BFS, Explorer 8300 DHCTs will not receive the BRF and will be unable to run in DOCSIS mode.

### You Need to Know

Time to Complete

Updating the BFS takes about one minute.

Performance Impact

Updating the BFS does not impact network performance. You can complete this procedure at any time.

### Updating the BFS

An easy way to update the BFS is to re-save an existing CMTS bridge. For assistance re-saving a CMTS bridge that you have created, follow these steps.

1. From the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront
2. Click the **Network Element Provisioning** tab. The Element Provisioning tab moves to the forefront.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Select a CMTS and click **File > Open**. The Set Up CMTS List Bridge window opens for the CMTS you selected.
5. Click **Save**. The DNCS updates the CMTS bridge and closes the Set UP CMTS Bridge window. You have successfully set up the DNCS to send the BRF to Explorer 8300 DHCTs. To close the Set Up CMTS window, click **Cancel**.
6. To close the QPSK/CMTS List window, click **File > Close**.

## DSG Timers and Filters

The Client Filters windows allow you to change the following settings in the global default DCD (Downstream Channel Descriptor) file, which supports basic DSG:

- **Timer Settings** - These settings define the overall amount of time a DHCT's embedded cable modem waits to receive DSG packets. Timer settings can be applied to **any** system running basic DSG, including systems that use the PowerKEY® conditional access (CA) method and systems using a third-party CA method.
- **Client Filter Settings** - These settings control the provisioning of certain DSG client filter settings for DHCTs that use a third-party CA system and operate in Basic DSG mode. (Unlike the timer settings, the filter settings can be applied only to systems that use a third-party CA system. They cannot be applied to systems that use the PowerKEY CA system.)

The DCD file is loaded on the BFS in the following location: BFS:///brf/default_global.dcd.

## What do you want to do?

- Change DSG timer settings
- Define filters for DSG clients that use a third-party CA system

### Change Timer Settings for DSG

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Client Filters > Configuration**

**Important:** The DSG Timer user interface is intended for use by operators with DOCSIS network experience. If you need more detailed information on Basic DSG, please review the **DOCSIS Set-top Gateway (DSG) Interface Specification**, which you can access from the CableLabs® website (http://www.cablelabs.com/).

The Client Filters user interface allows you to change any of the pre-configured timer settings in the global default DCD (Downstream Channel Descriptor) file. These settings define the overall amount of time a set-top's embedded cable modem waits to receive DSG packets. Timer settings are pre-configured with recommended default values and are applicable to **any** system running basic DSG, including systems that use the PowerKEY® CA method and systems using a third-party CA method.

#### Changing Timer Settings for DSG

Follow these steps to change timer settings for basic DSG.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Client Filters**. The Rules for Client Filters window opens.
3. Click **Configuration**. The Configuration for Client Filters window opens.
4. Update the timer settings as necessary. The following list provides a brief description of each setting.
   - **DSG Initialization Timeout (TDSG1)** - The time the DHCT's embedded cable modem (also known as the eCM) stays on a DOCSIS channel during initialization, waiting for DSG packets to arrive from the CMTS. If DSG packets are not received within this time period, the DOCSIS channel is declared invalid, and the set-top does not lock on a particular DOCSIS channel. The default value is 2 seconds. You cannot set this timer to 0.
   - **DSG Operational Timeout (TDSG2)** - The time allowed for DSG packets to reach the set-top's embedded cable modem during normal operation. If DSG packets do not arrive within this time period, the DSG One-Way retry Timer (TDSG4) is activated. The default value for TDSG2 is 600 seconds. You cannot set this timer to 0.
   - **DSG Two-Way retry Timer (TDSG3)** - The time the set-top's embedded cable modem waits before trying to re-establish two-way connectivity with the CMTS while the embedded cable modem is in a one-way operational state. The default value is 300 seconds. You cannot set this timer to 0.

     **Note:** "One-way" and "Two-way" in these descriptions refer to the state of the embedded cable modem, not the operational state of the set-top.

   - **DSG One-Way retry Timer (TDSG4)** - Determines how long the set-top's embedded cable modem waits to rescan for a DOCSIS downstream channel that contains DSG packets after an operational timeout occurs. If this time period expires, the DOCSIS channel is declared invalid and the DHCT's embedded cable modem will scan for another DOCSIS channel. The default value is 1800 seconds. You cannot set this timer to 0.
5. When you have finished updating the settings, click **Save**. The DCD file is updated with the values and reloaded on the BFS.

#### Related Topics

- Define Third-Party Client Filters

### Change Timer Settings for DSG

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Client Filters > Configuration**

**Important:** The DSG Timer user interface is intended for use by operators with DOCSIS network experience. If you need more detailed information on Basic DSG, please review the **DOCSIS Set-top Gateway (DSG) Interface Specification**, which you can access from the CableLabs® website (http://www.cablelabs.com/).

The Client Filters user interface allows you to change any of the pre-configured timer settings in the global default DCD (Downstream Channel Descriptor) file. These settings define the overall amount of time a set-top's embedded cable modem waits to receive DSG packets. Timer settings are pre-configured with recommended default values and are applicable to **any** system running basic DSG, including systems that use the PowerKEY® CA method and systems using a third-party CA method.

### Changing Timer Settings for DSG

Follow these steps to change timer settings for basic DSG.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Client Filters**. The Rules for Client Filters window opens.
3. Click **Configuration**. The Configuration for Client Filters window opens.
4. Update the timer settings as necessary. The following list provides a brief description of each setting.
   - **DSG Initialization Timeout (TDSG1)** - The time the DHCT's embedded cable modem (also known as the eCM) stays on a DOCSIS channel during initialization, waiting for DSG packets to arrive from the CMTS. If DSG packets are not received within this time period, the DOCSIS channel is declared invalid, and the set-top does not lock on a particular DOCSIS channel. The default value is 2 seconds. You cannot set this timer to 0.
   - **DSG Operational Timeout (TDSG2)** - The time allowed for DSG packets to reach the set-top's embedded cable modem during normal operation. If DSG packets do not arrive within this time period, the DSG One-Way retry Timer (TDSG4) is activated. The default value for TDSG2 is 600 seconds. You cannot set this timer to 0.
   - **DSG Two-Way retry Timer (TDSG3)** - The time the set-top's embedded cable modem waits before trying to re-establish two-way connectivity with the CMTS while the embedded cable modem is in a one-way operational state. The default value is 300 seconds. You cannot set this timer to 0.

     **Note:** "One-way" and "Two-way" in these descriptions refer to the state of the embedded cable modem, not the operational state of the set-top.

   - **DSG One-Way retry Timer (TDSG4)** - Determines how long the set-top's embedded cable modem waits to rescan for a DOCSIS downstream channel that contains DSG packets after an operational timeout occurs. If this time period expires, the DOCSIS channel is declared invalid and the DHCT's embedded cable modem will scan for another DOCSIS channel. The default value is 1800 seconds. You cannot set this timer to 0.
5. When you have finished updating the settings, click **Save**. The DCD file is updated with the values and reloaded on the BFS.

### Related Topics

- Define Third-Party Client Filters

### Define Third-Party Client Filters

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Client Filters**

**Important:** The Client Filters user interface is intended for use by operators with DOCSIS network experience. If you need more detailed information on Basic DSG, please review the **DOCSIS Set-top Gateway (DSG) Interface Specification**, which you can access from the CableLabs website (http://www.cablelabs.com/).

The Client Filters user interface allows you to control the provisioning of certain DSG client filter settings for set-tops that use a third-party conditional access (CA) system and operate in Basic DSG mode. A client filter identifies packet characteristics (such as destination MAC address, destination IP address, and so on) with the ID of the client needing those packets. In this context, the clients are software running on set-tops operating in Basic DSG mode.

**Important:** Do **not** define basic DSG client filters to provision standard network flows on a PowerKEY-only system. Basic DSG filters for PowerKEY systems are already implicit in the Bridge Resolution File (BRF). The **Rules for Client Filters** window is provided for cable operators provisioning additional DSG flows, such as third-party CA systems.

### Client Filter Basics

To properly configure client filters through the Client Filters user interface, it is necessary to understand the way Basic DSG DHCTs are provisioned with DSG information. The system architecture for provisioning DSG information to Basic Mode DHCTs has the following key features:

- Each hub has one or more DAVIC QPSK Modulators carrying all OOB information for the hub.
- The DNCS publishes a BRF on OOB BFS that provides the mapping of hub ID to DSG Tunnel MAC address. The BRF provides the information needed by the DHCT to locate the correct DSG OOB Bridge. This file and its contents are automatically generated by the DNCS when operators set up a CMTS bridge for multicasting. No user configuration of the contents of this file is available or necessary.
- The DNCS publishes a global default DCD file on OOB BFS. The global default DCD file communicates rules, classifiers, and DSG Configuration information to DHCTs operating in Basic DSG mode. The rules and classifiers map DSG Client IDs to packet filter settings used to acquire traffic for those clients. These filter settings are in addition to the information provided in the BRF and do not affect the DHCT DOCSIS scan behaviors. The Client Filters user interface provides a way for the operator to configure the rules and classifiers portion of the global default DCD file.
- Upon boot, DHCTs operating in Basic DSG mode first find a DAVIC QPSK Modulator to obtain the correct hub ID and read the BRF before attempting to locate a DSG OOB Bridge.
- Once a DHCT has acquired the correct DSG OOB Bridge per the BRF, it uses the client filter information in the global default DCD file to acquire traffic for applicable Client IDs supported by the DHCT. The DHCT monitors the DCD file for changes and uses the latest version available.

### Related Topics

- Third-Party Client Filter Settings
- Building the Global Default DCD File

### Define Third-Party Client Filters

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Client Filters**

**Important:** The Client Filters user interface is intended for use by operators with DOCSIS network experience. If you need more detailed information on Basic DSG, please review the **DOCSIS Set-top Gateway (DSG) Interface Specification**, which you can access from the CableLabs website (http://www.cablelabs.com/).

The Client Filters user interface allows you to control the provisioning of certain DSG client filter settings for set-tops that use a third-party conditional access (CA) system and operate in Basic DSG mode. A client filter identifies packet characteristics (such as destination MAC address, destination IP address, and so on) with the ID of the client needing those packets. In this context, the clients are software running on set-tops operating in Basic DSG mode.

**Important:** Do **not** define basic DSG client filters to provision standard network flows on a PowerKEY-only system. Basic DSG filters for PowerKEY systems are already implicit in the Bridge Resolution File (BRF). The **Rules for Client Filters** window is provided for cable operators provisioning additional DSG flows, such as third-party CA systems.

### Client Filter Basics

To properly configure client filters through the Client Filters user interface, it is necessary to understand the way Basic DSG DHCTs are provisioned with DSG information. The system architecture for provisioning DSG information to Basic Mode DHCTs has the following key features:

- Each hub has one or more DAVIC QPSK Modulators carrying all OOB information for the hub.
- The DNCS publishes a BRF on OOB BFS that provides the mapping of hub ID to DSG Tunnel MAC address. The BRF provides the information needed by the DHCT to locate the correct DSG OOB Bridge. This file and its contents are automatically generated by the DNCS when operators set up a CMTS bridge for multicasting. No user configuration of the contents of this file is available or necessary.
- The DNCS publishes a global default DCD file on OOB BFS. The global default DCD file communicates rules, classifiers, and DSG Configuration information to DHCTs operating in Basic DSG mode. The rules and classifiers map DSG Client IDs to packet filter settings used to acquire traffic for those clients. These filter settings are in addition to the information provided in the BRF and do not affect the DHCT DOCSIS scan behaviors. The Client Filters user interface provides a way for the operator to configure the rules and classifiers portion of the global default DCD file.
- Upon boot, DHCTs operating in Basic DSG mode first find a DAVIC QPSK Modulator to obtain the correct hub ID and read the BRF before attempting to locate a DSG OOB Bridge.
- Once a DHCT has acquired the correct DSG OOB Bridge per the BRF, it uses the client filter information in the global default DCD file to acquire traffic for applicable Client IDs supported by the DHCT. The DHCT monitors the DCD file for changes and uses the latest version available.

### Related Topics

- Third-Party Client Filter Settings
- Building the Global Default DCD File

### Third-Party Client Filter Settings

Use the following fields when you manage third-party client filters with the DNCS.

| Field | Description |
|---|---|
| Client ID Type | **Broadcast ID** - Determines whether the traffic being sent to set-tops conforms to specific industry standards, such as SCTE 65, SCTE 18, OCAP Object Carousel, and OpenCable Common Download Carousel. |
| | **Well Known MAC** - Determines whether the client is identified with a six-byte MAC address. |
| | **CA System ID** - Determines whether the client is identified with a third-party CA system ID. |
| | **Application ID** - Refer to the DOCSIS Set-top Gateway (DSG) Interface Specification if you need information on this option. |
| Client ID | The corresponding ID or address:<br>▪If the Client ID Type is **Broadcast ID**, type the corresponding ID<br>▪If the Client ID Type is **Well Known MAC**, type the MAC address in the form AA:BB:CC:DD:EE:FF<br>▪If the Client ID Type is **CA System ID**, type the ID assigned to the set-tops (for example, 09:00 for DHCTs that receive NDS)<br>Refer to the DOCSIS Set-top Gateway (DSG) Interface Specification if you need information on this option. |
| DSG Tunnel Address | The destination MAC address of the DSG Tunnel.<br>If RFC 1112 compliant mapping is being used for this tunnel, check that the DHCT Tunnel Address and Destination IP Address match per RFC 1112. |
| Source IP Address | The IP address of the DNCS or server that originates the traffic associated with the Client ID.<br>If this information is not required, you can type **0** or leave this field blank.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Source IP Mask | The subnet mask of the originator of the associated IP address of the DNCS or server that originates the DSG data.<br>If this information is not required, you can type **0** or leave this field blank. |
| Destination IP Address | The multicast destination IP address of the traffic associated with the Client ID. |
| Destination Port Start<br>Destination Port End | The ports associated with the multicast destination.<br>Complete these fields using the following guidelines.<br>▪To specify a single port, enter the same value in both of these fields.<br>▪To specify a continuous range of a few ports, enter the lower and upper values of this range.<br>▪If no ports are being specified, leave both fields blank. |

### Building the Global Default DCD File

Follow these steps to configure the filters for the global default DCD file for your system.

**Important:** Do not define basic DSG client filters to provision standard network flows on a PowerKEY-only system.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Client Filters**. The Rules for Client Filters window opens.
3. Click **Add Rule**. The new data fields appear.
4. Complete the fields on the screen as described in Third-Party Client Filter Settings.

Use the following fields when you manage third-party client filters with the DNCS.

| Field | Description |
|---|---|
| Client ID Type | **Broadcast ID** - Determines whether the traffic being sent to set-tops conforms to specific industry standards, such as SCTE 65, SCTE 18, OCAP Object Carousel, and OpenCable Common Download Carousel. |
| | **Well Known MAC** - Determines whether the client is identified with a six-byte MAC address. |
| | **CA System ID** - Determines whether the client is identified with a third-party CA system ID. |
| | **Application ID** - Refer to the DOCSIS Set-top Gateway (DSG) Interface Specification if you need information on this option. |
| Client ID | The corresponding ID or address:<br>▪ If the Client ID Type is **Broadcast ID**, type the corresponding ID<br>▪ If the Client ID Type is **Well Known MAC**, type the MAC address in the form AA:BB:CC:DD:EE:FF<br>▪ If the Client ID Type is **CA System ID**, type the ID assigned to the set-tops (for example, 09:00 for DHCTs that receive NDS)<br>Refer to the DOCSIS Set-top Gateway (DSG) Interface Specification if you need information on this option. |
| DSG Tunnel Address | The destination MAC address of the DSG Tunnel.<br>If RFC 1112 compliant mapping is being used for this tunnel, check that the DHCT Tunnel Address and Destination IP Address match per RFC 1112. |
| Source IP Address | The IP address of the DNCS or server that originates the traffic associated with the Client ID.<br>If this information is not required, you can type **0** or leave this field blank.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Source IP Mask | The subnet mask of the originator of the associated IP address of the DNCS or server that originates the DSG data.<br>If this information is not required, you can type **0** or leave this field blank. |

| | |
|---|---|
| Destination IP Address | The multicast destination IP address of the traffic associated with the Client ID. |
| Destination Port Start | The ports associated with the multicast destination.<br>Complete these fields using the following guidelines.<br>▪ To specify a single port, enter the same value in both of these fields.<br>▪ To specify a continuous range of a few ports, enter the lower and upper values of this range.<br>▪ If no ports are being specified, leave both fields blank. |
| Destination Port End | |

5. Repeat this procedure from step 3 as needed. You can add up to 21 filters.

**Example:** If you are implementing multiple industry standard flows or if you have non-contiguous port numbers, you need to add a filter for each standard or for each range of port numbers.

6. When you have finished adding all filters for the DCD file, click **Save**. The system builds the DCD file and loads this file on the BFS in the following location: BFS:///brf/default_global.dcd.

# Enhanced Channel Maps

The Enhanced Channel Maps feature frees you from the restriction of hub-based channel maps. This gives you greater flexibility in assigning channel maps. For example, this feature allows you to add a channel that is visible to all high-definition (HD) DHCTs but does not appear on standard-definition (SD) DHCTs.

**Note:** For additional information, refer to the Enhanced Channel Maps User's Guide (part number 4011413). To obtain this guide, refer to Printed Resources.

## What do you want to do?

- Review a list of client code required to support this feature
- Verify that this feature was enabled during installation
- Learn how to provide DHCTs with enhanced channel maps
- Add a group definition rule
- Modify a group definition rule
- Delete a group definition rule
- Review tools for troubleshooting Enhanced Channel Maps

## Client Code Requirements

In order to use enhanced channel maps, the following client code must be installed on the DHCT:

- SARA 1.58 and later
- DVR 1.5.X DAVIC and later
- HD 1.5.0 and later

**Note:** Released software is available for download from our FTP site. For information about a specific version of software and how to download it, refer to the release notes for that version of software. Also refer to the Enhanced Channel Maps User's Guide (part number 4011413) for more information. To obtain a copy of these publications, see Printed Resources.

### Related Topics

- Verify That Your System Is Enabled for Enhanced Channel Maps
- Special Requirements for SSC DHCTs
- Set Up Enhanced Channel Maps
- Troubleshooting Enhanced Channel Maps

## Verify That Your System Is Enabled for Enhanced Channel Maps

The Enhanced Channel Maps feature remains inactive until installers enable a setting on the DNCS. After this setting is enabled, the Set Up Display Channel Map window allows you to associate channel maps with a Lineup Group Identifier (LUG ID).

If you determine that the Enhanced Channel Maps feature is not enabled, contact Cisco Services for assistance.

### Verifying That Your System is Enabled for Enhanced Channel Maps

1. On the DNCS Administrative Console, click **Application Interface Modules** tab.
2. Click **BFS Client**. The Broadcast File List window opens.

   **Note:** For multi-site systems (those with the RCS option enabled), the Please Select a Site window opens. From this window, click **File > All Sites** to open the Site All Sites Broadcast File List window.

3. Double-click the **sam** cabinet. The cabinet opens and displays its contents.
4. Is a folder named **lug** contained in the sam cabinet?
   - If **yes**, the Enhanced Channel Maps feature is enabled on your system.
   - If **no**, the Enhanced Channel Maps feature is not enabled. Contact Cisco Services for assistance.

### Related Topics

- Special Requirements for SSC DHCTs
- Set Up Enhanced Channel Maps

## Verify That Your System Is Enabled for Enhanced Channel Maps

The Enhanced Channel Maps feature remains inactive until installers enable a setting on the DNCS. After this setting is enabled, the Set Up Display Channel Map window allows you to associate channel maps with a Lineup Group Identifier (LUG ID).

If you determine that the Enhanced Channel Maps feature is not enabled, contact Cisco Services for assistance.

### Verifying That Your System is Enabled for Enhanced Channel Maps

1. On the DNCS Administrative Console, click **Application Interface Modules** tab.
2. Click **BFS Client**. The Broadcast File List window opens.

   **Note:** For multi-site systems (those with the RCS option enabled), the Please Select a Site window opens. From this window, click **File > All Sites** to open the Site All Sites Broadcast File List window.

3. Double-click the **sam** cabinet. The cabinet opens and displays its contents.
4. Is a folder named **lug** contained in the sam cabinet?
   - If **yes**, the Enhanced Channel Maps feature is enabled on your system.
   - If **no**, the Enhanced Channel Maps feature is not enabled. Contact Cisco Services for assistance.

### Related Topics

- Special Requirements for SSC DHCTs
- Set Up Enhanced Channel Maps

## Special Requirements for SSC DHCTs

When you create group definition rules for SSC DHCTs, create rules based only one of the following attributes:

- DHCT attributes
- CableCARD module attributes

**Note:** An SSC DHCT includes the functionality of the stand-alone DHCT, but adds the convenience of a factory-installed PowerKEY Multi-Stream CableCARD module (or M-Card). The M-Card module is mounted in the rear of the DHCT and is secured with a cover plate to deter tampering. A label provides the bar codes for the serial number and MAC address of the M-Card module is also provided on the rear panel of the DHCT.

### Rules for SSC DHCTs

Group Definition rules should use DHCT attributes for the following conditions:

- Model number
- Version number
- Physical hub where the SSC DHCT resides
- OUI

### Rules for CableCARD Modules

Group Definition rules should use CableCARD attributes for the following conditions:

- CableCARD MAC address
- PowerKEY package authorization
- Physical hub where the module resides

### Related Topics

- Set Up Enhanced Channel Maps
- Troubleshooting Enhanced Channel Maps

### Rules for SSC DHCTs

Group Definition rules should use DHCT attributes for the following conditions:

- Model number
- Version number
- Physical hub where the SSC DHCT resides
- OUI

## Special Requirements for SSC DHCTs

When you create group definition rules for SSC DHCTs, create rules based only one of the following attributes:

- DHCT attributes
- CableCARD module attributes

**Note:** An SSC DHCT includes the functionality of the stand-alone DHCT, but adds the convenience of a factory-installed PowerKEY Multi-Stream CableCARD module (or M-Card). The M-Card module is mounted in the rear of the DHCT and is secured with a cover plate to deter tampering. A label provides the bar codes for the serial number and MAC address of the M-Card module is also provided on the rear panel of the DHCT.

### Rules for SSC DHCTs

Group Definition rules should use DHCT attributes for the following conditions:

- Model number
- Version number
- Physical hub where the SSC DHCT resides
- OUI

### Rules for CableCARD Modules

Group Definition rules should use CableCARD attributes for the following conditions:

- CableCARD MAC address
- PowerKEY package authorization
- Physical hub where the module resides

### Related Topics

- Set Up Enhanced Channel Maps
- Troubleshooting Enhanced Channel Maps

## Set Up Enhanced Channel Maps

As part of setting up enhanced channel maps for your facility, you build a set of group definition rules. This page describes how to create an enhanced channel map and build a set of group definition rules.

### You Need to Know

Before You Begin

Before you begin, make certain that you understand what occurs when you build a set of group definition rules. When you create these rules, the following events occur.

- The DNCS stores these rules in a file and posts the group definition rules file on the BFS for the DHCT to read.
- When the DHCT boots up, it looks for this file on the BFS and reads the file if it exists. During normal operation, the DHCT also monitors this file for modifications.
- If the DHCT finds a rule that matches the DHCT's configuration, then it uses the first rule that matches to apply the channel map associated with that rule. If the DHCT does not find a rule that matches its configuration, it uses the channel map for the hub where it resides.

**Important:** The order of the rules in the group definition rules file is very important: the DHCT stops searching as soon as it finds a matching group definition rule. Therefore, if a DHCT matches more than one rule, it chooses the channel map associated with the first matching rule in the list. Be sure that you build the group definition rules file in the appropriate order based on your desired configuration. In addition, check for typographical errors. For example, if you type "15" for the DHCT hardware version instead of "1.5," DHCTs will ignore the rule containing this typographical error. As a result, these DHCTs may download the lug-based channel map that is associated with the next rule matching the DHCT's attributes.

### Setting Up Enhanced Channel Maps

Follow these instructions to set up an enhanced channel map:

1. Add a custom channel map to the DNCS and determine its LUG ID.

   **Example:** You might create a channel map that contains only high-definition (HD) channels. When giving a name to the channel map, we suggest that you use a name that identifies the lineup group function. For example, you might name a lug-based channel map that contains only HD channels **HD_LUG**.

   **Note:** Add a customized channel map the same way you would add a typical hub-based channel map to the DNCS. See Add a Channel Map for assistance.

2. Determine the LUG ID of the custom channel map that you created in step 1: Open the Display Channel Map window for the channel map you just created and write down the Lug ID (lineup group ID) that the DNCS assigned to the new channel map.

3. Repeat steps 1 and 2 to create other custom channel maps.

   **Note:** Several minutes after creating a new channel map, the channel map file can be viewed in the sam cabinet on the BFS Client window. New channel map files are listed under the lug folder in order by lug ID. If a channel map is associated with a hub, then the channel map file will also appear in the sam cabinet by hub ID.

4. Create a set of group definition rules that a DHCT must meet in order to receive a custom channel map (Lug ID) that you have created. The DNCS places these rules on the BFS as a file for distribution to

DHCTs. DHCTs use the file to determine their Lug ID assignment and download the appropriate channel map.

**Note:** As the last step in creating a set of group definition rules, click **Write File** to update the group_defs.txt file on the BFS with the rules you have created. After clicking Write File, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

**Important:** The order in which you create group definition rules is very important: the DHCT stops searching as soon as it finds a matching group definition rule.

## Set Up Enhanced Channel Maps

As part of setting up enhanced channel maps for your facility, you build a set of group definition rules. This page describes how to create an enhanced channel map and build a set of group definition rules.

### You Need to Know

Before You Begin

Before you begin, make certain that you understand what occurs when you build a set of group definition rules. When you create these rules, the following events occur.

- The DNCS stores these rules in a file and posts the group definition rules file on the BFS for the DHCT to read.
- When the DHCT boots up, it looks for this file on the BFS and reads the file if it exists. During normal operation, the DHCT also monitors this file for modifications.
- If the DHCT finds a rule that matches the DHCT's configuration, then it uses the first rule that matches to apply the channel map associated with that rule. If the DHCT does not find a rule that matches its configuration, it uses the channel map for the hub where it resides.

**Important:** The order of the rules in the group definition rules file is very important: the DHCT stops searching as soon as it finds a matching group definition rule. Therefore, if a DHCT matches more than one rule, it chooses the channel map associated with the first matching rule in the list. Be sure that you build the group definition rules file in the appropriate order based on your desired configuration. In addition, check for typographical errors. For example, if you type "15" for the DHCT hardware version instead of "1.5," DHCTs will ignore the rule containing this typographical error. As a result, these DHCTs may download the lug-based channel map that is associated with the next rule matching the DHCT's attributes.

### Setting Up Enhanced Channel Maps

Follow these instructions to set up an enhanced channel map:

1. Add a custom channel map to the DNCS and determine its LUG ID.

   **Example:** You might create a channel map that contains only high-definition (HD) channels. When giving a name to the channel map, we suggest that you use a name that identifies the lineup group function. For example, you might name a lug-based channel map that contains only HD channels **HD_LUG**.

   **Note:** Add a customized channel map the same way you would add a typical hub-based channel map to the DNCS. See Add a Channel Map for assistance.

2. Determine the LUG ID of the custom channel map that you created in step 1: Open the Display Channel Map window for the channel map you just created and write down the Lug ID (lineup group ID) that the DNCS assigned to the new channel map.

3. Repeat steps 1 and 2 to create other custom channel maps.

   **Note:** Several minutes after creating a new channel map, the channel map file can be viewed in the sam cabinet on the BFS Client window. New channel map files are listed under the lug folder in order by lug ID. If a channel map is associated with a hub, then the channel map file will also appear in the sam cabinet by hub ID.

4. Create a set of group definition rules that a DHCT must meet in order to receive a custom channel map (Lug ID) that you have created. The DNCS places these rules on the BFS as a file for distribution to

DHCTs. DHCTs use the file to determine their Lug ID assignment and download the appropriate channel map.

**Note:** As the last step in creating a set of group definition rules, click **Write File** to update the group_defs.txt file on the BFS with the rules you have created. After clicking Write File, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

**Important:** The order in which you create group definition rules is very important: the DHCT stops searching as soon as it finds a matching group definition rule.

### Group Definition Rule Settings

Use the following fields when you manage a group definition rule in the DNCS.

| Field | Description | |
|---|---|---|
| lug_id | The number of the Lug ID that you want to assign to these rules. This is the number that the DNCS assigned when you created the channel map | Do **only one** of these. |
| virtual_hub | The number of the virtual hub that you want to assign to these rules | |
| Conditions | Set the criteria fields that a DHCT must satisfy to receive this channel map. | |
| | **PowerKEY Package Authorization** - When entering this value, you must use a four-digit hexadecimal EID format.<br>**Example: 0x01BD**. | ▪To exclude any criteria, check the box labeled not.<br>**Example:** If you want a channel map to be used by every DHCT model except for the Explorer 2000, set the DHCT Hardware Model to **2000** and select the box labeled **not**.<br>▪Two or more sets of rules can use the same Lug ID.<br>▪If a DHCT meets more than one set of criteria (and is eligible for more than one Lug ID), the DHCT will be assigned to the first Lug ID for which it meets the conditions.<br>▪A rule must have at least one condition and only one action. |
| | **Set-Top Hardware Model** - When entering this value, you must use a four-digit model number format. **Example: 4200** or **8300**. | |
| | **Set-Top Hardware Version** - When entering this value, you must use the major #.minor # version string format.<br>**Example: 1.0**, **1.2**, or **2.1**. | |
| | **MAC Address** - Specifies the MAC Address for this LUG. | |
| | **Physical Hub** - When entering this value you must use a whole number.<br>**Example: 1**, **13**, or **44**. | |
| | **OUI** - Specifies the Organizationally Unique Identifier for this LUG. See Create a Group Definition Rule for more information. | |
| | **Bouquet Assignment** - Specifies the bouquet for this LUG. See Create a Group Definition Rule for more information. | |
| | **Service Group ID** - Specifies the Service Group ID for this LUG. See Create a Group Definition Rule for more information. | |

### Related Topics

- Add a Group Definition Rule
- Modify a Group Definition Rule

- Delete a Group Definition Rule

**Add a Group Definition Rule**

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Group Definitions > Add Rule**

After you create channel maps and determine the Lug ID that was assigned to the channel map, define a set of group definition rules that a DHCT must meet to download the appropriate channel map. The DNCS places these rules on the out-of-band BFS carousel as a file for distribution to DHCTs. A DHCT receives and parses the file to determine the Lug ID for the channel map that the DHCT should use, based on the first rule that the DHCT matches. The DHCT then downloads the appropriate channel map for its Lug ID.

Rules can be based on any one of the following attributes or on any combination of the following attributes, which are displayed in the Group Definitions window when **Add** is selected:

**Note:** In the future, other attributes may be added to the Group Definitions window.

- **PowerKEY Package Authorization (hex)** - This field specifies the Entitlement ID (EID). You can obtain this value by opening a package in the Package List window and displaying the Set Up Package List window. (When entering this value, you must use a four-digit hexadecimal EID format, for example, 0x01BD.)
- **Set-Top Hardware model (decimal)** - You can obtain this value from the Type column in the DHCT Type List window or from the label on the DHCT. (When entering this value, you must use a four-digit model number format, for example 4200 or 8300.)
- **Set-Top Hardware version (dotted decimal)** - You can obtain this value from the version number listed in the Name column on the DHCT Type List window. (When entering this value, you must use the major #.minor # version string format, for example, 1.0, 1.2, or 2.1.)
- **MAC Address (NN:NN:NN:NN:NN:NN)** - You can obtain this number by displaying page 3 of the DHCT diagnostic screen or by looking on the back of the DHCT for a label with the MAC address on it.
- **Physical hub (decimal)** - You can obtain this value from the Hub List window. (When entering this value you must use a whole number, for example, 1, 13, or 44.)
- **OUI (NN:NN:NN)** - This field specifies the organizationally unique identifier (OUI), which is the first six digits of a DHCT MAC address. The OUI is sometimes called the "company ID" portion of the MAC Address. For example, our MAC Addresses currently use an OUI of 00:14:F8.
- **Bouquet Assignment (decimal)** - Systems that use Digital Video Broadcast- Service Information (DVB-SI), instead of ATSC-SI, use bouquets.
- Service Group ID (decimal) - Specifies the Service Group ID for this LUG.

### Creating a Group Definition Rule

1. In the DNCSAdministrative Console, click the **Applications Interface Modules** tab.
2. Click **Group Definitions**. The Enhanced Channel Map Group Definitions Rules window opens.
3. Click **Add Rule**. The Conditions and Actions window opens.
4. Complete the fields on the screen as described in Group Definition Rule Settings.

Use the following fields when you manage a group definition rule in the DNCS.

| Field | Description | |
|---|---|---|
| lug_id | The number of the Lug ID that you want to assign to these rules. This is the number that the DNCS assigned when you created the channel map | Do **only one** of these. |
| virtual_hub | The number of the virtual hub that you want to assign to these rules | |
| Conditions | Set the criteria fields that a DHCT must satisfy to receive this channel map. | |
| | **PowerKEY Package Authorization** - When entering this value, you must use a four-digit hexadecimal EID format.<br>**Example: 0x01BD**. | ▪ To exclude any criteria, check the box labeled not.<br>**Example:** If you want a channel map to be used by every DHCT model except for the Explorer 2000, set the DHCT Hardware Model to **2000** and select the box labeled **not**.<br>▪ Two or more sets of rules can use the same Lug ID.<br>▪ If a DHCT meets more than one set of criteria (and is eligible for more than one Lug ID), the DHCT will be assigned to the first Lug ID for which it meets the conditions.<br>▪ A rule must have at least one condition and only one action. |
| | **Set-Top Hardware Model** - When entering this value, you must use a four-digit model number format.<br>**Example: 4200** or **8300**. | |
| | **Set-Top Hardware Version** - When entering this value, you must use the major #.minor # version string format.<br>**Example: 1.0**, **1.2**, or **2.1**. | |
| | **MAC Address** - Specifies the MAC Address for this LUG. | |
| | **Physical Hub** - When entering this value you must use a whole number.<br>**Example: 1**, **13**, or **44**. | |
| | **OUI** - Specifies the Organizationally Unique Identifier for this LUG. See Create a Group Definition Rule for more information. | |
| | **Bouquet Assignment** - Specifies the bouquet for this LUG. See Create a Group Definition Rule for more information. | |
| | **Service Group ID** - Specifies the Service Group ID for this LUG. See Create a Group Definition Rule for more information. | |

5. Click **Save**. The DNCS saves this rule in the Enhanced Channel Maps Group Definition Rules window.

**Notes:**

- A DHCT must meet all criteria in a rule to receive this channel map.
- If a DHCT meets more than one set of criteria and is eligible for more than one channel map, the DHCT will be assigned to the first channel map for which it meets conditions.
- Verify that you have entered each value correctly and that the rules are listed in the correct order. Otherwise, DHCTs may download the wrong channel map.

6. Click **Write**. The DNCS updates the **group_defs.txt** file on the BFS with the rules you have created. You can verify the update by viewing the time stamp of the file /dvs/dvsFiles/BFS/osm/group_defs.txt, or by viewing the contents of the file.

**Important:** Until you click **Write**, the group definition rules are not placed on the BFS for distribution to DHCTs. After you click Write, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

7. Click **Exit** to close the Enhanced Channel Map Group Definition Rules window.

**Note:** If you forget to click **Write** and click **Exit**, a message window opens and prompts you to save the changes you made to the Enhanced Channel Map Group Definition Rules window. Click **Save** to save your changes, or click **Cancel** to close the window without saving changes.

## Related Topics

- Modify a Group Definition Rule
- Delete a Group Definition Rule
- Troubleshooting Enhanced Channel Maps

### Modify a Group Definition Rule

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Group Definitions > [Select Rule] > Edit Selected Rule**

Complete these steps to change an existing rule.

1. In the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Group Definitions**. The Enhanced Channel Map Group Definitions Rules window opens.
3. Select the check box beside the rule that you want to change.
4. Click **Edit Selected Rule**. Conditions and Actions fields appear with existing values listed.
5. In the **Conditions** or **Actions** area, change any of the existing criteria. When making changes, keep the following information in mind:
   - To exclude any criteria, check the box labeled **not**. For example, if you want a channel map to be used by every DHCT model except for the Explorer 2000, set the DHCT Hardware Model to 2000 and select the box labeled **not**.
   - Two or more sets of rules can use the same Lug ID.
   - A rule must contain at least one condition and only one action.

**Note:** See Group Definition Rule Settings for more information on the criteria on this screen.

Use the following fields when you manage a group definition rule in the DNCS.

| Field | Description | |
|---|---|---|
| lug_id | The number of the Lug ID that you want to assign to these rules. This is the number that the DNCS assigned when you created the channel map | Do **only one** of these. |
| virtual_hub | The number of the virtual hub that you want to assign to these rules | |
| Conditions | Set the criteria fields that a DHCT must satisfy to receive this channel map. | |
| | **PowerKEY Package Authorization** - When entering this value, you must use a four-digit hexadecimal EID format.<br>**Example: 0x01BD**. | ▪To exclude any criteria, check the box labeled not.<br>**Example:** If you want a channel map to be used by every DHCT model except for the Explorer 2000, set the DHCT Hardware Model to **2000** and select the box labeled **not**.<br>▪Two or more sets of rules can use the same Lug ID.<br>▪If a DHCT meets more than one set of criteria (and is eligible for more than one |
| | **Set-Top Hardware Model** - When entering this value, you must use a four-digit model number format. **Example: 4200** or **8300**. | |
| | **Set-Top Hardware Version** - When entering this value, you must use the major #.minor # version string format.<br>**Example: 1.0**, **1.2**, or **2.1**. | |
| | **MAC Address** - Specifies the MAC Address for this LUG. | |
| | **Physical Hub** - When entering this | |

| | | |
|---|---|---|
| | value you must use a whole number.<br>**Example: 1**, **13**, or **44**. | Lug ID), the DHCT will be assigned to the first Lug ID for which it meets the conditions.<br>▪A rule must have at least one condition and only one action. |
| | **OUI** - Specifies the Organizationally Unique Identifier for this LUG. See Create a Group Definition Rule for more information. | |
| | **Bouquet Assignment** - Specifies the bouquet for this LUG. See Create a Group Definition Rule for more information. | |
| | **Service Group ID** - Specifies the Service Group ID for this LUG. See Create a Group Definition Rule for more information. | |

6.Verify that you have entered each value correctly and that the rules are listed in the correct order. Otherwise, DHCTs may download the wrong channel map.

7.Click **Save.** The DNCS saves these changes in the Enhanced Channel Maps Group Definition Rules window.

8.Click **Write**. The DNCS updates the **group_defs.txt** file on the BFS with your changes. You can verify the update by viewing the contents of the file /dvs/dvsFiles/BFS/osm/group_defs.txt.

**Important:** Until you click **Write**, the group definition rules are not placed on the BFS for distribution to DHCTs. After you click Write, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

9.Click **Exit** to close the Enhanced Channel Map Group Definition Rules window.

**Note:** If you forget to click **Write** and click **Exit**, a message window opens and prompts you to save the changes you made to the Enhanced Channel Map Group Definition Rules window. Click **Save** to save your changes, or click **Cancel** to close the window without saving changes.

## Related Topics

- Delete a Group Definition Rule
- Troubleshooting Enhanced Channel Maps

### Delete a Group Definition Rule

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Group Definitions > [Select Rule] > Delete Selected Rule**

Complete these steps to delete an existing rule.

1. In the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Group Definitions**. The Enhanced Channel Map Group Definitions Rules window opens.
3. Select the check box beside the rule that you want to delete.
4. Click **Delete**. A message window prompts you to confirm that you want to delete the selected rule.
5. Click **OK**. The rule is removed from the Enhanced Channel Map Group Definitions Rules window.
6. Click **Write**. The DNCS updates the **group_defs.txt** file on the BFS with your changes. You can verify the update by viewing the contents of the file /dvs/dvsFiles/BFS/osm/group_defs.txt.

   **Important:** Until you click **Write**, the group definition rules are not placed on the BFS for distribution to DHCTs. After you click Write, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

7. Click **Exit** to close the Enhanced Channel Map Group Definition Rules window.

   **Note:** If you forget to click **Write** and click **Exit**, a message window opens and prompts you to save the changes you made to the Enhanced Channel Map Group Definition Rules window. Click **Save** to save your changes, or click **Cancel** to close the window without saving changes.

### Related Topics

- Troubleshooting Enhanced Channel Maps

## Troubleshooting Enhanced Channel Maps

There are a few quick checks you can make from the DNCS to troubleshoot enhanced channel maps. In addition, if you have access to a local DHCT that matches a set of rules you have defined, you can use the SAM EDCT (Enhanced Display Channel Table) Information diagnostic screen to troubleshoot Enhanced Channel Maps.

**Note:** For assistance using the **SAM EDCT Information** screen to troubleshoot Enhanced Channel Map errors, refer to Enhanced Channel Maps User's Guide (part number 4011413). To obtain a copy of this publication, see Printed Resources.

The following checks can help you troubleshoot errors that may have occurred when creating enhanced channel maps:

- **Look for Lug Files in the SAM cabinet** - View the contents of the SAM cabinet in the BFS Client window to ensure that new Lug files appear there. Several minutes after creating a new Lug-based channel map, the channel map file can be viewed in the SAM cabinet on the BFS Client window. New Lug-based channel map files are listed beneath the lug folder in order by lug ID. If a channel map is associated with a hub, then the channel map file will also appear in the SAM cabinet by hub ID.
- **Look for updates to the group_defs.txt file** - View the time stamp of the /dvs/dvsFiles/BFS/DNCS/osm/group_defs.txt file to determine if it was updated after you clicked **Write** in the Enhanced Channel Map Group Definition Rules window. If the time stamp is correct, you may also want to view the contents of the group_defs.txt file to ensure that the data is correct.
- **Verify Lug ID numbers assigned to lug- based channel maps** - Open the channel map that is expected to be assigned to a DHCT, or group of DHCTs, and verify its Lug ID. Also verify that the channel slot assignments are correct.
- **Contact Cisco Services for assistance** - If you determine that the Lug files are not in the SAM cabinet or the group_defs.txt file was not updated.

# GQAM Redundancy

GQAM redundancy (also known as the **QAM Protection Switch** feature) consists of pairing two GbE GQAMs in a redundant relationship. If the primary GQAM becomes inoperative, the DNCS operator can switch to the secondary GQAM in the pair using the DNCS GUI. This switching causes the secondary GQAM to take over the processing of the broadcast sessions from the primary GQAM.

## What do you want to do?

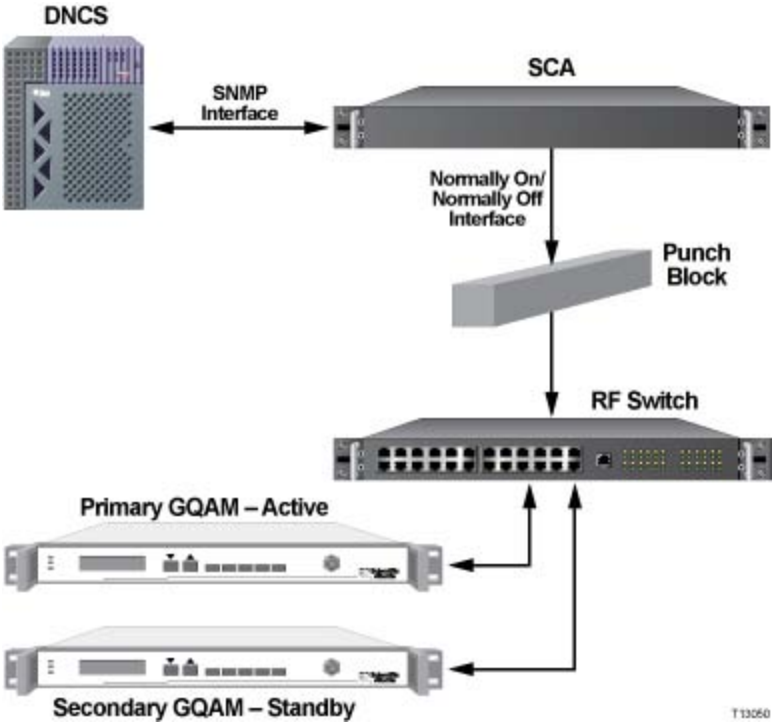
- Learn about the components used in GQAM redundancy
- Learn about the requirements for GQAM redundancy
- Learn about the types of GQAM redundancy
- Learn how to set up the system parameters for GQAM redundancy
- Learn how to set up switch control agents (SCAs)
- Learn how to set up GQAM redundancy
- Learn how to trigger the protection switch

## Components Used in GQAM Redundancy

The following components are required for setting up GQAM redundancy pairs:

- **Switch Control Agent (SCA):** A switch controller (initially, the ROSA EM) that receives and executes the forced protection switch from the Switch Control Manager. The SCA controls an RF switch.
- **RF switch:** A switch that is capable of handling three RF input pairs where each pair is composed of a primary and a secondary RF feed. This switch can isolate one of the feeds and pass the other.
- **Switch Control Manager (SCM):** Contained in the DNCS, the SCM interfaces with the SCA using SNMP and commands the SCA to switch from one GQAM to its backup GQAM.

**Note:** Only full GQAM switching is supported. Individual session switching is not supported with GQAM redundancy.




### Related Topics

- Requirements for GQAM Redundancy
- Types of GQAM Redundancy
- Set Up System Parameters for GQAM Redundancy

## Requirements for GQAM Redundancy

GQAMs available for redundancy pairs must meet the following requirements:

- They must not already be in a redundancy pair.
- They must be in a service group.
- Those GQAMs selected as the primary GQAM in the pair must carry only broadcast sessions; exclusive sessions (such as VOD or xOD) or switched (SDV) sessions cannot be processed by redundant GQAMs.
- Those GQAMs selected as the secondary GQAM in the pair must not have any existing sessions. The sessions on the primary GQAM will be duplicated onto the secondary GQAM.

### Related Topics

- Types of GQAM Redundancy
- Set Up System Parameters for GQAM Redundancy

## Types of GQAM Redundancy

GQAMs can be characterized as one of the following types, based on their inclusion and status in a redundancy pair:

- **Simplex** - An unpaired GQAM. If this GQAM is in a service group and does not have any existing sessions, it is a candidate for becoming either a primary or secondary GQAM in a redundant pair.
- **Primary** - The first GQAM in a redundant pair. In the typical setup, the primary GQAM is "online" and processing broadcast sessions.
- **Secondary** - The second or backup GQAM in a redundant pair. In the typical setup, the secondary GQAM is the "backup" GQAM. The DNCS has copied the configuration of the primary GQAM to the secondary GQAM. After you select a GQAM as a secondary GQAM in a redundant pair, you can no longer create sessions on it. When the DNCS operator triggers the protection switch, the secondary GQAM takes over the processing of the broadcast sessions from the primary GQAM.

**Related Topics**

- Set Up System Parameters for GQAM Redundancy
- Set Up Switch Control Agents
- Set Up QAM Redundancy
- Triggering the Protection Switch

# Set Up System Parameters for GQAM Redundancy

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Sys Config > Miscellaneous tab**

### Setting Up System Parameters for GQAM Redundancy

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Sys Config**. The DNCS System Configuration window opens.
4. Click the **Miscellaneous** tab.
5. In the **GQAM Redundancy Polling Interval** field, enter the number corresponding to how often (in minutes) the DNCS requests information from the SCA regarding GQAM status. You can use any number from 2 to 1440. The default value is 2 minutes.
6. In the **Switch Control Agent Trap Timeout** field, enter the number corresponding to how long (in seconds) the DNCS waits for information from the SCA, in response to the polling request, before sending another polling request. You can use any number from 1 to 600.
7. Click **Save** to save your changes and to close the DNCS System Configuration window.

### Related Topics

- Set Up Switch Control Agents
- Set Up QAM Redundancy
- Triggering the Protection Switch

# Set Up System Parameters for GQAM Redundancy

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Sys Config > Miscellaneous tab**

### Setting Up System Parameters for GQAM Redundancy

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Sys Config**. The DNCS System Configuration window opens.
4. Click the **Miscellaneous** tab.
5. In the **GQAM Redundancy Polling Interval** field, enter the number corresponding to how often (in minutes) the DNCS requests information from the SCA regarding GQAM status. You can use any number from 2 to 1440. The default value is 2 minutes.
6. In the **Switch Control Agent Trap Timeout** field, enter the number corresponding to how long (in seconds) the DNCS waits for information from the SCA, in response to the polling request, before sending another polling request. You can use any number from 1 to 600.
7. Click **Save** to save your changes and to close the DNCS System Configuration window.

### Related Topics

- Set Up Switch Control Agents
- Set Up QAM Redundancy
- Triggering the Protection Switch

## Set Up Switch Control Agents

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Switch Control Models**

The Switch Control Agent (SCA) is the entity in the DBDS that receives and executes the forced protection switch from one GbE GQAM to its backup. Initially, the SCA is the ROSA EM. The SCA is connected to an RF switch.

**Note:** Each GQAM redundancy pair is controlled by only one SCA.

### Related Topics

- Switch Control Agent Settings
- Adding an SCA

### Switch Control Agent Settings

Use the following fields when you manage SCAs for GQAM redundancy.

| Field | Description |
|---|---|
| Name | The name of this SCA.<br>You can use up to 16 alphanumeric characters. |
| IP Address | The IP address of this SCA.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address of this SCA. |
| Gateway IP Address | If your system uses a default gateway, the IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a GQAM is rebooted. |
| Subnet Mask | The subnet mask where this SCA resides.<br>Be careful to properly place the dots (.) between numbers. |

### Related Topics

- Adding an SCA

### Adding an SCA

The DNCS interfaces with the SCA using SNMP and commands the SCA to switch from one GQAM to its backup GQAM.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Switch Control Models**. The Switch Control Models List window opens listing all the available SCA models.
4. Click **New**.
5. Complete the fields on the screen as described in Switch Control Agent Settings.

   Use the following fields when you manage SCAs for GQAM redundancy.

| Field | Description |
|---|---|
| Name | The name of this SCA.<br>You can use up to 16 alphanumeric characters. |
| IP Address | The IP address of this SCA.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The MAC address of this SCA. |
| Gateway IP Address | If your system uses a default gateway, the IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a GQAM is rebooted. |
| Subnet Mask | The subnet mask where this SCA resides.<br>Be careful to properly place the dots (.) between numbers. |

#### Related Topics

- Adding an SCA

6. Click **Save**. The DNCS stores the information in its database and issues an OC event.

### Related Topics

- Set Up QAM Redundancy
- Triggering the Protection Switch

## Set Up QAM Redundancy

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > GQAM Redundancy > Administer GQAM Redundancy screen**

When you set up the redundant GQAM pair in the DNCS, the SCM copies the configuration of the primary GQAM to the secondary GQAM. If the primary GQAM becomes inoperative, the DNCS operator can trigger the protection switch. This switching causes the secondary GQAM to take over the processing of the broadcast sessions from the primary GQAM.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **GQAM Redundancy**. The Administer GQAM Redundancy screen opens and displays a list of the GQAMs in your system.
4. Select the simplex GQAM that you want to designate as the primary GQAM and click **Make Primary**. The Candidate Secondary GQAMs list opens, which lists the GQAMs that can you can choose as secondary GQAMs.

**Note:** Only those GQAMs that meet the redundancy requirements will have active Make Primary buttons or be listed as secondary GQAM candidates.

5. Select the GQAM listed in the Candidate Secondary GQAMs list that you want to designate as the secondary GQAM and click **Create Redundancy Pair**. The Switch Control Selection list opens, which lists the SCAs that you can choose to manage this redundancy pair.
6. Select the SCA that you want to use to manage this redundancy pair. A list of ports on the SCA opens.
7. Select the port on the SCA that you want to use to administer this redundancy pair.
8. Click **Save**.

**Results:**

- The DNCS replicates the sessions between the primary and secondary GQAMs when you assign the pair to an SCA port.
- You can only set up new sessions on the primary GQAM. The DNCS will replicate the new sessions on the secondary GQAM.
- The DNCS will monitor the protection switch status and the status of each GQAM in the pair (for availability, position in the pair, and which GQAM is currently online).

**Related Topics**

- Triggering the Protection Switch

## Triggering the Protection Switch

To activate the backup GQAM, you must trigger the force protection switch. This makes the backup GQAM active and takes the active GQAM offline.

**Note:** The force protection switch will not work if the target GQAM is either offline or does not have all of its redundant sessions online.

Complete these steps to trigger the protection switch and make the backup GQAM active.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **GQAM Redundancy**. The Administer GQAM Redundancy screen opens and displays a list of the redundant GQAM pairs in your system.

   **Note:** The currently active GQAM in the pair is highlighted in **GREEN** text.

4. Click **Force Protection Switch**. The Switch Control Administration screen opens.
5. Select the redundancy pair that you want to switch and click **Force Protection Switch**. The DNCS sends a message to the SCA to activate the backup GQAM in the redundancy pair.
6. Click the **Switch Control Administration** link at the top of the page to refresh the screen. The newly activated GQAM should now be highlighted in **GREEN** text.
7. Click **Exit** to close the Switch Control Administration window.

# InstaStaging

## Overview of InstaStaging

InstaStaging streamlines the staging process for two-way, PowerKEY conditional access systems. Instead of racking up large quantities of DHCTs to stage from your warehouse, you can allow professional installers or your subscribers to stage DHCTs automatically when they are installed in subscribers' homes.

**Important:** InstaStaging is not recommended for use with Separable Security Host with CableCARD Module (SSC) DHCTs.

InstaStaging provides several benefits over traditional staging methods. Staging personnel are not required to pre-stage new DHCTs or DHCTs that are returned from repair. In addition, the InstaStaging process simplifies DHCT installations by automatically sending authorization information (a "hit") when the DHCT boots in two-way mode. This feature means that installers no longer need to call in from the subscriber's home and wait for a customer service representative to send a hit to the DHCT.

**Important:** To prepare the DNCS for InstaStaging, you must stop and restart DNCS processes. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time, because when DNCS processes are stopped, two-way communication also stops in the DBDS. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator/demodulator code. For this reason, prepare your DNCS for InstaStaging during a period when system usage is low, such as during a maintenance window.

## What do you want to do?

- Review the requirements for InstaStaging
- Get an overview of InstaStaging methods
- Learn how to prepare the DNCS to support InstaStaging
- Review the processes for InstaStaging DHCTs

# InstaStaging

## Overview of InstaStaging

InstaStaging streamlines the staging process for two-way, PowerKEY conditional access systems. Instead of racking up large quantities of DHCTs to stage from your warehouse, you can allow professional installers or your subscribers to stage DHCTs automatically when they are installed in subscribers' homes.

**Important:** InstaStaging is not recommended for use with Separable Security Host with CableCARD Module (SSC) DHCTs.

InstaStaging provides several benefits over traditional staging methods. Staging personnel are not required to pre-stage new DHCTs or DHCTs that are returned from repair. In addition, the InstaStaging process simplifies DHCT installations by automatically sending authorization information (a "hit") when the DHCT boots in two-way mode. This feature means that installers no longer need to call in from the subscriber's home and wait for a customer service representative to send a hit to the DHCT.

**Important:** To prepare the DNCS for InstaStaging, you must stop and restart DNCS processes. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time, because when DNCS processes are stopped, two-way communication also stops in the DBDS. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator/demodulator code. For this reason, prepare your DNCS for InstaStaging during a period when system usage is low, such as during a maintenance window.

## What do you want to do?

- Review the requirements for InstaStaging
- Get an overview of InstaStaging methods
- Learn how to prepare the DNCS to support InstaStaging
- Review the processes for InstaStaging DHCTs

## Requirements for InstaStaging

To use InstaStaging, your system must meet the following requirements:

- System Release (SR) 2.5/3.5, SR 4.0, CV SR 3.3, or later must be installed.
- You must not use Separable Security with CableCARD Module (SSC) set-tops in your system.
- The billing system must be configured to assign an Out-Of-Service status to DHCTs when they are placed in inventory.
- The DNCS must be configured to support InstaStaging.
- The DHCT must be able to boot in two-way mode.

**Note**: You can use InstaStaging in sites that use either the SARA or the Passport application servers.

**Important:** InstaStaging is not recommended for use with Separable Security Host with CableCARD Module (SSC) DHCTs.

### Related Topics

- Overview of InstaStaging
- InstaStaging Methods
- Prepare the DNCS for InstaStaging

## InstaStaging Methods

The InstaStaging process supports the following configurations. A site may choose to use only one of these methods or both of these methods. Each DHCT will stage according to the administrative status it receives.

- Subscriber Chooses Services - Allows the subscriber to choose a group of services before installing the DHCT. When using this method, the DHCT must have an administrative status of In-Service Two-Way.
- Using Default Packages - Assigns a default group of services and adjusts the DHCT to receive the requested services at a later time. When using this method, the DHCT must have an administrative status of Out-Of-Service or Deployed Status.

**Important:** To successfully use the InstaStaging process, certain requirements must be in place. To review a list of these requirements, refer to Requirements for InstaStaging.

### Subscriber Chooses Services

If you want subscribers to choose the services they want before installing DHCTs, give those DHCTs an administrative status of In-Service Two-Way in the billing system. Subscribers choose the services they want to receive when they pick up the DHCT for installation. This method was designed to accommodate self-installations.

Before the DHCT is installed, the billing system must send the following two transactions:

- **ModifyDhctAdminStatus** to set the administrative status to In-Service Two-Way.
- **ModifyDhctConfiguration** to authorize the DHCT for the customer's requested service level.

For example, the DHCT may be placed on the subscriber's account from a retail center. This action triggers the billing system to set the administrative status to In-Service Two-Way and to associate the packages that the subscriber ordered with the DHCT. When the DHCT is installed and boots in two-way mode, the DNCS sends the Entitlement Management Messages (EMMs) and package authorizations for the services that the subscriber ordered, and the subscriber begins receiving services.

### Using Default Packages (Out-Of-Service or Deployed Status)

If you use default staging packages, you must use the DNCS to identify the packages that make up your default level of services. Whenever you set the status for a DHCT to Out-Of-Service, the DNCS automatically changes the status to Deployed. In this way, the DHCT is ready for redistribution as soon as it is taken out of service.

**Note:** You will continue to perform batch installations of new DHCTs using the method described in the Explorer Digital Home Communications Terminal Staging Guide (part number 734375). The DNCS automatically changes the status of the new DHCTs from Out-Of-Service to Deployed.

- When the DHCT signs on for the first time, the DNCS sends all of the EMMs and package authorizations for the default packages, and the subscriber begins receiving the default services.
- When the DHCT is added to the subscriber's account, the DHCT will be upgraded or downgraded to receive only the requested services.

This InstaStaging method works well for installations performed by a technician. In this case, the subscriber continues to receive the default services, which may include premium services, until the DHCT is added to the subscriber's account.

**Important:** If you use this method, you should be sure that you have tight inventory controls in place. If you do not, you run the risk of theft of services if a DHCT is distributed, but is never added to a subscriber's account.

**Note**: DHCTs in a deployed status will not receive updated EMMs. As a result, these DHCTs will function for only

30 days (or for the time limit set for EMMs in your network).

### Related Topics

- Processes for InstaStaging DHCTs
- Prepare the DNCS for InstaStaging

### Subscriber Chooses Services

If you want subscribers to choose the services they want before installing DHCTs, give those DHCTs an administrative status of In-Service Two-Way in the billing system. Subscribers choose the services they want to receive when they pick up the DHCT for installation. This method was designed to accommodate self-installations.

Before the DHCT is installed, the billing system must send the following two transactions:

- **ModifyDhctAdminStatus** to set the administrative status to In-Service Two-Way.
- **ModifyDhctConfiguration** to authorize the DHCT for the customer's requested service level.

For example, the DHCT may be placed on the subscriber's account from a retail center. This action triggers the billing system to set the administrative status to In-Service Two-Way and to associate the packages that the subscriber ordered with the DHCT. When the DHCT is installed and boots in two-way mode, the DNCS sends the Entitlement Management Messages (EMMs) and package authorizations for the services that the subscriber ordered, and the subscriber begins receiving services.

## InstaStaging Methods

The InstaStaging process supports the following configurations. A site may choose to use only one of these methods or both of these methods. Each DHCT will stage according to the administrative status it receives.

- Subscriber Chooses Services - Allows the subscriber to choose a group of services before installing the DHCT. When using this method, the DHCT must have an administrative status of In-Service Two-Way.
- Using Default Packages - Assigns a default group of services and adjusts the DHCT to receive the requested services at a later time. When using this method, the DHCT must have an administrative status of Out-Of-Service or Deployed Status.

**Important:** To successfully use the InstaStaging process, certain requirements must be in place. To review a list of these requirements, refer to Requirements for InstaStaging.

### Subscriber Chooses Services

If you want subscribers to choose the services they want before installing DHCTs, give those DHCTs an administrative status of In-Service Two-Way in the billing system. Subscribers choose the services they want to receive when they pick up the DHCT for installation. This method was designed to accommodate self-installations.

Before the DHCT is installed, the billing system must send the following two transactions:

- **ModifyDhctAdminStatus** to set the administrative status to In-Service Two-Way.
- **ModifyDhctConfiguration** to authorize the DHCT for the customer's requested service level.

For example, the DHCT may be placed on the subscriber's account from a retail center. This action triggers the billing system to set the administrative status to In-Service Two-Way and to associate the packages that the subscriber ordered with the DHCT. When the DHCT is installed and boots in two-way mode, the DNCS sends the Entitlement Management Messages (EMMs) and package authorizations for the services that the subscriber ordered, and the subscriber begins receiving services.

### Using Default Packages (Out-Of-Service or Deployed Status)

If you use default staging packages, you must use the DNCS to identify the packages that make up your default level of services. Whenever you set the status for a DHCT to Out-Of-Service, the DNCS automatically changes the status to Deployed. In this way, the DHCT is ready for redistribution as soon as it is taken out of service.

**Note:** You will continue to perform batch installations of new DHCTs using the method described in the Explorer Digital Home Communications Terminal Staging Guide (part number 734375). The DNCS automatically changes the status of the new DHCTs from Out-Of-Service to Deployed.

- When the DHCT signs on for the first time, the DNCS sends all of the EMMs and package authorizations for the default packages, and the subscriber begins receiving the default services.
- When the DHCT is added to the subscriber's account, the DHCT will be upgraded or downgraded to receive only the requested services.

This InstaStaging method works well for installations performed by a technician. In this case, the subscriber continues to receive the default services, which may include premium services, until the DHCT is added to the subscriber's account.

**Important:** If you use this method, you should be sure that you have tight inventory controls in place. If you do not, you run the risk of theft of services if a DHCT is distributed, but is never added to a subscriber's account.

**Note**: DHCTs in a deployed status will not receive updated EMMs. As a result, these DHCTs will function for only 30 days (or for the time limit set for EMMs in your network).

### Related Topics

- Processes for InstaStaging DHCTs
- Prepare the DNCS for InstaStaging

### Processes for InstaStaging DHCTs

This section lists the work flow for each InstaStaging method.

### Subscriber Chooses Services (In- Service Two-Way Status)

The following describes the InstaStaging process that is followed when the subscriber chooses services.

1. Load the EMM CD with no options.
2. Billing changes the status to In-Service Two-Way and adds packages.
3. In the subscriber's home, connect the RF input and power supply.
4. Wait for the DHCT to download software.
5. Press the power button to sign-on two-way.
6. The DNCS sends staging EMMs and authorization for selected services.
7. The DHCT receives the selected services.

### Using Default Packages (Out-Of-Service or Deployed Status)

The following describes the InstaStaging process that is followed when default packages are used.

1. Load the EMM CD with no options.
2. In the subscriber's home, connect the RF input and power supply.
3. Wait for the DHCT to download software.
4. Press the power button to sign on two-way.
5. The DNCS sends staging EMMs and the default package authorization.
6. Process the work order and update the DHCT with selected services.

### Related Topics

- Prepare the DNCS for InstaStaging

## Prepare the DNCS for InstaStaging

This section summarizes the steps you need to take in order to prepare the DNCS for InstaStaging. We recommend that you read all of the information on this page before attempting to prepare the DNCS for InstaStaging.

### You Need to Know

Before You Begin

Some of the procedures required to prepare the DNCS for InstaStaging require advanced knowledge of UNIX, including experience with UNIX vi editor. UNIX vi editor is not intuitive. Be aware that these instructions are no substitute for an advanced working knowledge of vi. For this reason, we recommend that you do not proceed unless you have experience with UNIX vi editor.

Time to Complete

Preparing the DNCS for InstaStaging takes approximately 15 minutes. However, as part of this process, you will stop and restart the DNCS. Stopping and restarting the DNCS properly can take from 10 minutes to several hours, depending on the size of your system and how many sessions are active. For this reason, prepare the DNCS for InstaStaging during a period when system usage is low, such as during a maintenance window.

Performance Impact

Most of the procedures that you will complete do not impact the network and can be performed at any time. However, in order enable InstaStaging, you must stop and re- start the DNCS. When DNCS processes are stopped, two-way communication also stops in the DBDS. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator/demodulator code.

For this reason, stop and restart the DNCS during a period when system usage is low, such as during a scheduled maintenance window.

### Preparing the DNCS for InstaStaging

The following steps give an overview of the process you must follow to prepare the DNCS for InstaStaging. Click any link to display step-by-step instructions for the procedures summarized here.

**Important:** InstaStaging is not recommended for use with Separable Security Host with CableCARD Module (SSC) DHCTs.

1. Add the InstaStaging Flag to the .profile File. To enable InstaStaging, add the InstaStaging flag to the .profile file and then stop and restart the DNCS. Until the DNCS is stopped and restarted, InstaStaging remains disabled.

   **Important:** When DNCS processes are stopped, two-way communication also stops in the DBDS. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator /demodulator code. For this reason, stop and restart the DNCS during a period when system usage is low, such as during a maintenance window.

2. Choose the InstaStaging method (or methods) that you want to use: provide default packages and/or allow subscribers to choose services. For assistance, see Choose InstaStaging Methods for Your Site.

3. If you are using default staging packages to provision DHCTs, set IPPV and VOD options. For assistance, see Set InstaStaging Options.

4. If you are using default staging packages to provision DHCTs, set up default staging packages on the DNCS. For assistance, see Add a Service Package.

5. You can also identify existing packages as default packages for InstaStaging.

## Prepare the DNCS for InstaStaging

This section summarizes the steps you need to take in order to prepare the DNCS for InstaStaging. We recommend that you read all of the information on this page before attempting to prepare the DNCS for InstaStaging.

### You Need to Know

Before You Begin

Some of the procedures required to prepare the DNCS for InstaStaging require advanced knowledge of UNIX, including experience with UNIX vi editor. UNIX vi editor is not intuitive. Be aware that these instructions are no substitute for an advanced working knowledge of vi. For this reason, we recommend that you do not proceed unless you have experience with UNIX vi editor.

Time to Complete

Preparing the DNCS for InstaStaging takes approximately 15 minutes. However, as part of this process, you will stop and restart the DNCS. Stopping and restarting the DNCS properly can take from 10 minutes to several hours, depending on the size of your system and how many sessions are active. For this reason, prepare the DNCS for InstaStaging during a period when system usage is low, such as during a maintenance window.

Performance Impact

Most of the procedures that you will complete do not impact the network and can be performed at any time. However, in order enable InstaStaging, you must stop and re- start the DNCS. When DNCS processes are stopped, two-way communication also stops in the DBDS. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator/demodulator code.

For this reason, stop and restart the DNCS during a period when system usage is low, such as during a scheduled maintenance window.

### Preparing the DNCS for InstaStaging

The following steps give an overview of the process you must follow to prepare the DNCS for InstaStaging. Click any link to display step-by-step instructions for the procedures summarized here.

**Important:** InstaStaging is not recommended for use with Separable Security Host with CableCARD Module (SSC) DHCTs.

1. Add the InstaStaging Flag to the .profile File. To enable InstaStaging, add the InstaStaging flag to the .profile file and then stop and restart the DNCS. Until the DNCS is stopped and restarted, InstaStaging remains disabled.

   **Important:** When DNCS processes are stopped, two-way communication also stops in the DBDS. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator /demodulator code. For this reason, stop and restart the DNCS during a period when system usage is low, such as during a maintenance window.

2. Choose the InstaStaging method (or methods) that you want to use: provide default packages and/or allow subscribers to choose services. For assistance, see Choose InstaStaging Methods for Your Site.

3. If you are using default staging packages to provision DHCTs, set IPPV and VOD options. For assistance, see Set InstaStaging Options.

4. If you are using default staging packages to provision DHCTs, set up default staging packages on the DNCS. For assistance, see Add a Service Package.

5. You can also identify existing packages as default packages for InstaStaging.

### Add the InstaStaging Flag to the .profile File

The first step in preparing the DNCS for InstaStaging is to add the InstaStaging file to the .profile file. Adding the InstaStaging flag to this file enables InstaStaging as soon as the DNCS is stopped and restarted. Until the DNCS is stopped and restarted, InstaStaging remains disabled.

The InstaStaging flag serves two functions:

- Whenever a DHCT receives a status of Out-Of-Service, the DNCS automatically changes the status to Deployed to prepare the DHCT for InstaStaging.
- The DNCS sends new staging EMMs to any DHCT with a status of Deployed or In-Service Two-Way the first time the DHCT makes a two-way connection to the network.

### You Need to Know

Before You Begin

Completing this procedure requires advanced knowledge of UNIX, including experience with UNIX vi editor. UNIX vi editor is not intuitive. Be aware that the instructions provided here are no substitute for an advanced working knowledge of vi. For this reason, we recommend that you do not proceed unless you have experience with UNIX vi editor.

Time to Complete

Adding the InstaStaging flag to the .profile file takes about 15 minutes.

Stopping and restarting the DNCS properly can take from 10 minutes to several hours, depending on the size of your system, how many sessions are active, and so forth.

Performance Impact

To enable InstaStaging, stop and re-start the DNCS. When DNCS processes are stopped, two-way communication also stops in the DBDS. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator /demodulator code.

For this reason, stop and restart the DNCS during a period when system usage is low.

### Adding the InstaStaging Flag to the .profile File

Complete these steps to add the InstaStaging flag to the .profile file.

**Important:** The UNIX vi editor is case-sensitive. Type each command exactly as shown in these instructions.

1. Log into an xterm window on the DNCS as the **dncs** user.
2. Type **cd /export/home/dncs** and press **Enter**. The directory /export/home/dncs becomes the working directory.
3. Type **cp .profile .profile.old** and press **Enter**. The system makes a backup copy of the file .profile, and names the backup copy .profile.old.
4. Use the UNIX editor of your choice to edit the .profile file and add the following two lines:

   **####Setting the flag for InstaStaging ####**.

**HCTM_PROVISIONING_APP=1; export HCTM_PROVISIONING_APP**

5. Save your changes and close the .profile file.

6. Stop and restart the DNCS to ensure that all processes are synchronized. For assistance, go to Stopping DNCS Processes.

7. After you stop and restart the DNCS, you are ready to Choose InstaStaging Methods for Your Site.

### Add the InstaStaging Flag to the .profile File

The first step in preparing the DNCS for InstaStaging is to add the InstaStaging file to the .profile file. Adding the InstaStaging flag to this file enables InstaStaging as soon as the DNCS is stopped and restarted. Until the DNCS is stopped and restarted, InstaStaging remains disabled.

The InstaStaging flag serves two functions:

- Whenever a DHCT receives a status of Out-Of-Service, the DNCS automatically changes the status to Deployed to prepare the DHCT for InstaStaging.
- The DNCS sends new staging EMMs to any DHCT with a status of Deployed or In-Service Two-Way the first time the DHCT makes a two-way connection to the network.

### You Need to Know

Before You Begin

Completing this procedure requires advanced knowledge of UNIX, including experience with UNIX vi editor. UNIX vi editor is not intuitive. Be aware that the instructions provided here are no substitute for an advanced working knowledge of vi. For this reason, we recommend that you do not proceed unless you have experience with UNIX vi editor.

Time to Complete

Adding the InstaStaging flag to the .profile file takes about 15 minutes.

Stopping and restarting the DNCS properly can take from 10 minutes to several hours, depending on the size of your system, how many sessions are active, and so forth.

Performance Impact

To enable InstaStaging, stop and re-start the DNCS. When DNCS processes are stopped, two-way communication also stops in the DBDS. As a result, you will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator /demodulator code.

For this reason, stop and restart the DNCS during a period when system usage is low.

### Adding the InstaStaging Flag to the .profile File

Complete these steps to add the InstaStaging flag to the .profile file.

**Important:** The UNIX vi editor is case-sensitive. Type each command exactly as shown in these instructions.

1. Log into an xterm window on the DNCS as the **dncs** user.
2. Type **cd /export/home/dncs** and press **Enter**. The directory /export/home/dncs becomes the working directory.
3. Type **cp .profile .profile.old** and press **Enter**. The system makes a backup copy of the file .profile, and names the backup copy .profile.old.
4. Use the UNIX editor of your choice to edit the .profile file and add the following two lines:

**####Setting the flag for InstaStaging ####**.

**HCTM_PROVISIONING_APP=1; export HCTM_PROVISIONING_APP**

5. Save your changes and close the .profile file.

6. Stop and restart the DNCS to ensure that all processes are synchronized. For assistance, go to Stopping DNCS Processes.

7. After you stop and restart the DNCS, you are ready to Choose InstaStaging Methods for Your Site.

### Choose InstaStaging Methods for Your Site

After you add the InstaStaging flag to the .profile file, your next step is to choose whether or not you want to set up default packages for new subscribers. If you do not want to use default staging packages, then subscribers must choose the services that they want and billing must send this information to the DNCS before installing the DHCT.

If you choose to use default staging packages, you must define the default packages that each DHCT will receive when it is installed. You can use either of the following methods to define default packages:

- Create a new service package as a default package and provision it accordingly. For assistance, see Add a Service Package.
- Define existing service packages as a default packages that every DHCT should receive. For assistance, see Identify Existing Packages as Default Packages.

**Note:** For more information on InstaStaging Methods, see InstaStaging Methods.

## Set InstaStaging Options

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DNCS System > InstaStaging tab > [Select Desired Options] > Save**

If you are using default packages to provision DHCTs and you have already added the InstaStaging flag to the .profile File, set the impulse-pay-per-view (IPPV) and video-on-demand (VOD) options for DHCTs to be deployed. Once set, the InstaStaging process will use these settings for DHCTs that sign on with an administrative status of Deployed. This topic provides instructions for setting InstaStaging options.

**Note:** These settings are applied only to DHCTs that are provisioned using default packages. If default packages are not used, the specific settings assigned to each individual box are applied.

Complete these steps to set InstaStaging options.

### Setting InstaStaging Options

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DNCS System**. The DNCS System Configuration window opens.
4. Click the **InstaStaging** tab and make the following selections:
   - Click **IPPV Enable** to allow DHCTs provisioned with default packages to support IPPV purchases. (The default setting is Enabled.) When enabled, the IPPV Credit Limit and Maximum IPPV Events fields become available.
   - In the **IPPV Credit Limit** field, enter the credit limit that your company allows for IPPV purchases. (The default setting is 5.)
   - In the **Maximum IPPV Events** field, enter the maximum number of IPPV events that your company allows for each DHCT. (The default setting is 1.)
   - Click **IPPV Acknowledge** to specify whether an "acknowledge" EMM is generated for IPPV purchases reported by DHCTs. When enabled, an Acknowledge EMM is sent to clear purchase records from the DHCT. If purchases are not cleared, the DHCT will eventually disallow further IPPV purchases when the current cache of purchase records equals the number defined by the Maximum IPPV Events setting. (The default setting is Enabled.)
5. Click **Save**. The InstaStaging process uses these settings for all DHCTs that sign on with an administrative status of Deployed.
6. Your next step is to add a default staging package to the DNCS. Go to Add a Service Package.

## Set InstaStaging Options

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DNCS System > InstaStaging tab > [Select Desired Options] > Save**

If you are using default packages to provision DHCTs and you have already added the InstaStaging flag to the .profile File, set the impulse-pay-per-view (IPPV) and video-on-demand (VOD) options for DHCTs to be deployed. Once set, the InstaStaging process will use these settings for DHCTs that sign on with an administrative status of Deployed. This topic provides instructions for setting InstaStaging options.

**Note:** These settings are applied only to DHCTs that are provisioned using default packages. If default packages are not used, the specific settings assigned to each individual box are applied.

Complete these steps to set InstaStaging options.

### Setting InstaStaging Options

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DNCS System**. The DNCS System Configuration window opens.
4. Click the **InstaStaging** tab and make the following selections:
   - Click **IPPV Enable** to allow DHCTs provisioned with default packages to support IPPV purchases. (The default setting is Enabled.) When enabled, the IPPV Credit Limit and Maximum IPPV Events fields become available.
   - In the **IPPV Credit Limit** field, enter the credit limit that your company allows for IPPV purchases. (The default setting is 5.)
   - In the **Maximum IPPV Events** field, enter the maximum number of IPPV events that your company allows for each DHCT. (The default setting is 1.)
   - Click **IPPV Acknowledge** to specify whether an "acknowledge" EMM is generated for IPPV purchases reported by DHCTs. When enabled, an Acknowledge EMM is sent to clear purchase records from the DHCT. If purchases are not cleared, the DHCT will eventually disallow further IPPV purchases when the current cache of purchase records equals the number defined by the Maximum IPPV Events setting. (The default setting is Enabled.)
5. Click **Save**. The InstaStaging process uses these settings for all DHCTs that sign on with an administrative status of Deployed.
6. Your next step is to add a default staging package to the DNCS. Go to Add a Service Package.

### Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

**You Need to Know**

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

**Guidelines for Adding Services**

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.
- You must add a service package for each VOD service. Otherwise, your authorized subscribers will not be able to access the VOD service.
- Because clear services are not encrypted, packaging a clear service does not protect it from being

accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

**Related Topics**

- Service Package Settings
- Adding a Service Package

### Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

#### You Need to Know

▸ Time to Complete

Adding a service package takes approximately 10 minutes.

▸ Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

#### Guidelines for Adding Services

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.
- You must add a service package for each VOD service. Otherwise, your authorized subscribers will not be able to access the VOD service.
- Because clear services are not encrypted, packaging a clear service does not protect it from being

accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

**Related Topics**

- Service Package Settings
- Adding a Service Package

### Service Package Settings

Use the following fields when you manage a service package in the DNCS.

| Field | Description |
|---|---|
| Package Name | The name that identifies this package.<br><br>You can use up to 20 alphanumeric characters.<br><br>**Important:** The package name that you enter must be compatible with the package name rules that your billing system uses. Default packages (those used for InstaStaging) are the only exception.<br><br>**Notes:**<br><br>▪The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br><br>▪Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Default Staging Package | Allows you to define a package as a default staging package.<br><br>This option appears only if you have enabled InstaStaging on the DNCS.<br><br>**Notes:**<br><br>▪The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br><br>▪Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Duration | Allows subscribers to have unlimited access to the package.<br><br>The **Unlimited** option in the Duration field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services. |
| Pay Per View | Not supported at this time. |
| Impulse Pay Per View | Not supported at this time. |
| Allow Event Extension | Not supported at this time. |

### Related Topics

- Adding a Service Package
- Guidelines for Adding Services

### Adding a Service Package

Complete these steps to add a new service package to the DNCS.

**Note:** This procedure applies to secure, VOD, and packaged clear services and default staging packages when using InstaStaging. It does not apply to PPV or unpackaged clear services.

**Packages for InstaStaging:** If you are adding default packages for use with InstaStaging, be aware that you can specify multiple default packages. In addition, if your site is a SARA site and uses a Service Disconnect package (sometimes referred to as a "brick mode" package), be sure that the default staging option is selected for the Service Disconnect package.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.

   **Note:** By default, the Package List window shows only non-PPV packages (Subscription Only). To view the list of all packages, click the **Show** button and select **All Packages**.

4. Click **File > New**. The Set Up Package window opens.
5. Complete the fields on the screen as described in Service Package Settings.

Use the following fields when you manage a service package in the DNCS.

| Field | Description |
|---|---|
| Package Name | The name that identifies this package.<br><br>You can use up to 20 alphanumeric characters.<br><br>**Important:** The package name that you enter must be compatible with the package name rules that your billing system uses. Default packages (those used for InstaStaging) are the only exception.<br><br>**Notes:**<br>▪ The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br>▪ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Default Staging Package | Allows you to define a package as a default staging package.<br><br>This option appears only if you have enabled InstaStaging on the DNCS.<br><br>**Notes:**<br>▪ The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br>▪ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Duration | Allows subscribers to have unlimited access to the package.<br><br>The **Unlimited** option in the Duration field is selected by default. This option |

| | |
|---|---|
| | allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services. |
| Pay Per View | Not supported at this time. |
| Impulse Pay Per View | Not supported at this time. |
| Allow Event Extension | Not supported at this time. |

**Related Topics**

- Adding a Service Package
- Guidelines for Adding Services

6.Click **Save**. The system saves the package information in the DNCS database and closes the Set Up Package window. The Package List window updates to include the new package.

**Note:** If you are using InstaStaging and have created a default staging package, an asterisk (*) appears next to this package to indicate it is a default staging package.

7.Are you using our RCS solution?

- If **yes**, go to step 8.
- If **no**, go to step 9.

8.Are there other RCS sites that will use the third-party application that this package provides?

- If **yes**, repeat this procedure from step 4 to add a package to another site.
- If **no**, go to step 9.

9.Do you need to add a secure service to this package?

- If **yes**, go to Adding a Secure Service to a Package.
- If no, go to step 10.

10.Do you need to add a VOD or clear service to this package?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to step 11.

11.Are you setting up Instastaging?

- If **yes**, you need to Identify Existing Packages as Default Packages.
- If **no**, go to step 12.

12.Click **File > Close** to close the Package List window.

13.Go to Registering a Service.

### Identify Existing Packages as Default Packages

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > [Select package] > Default Staging Package option > Save**

Complete these steps if you want to identify existing packages that every DHCT should receive.

### Identifying Existing Packages as Default Packages

**Note:** If your site uses SARA, you must identify the following packages as default packages:

- The brick mode package (if used), even if you have created a new default package.
- Some third-party applications use EIDs as part of the SAM URL. If you want the DHCT to receive any of these applications, you must identify them as default packages.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.
4. Double-click the name of the package that you want to identify as a default staging package.
5. Select the **Default Staging Package** box.
6. Click **Save**. In the Package List window, an asterisk (*) appears, indicating that this package is a default staging package.

### Identify Existing Packages as Default Packages

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > [Select package] > Default Staging Package option > Save**

Complete these steps if you want to identify existing packages that every DHCT should receive.

### Identifying Existing Packages as Default Packages

**Note:** If your site uses SARA, you must identify the following packages as default packages:

- The brick mode package (if used), even if you have created a new default package.
- Some third-party applications use EIDs as part of the SAM URL. If you want the DHCT to receive any of these applications, you must identify them as default packages.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.
4. Double-click the name of the package that you want to identify as a default staging package.
5. Select the **Default Staging Package** box.
6. Click **Save**. In the Package List window, an asterisk (*) appears, indicating that this package is a default staging package.

# Multiple Bootloader Carousels

This section discusses the benefits of using multiple bootloader carousels and provides examples of ways you might configure multiple bootloader carousels.

With multiple bootloader carousels, the BFS can send set-top software version images using more than one carousel. This enhancement gives you the flexibility you need to reduce download times and maintain system performance by creating the optimal number of bootloader carousels for your system.

**Note:** You must have DNCS System Release 4.3 or later to use the multiple bootloader feature.

## What do you want to do?

- Learn why you would use multiple bootloader carousels
- Learn the different ways to configure multiple bootloader carousels
- Set up multiple bootloader carousels
- Determine the bandwidth available for multiple bootloader carousels
- Review the settings for multiple bootloader carousels
- Add a bootloader source
- Configure set-tops to download images from a specific carousel

## Why Use Multiple Bootloaders?

Using more than one carousel can help you use the Broadcast File System (BFS) more efficiently. The packet interleave algorithm used by the DNCS allows a 1 MB image (file) to download in the same amount of time as an 8 MB file. In each case, it takes one full revolution of the carousel.

One way to optimize the carousels is to arrange the files so that each carousel is approximately the same size. Another option is to put the images for the new types of devices being staged (M-Card modules and hosts, for example) on one carousel and put the images for all legacy types on another.

We recommend that you place the images of similar devices on their own bootloader (for example, standalone M-Card module images on one bootloader and SSC set-top images on another). That way, you can keep the image sizes and cycle times appropriate for each device type.

**Important:** When you use more than one carousel, you should make certain that the BFS QAM has enough bandwidth to support a second bootloader carousel. Go to Determine Available Bandwidth for Multiple Bootloaders for more information.

### Related Topics

- Ways to Configure Multiple Bootloader Carousels
- Set Up Multiple Bootloader Carousels
- Determine Available Bandwidth for Multiple Bootloaders
- Multiple Bootloader Settings
- Add a Bootloader Source to the DNCS
- Set Up DHCTs to Download Images from a Specific Bootloader Carousel

## Ways to Configure Multiple Bootloader Carousels

Here are a few examples of how you might configure your bootloader carousels:

- Put CableCARD module images on a separate carousel from DHCT images. Because CableCARD module images are smaller, the carousel cycle time is lessened. As a result, the CableCARD modules receive their images quicker.
- Put larger images on one carousel and smaller images on the other carousel. The carousel that carries only the smaller images allows the receiving device (DHCT or CableCARD module) to get the smaller image in less time because it is not impacted by being interleaved with the larger content.
- If you need to send an image out to a device population quickly, you might create one carousel to carry this image.

**Note:** Faster downloads can sometimes be realized by increasing the data rate for the existing 199 bootloader carousel. Keep in mind that this strategy works only when using DHCTs (set-tops) that support download data rates greater than 10 Mbps.

### Related Topics

- Set Up Multiple Bootloader Carousels
- Determine Available Bandwidth for Multiple Bootloaders
- Multiple Bootloader Settings
- Add a Bootloader Source to the DNCS
- Set Up DHCTs to Download Images from a Specific Bootloader Carousel

## Set Up Multiple Bootloader Carousels

This section provides an overview of the steps required to set up more than one bootloader carousel and configure set-tops to use the correct carousel when downloading images.

1. Verify that the BFS QAM has enough bandwidth to support a second bootloader carousel. To make this determination, go to Determine Available Bandwidth for Multiple Bootloaders.

2. Add the new bootloader carousel to the DNCS by adding a bootloader source with the following characteristics to the BFS Administration window.

**Note:** For assistance adding a bootloader source to the BFS Administration window, go to Add a Bootloader Source to the DNCS.

- **Source Name** - Enter a name to describe this source; for example, **Bootloader2**.
- **Source ID** - Ideally, we recommend that you select an even number that is not in use and that is greater than 200 to correspond with our numbering convention.
- **Source Type** - Select **Bootloader**.
- **Transport Type** - Select **ASI In-band**.
- **Data Rate** - The rate depends on several factors, including the DHCT type, the BFS QAM setting, and the available bandwidth. When you make this decision, select a rate between 1.00 and 3.00 Mbps. For assistance, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377).

  **Important:** When you stage SCC DHCTs, use a data rate of 3.00 Mbps.

- **Block size** - Enter **4000**.
- **Indication Interval** - Enter **100**.
- **DataPump** - Set to **run**.

  **Note:** If your system uses the RCS feature, skip this field.

- **Selected Hosts** - Select the same hosts as the main Bootloader source.

3. Configure set-tops to use the correct bootloader carousel when downloading images. For assistance, go to Set Up DHCTs to Download Images from a Specific Bootloader Carousel.

**Important:** When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source.

### Related Topics

- Determine Available Bandwidth for Multiple Bootloaders
- Multiple Bootloader Settings
- Add a Bootloader Source to the DNCS
- Set Up DHCTs to Download Images from a Specific Bootloader Carousel
- Ways to Configure Multiple Bootloader Carousels

## Determine Available Bandwidth for Multiple Bootloaders

This section provides inband data carousel recommendations and procedures for determining how much bandwidth is currently available on the BFS QAM for bootloader sources.

### Why Determine Available Bandwidth?

Determining the amount of unused (or available) bandwidth for inband sources ensures that your system has sufficient bandwidth for additional bootloader carousels. Bootloader carousels require a data rate between 1.00 and 3.00 Mbps.

**Example:** If your BFS QAM has 4 Mbps of available bandwidth and you want to add two bootloader carousels, each with a data rate of 3 Mbps, you cannot; there is only enough available bandwidth to support one of the carousels.

**Note:** For assistance selecting a suitable rate for additional bootloader carousels, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377).

### How Much Bandwidth Can My System Support?

Depending on your QAM modulation mode, the sum of your inband carousel rates plus any audio-visual content that is combined on the BFS QAM modulator should not exceed the following totals:

| Modulation Type | Direct ASI Bandwidth | BFS BIG Bandwidth |
|---|---|---|
| 64-QAM modulation | 26 Mbps | 25 Mbps |
| 256-QAM modulation | 37 Mbps | 36 Mbps |

### Related Topics

- Determine Available Bandwidth for Your System (Determine Available Bandwidth for Your System, Determining Available Bandwidth for Direct ASI Systems)

### Why Determine Available Bandwidth?

Determining the amount of unused (or available) bandwidth for inband sources ensures that your system has sufficient bandwidth for additional bootloader carousels. Bootloader carousels require a data rate between 1.00 and 3.00 Mbps.

**Example:** If your BFS QAM has 4 Mbps of available bandwidth and you want to add two bootloader carousels, each with a data rate of 3 Mbps, you cannot; there is only enough available bandwidth to support one of the carousels.

**Note:** For assistance selecting a suitable rate for additional bootloader carousels, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377).

### How Much Bandwidth Can My System Support?

Depending on your QAM modulation mode, the sum of your inband carousel rates plus any audio-visual content that is combined on the BFS QAM modulator should not exceed the following totals:

| Modulation Type | Direct ASI Bandwidth | BFS BIG Bandwidth |
|---|---|---|
| 64-QAM modulation | 26 Mbps | 25 Mbps |
| 256-QAM modulation | 37 Mbps | 36 Mbps |

### Determine Available Bandwidth for Your System

To determine the available bandwidth for your system, go to one of the following topics:

- If your system uses ASI, go to Determining Available Bandwidth for Direct ASI Systems.
- If your system uses a BFS BIG, go to Determining Available Bandwidth for BFS BIG Systems.

### Determining Available Bandwidth for Direct ASI Systems

This section provides procedures for operators with direct ASI to use in determining how much bandwidth is available for inband sources. To determine the amount of bandwidth available for additional bootloader carousels, perform the following calculation:

Total Available Bandwidth - Bandwidth in Use = Available Bandwidth

**Notes:**

- The inband data rate for a 64-QAM is 26 Mbps.
- The inband data rate for a 256-QAM is 37 Mbps.

These rates are due to modulation coding and error corrections (real rates are higher).

1. Open an xterm window on the DNCS.
2. Type one of the following, based on the system release you have installed:
   - For SR 4.2.1 and earlier, type **cd /export/home/dncs/doctor** and press **Enter**.
   - For SR 4.3 and later, type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.

   **Note:** Be sure to type a space between **cd** and **/**.

   **Result:** The current directory is now the doctor directory.
3. Type **doctor -bv** and press **Enter**. A table appears that lists the inband and out-of-band data rates on the BFS carousel. The total inband carousel bandwidth in use is displayed in the **Aggregate IB Carousel Datarate** field.
4. Subtract the total inband carousel bandwidth in use from the total available bandwidth to determine the unused inband bandwidth on the BFS.

   **Examples:**

   - **64-QAM:** If your total inband carousel bandwidth in use is 14 Mbps, the available bandwidth is 12 Mbps.

     26 - 14 = 12 Mbps

   - **256-QAM:** If your total inband carousel bandwidth in use is 14 Mbps, the available bandwidth is 23 Mbps.

     37 - 14 = 23 Mbps
5. Compare the amount of unused bandwidth to the amount of bandwidth required for the additional bootloader carousels.
6. Is there enough bandwidth to add the new bootloader carousels? (Bootloader carousels require data rates between 1.00 and 3.00 Mbps.)
   - If **yes**, go to Add a Bootloader Source to the DNCS.
   - If **no**, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377) for details on how to increase the bandwidth of your system.

### Determining Available Bandwidth for BFS BIG Systems

This section provides procedures for operators with a BFS BIG to use in determining how much bandwidth is available for inband sources. To determine the amount of bandwidth available for additional bootloader carousels, perform the following calculation:

Total Available Bandwidth - Bandwidth in Use = Available Bandwidth

**Notes:**

- The inband data rate for a 64-QAM is 25 Mbps.
- The inband data rate for a 256-QAM is 36 Mbps.

1. Open an xterm window on the DNCS.
2. Type one of the following, based on the system release you have installed:
   - For SR 4.2.1 and earlier, type **cd /export/home/dncs/doctor** and press **Enter**.
   - For SR 4.3 and later, type **cd /dvs/dncs/Utilities/doctor** and press **Enter**.

   **Note:** Be sure to type a space between **cd** and **/**.

   **Result:** The current directory is now the doctor directory.
3. Type **doctor -bv** and press **Enter**. A table appears and lists the inband and out-of-band data rates on the BFS carousel. The total inband carousel bandwidth in use is displayed in the **Aggregate IB Carousel Datarate** field.
4. Add **1 Mbps** to the data rate in the **Aggregate IB Carousel Datarate** field to account for any overhead.

   **Example:** If you have a total inband data rate of 14 Mbps, add 1 Mbps for a total of 15 Mbps in use.

   14 + 1 = 15
5. Subtract the total inband carousel bandwidth in use from the total available bandwidth to determine the unused inband bandwidth on the BFS.

   **Examples:**

   - **64-QAM:** From the examples above, the available bandwidth is 10 Mbps.

     25 - 15 = 10 Mbps
   - **256-QAM:** From the examples above, the available bandwidth is 21 Mbps.

     36 - 15 = 21 Mbps
6. Compare the amount of unused bandwidth to the amount of bandwidth required for the additional bootloader carousels.
7. Is there enough bandwidth to add the new bootloader carousels? (Bootloader carousels require data rates between 1.00 and 3.00 Mbps.)
   - If **yes**, go to Verify a VCI for Inband BFS Sources on BFS BIG Systems.
   - If **no**, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377) for details on how to increase the bandwidth of your system.

### Verify a VCI for Inband BFS Sources on BFS BIG Systems

This section describes how to check the number of BFS sessions on your system to determine whether any unused VCIs are present for the inband BFS carousel.

**Notes:**

- Your network was initially installed and reserved with 20 Virtual Channel Indicator (VCI) connections (values 256-275) on the ATM switch. The VCIs carry inband BFS information from the DNCS to the BIG. Because you will create a new inband source, you must make sure that one VCI is available for each additional bootloader carousel that you add to the DNCS.
- If you need detailed instructions for this procedure, refer to the manual that came with your ATM switch.

Complete the following steps to determine whether there are enough unused VCIs available for the additional inband BFS carousels.

1. Using the manual that came with your ATM switch, check the ATM switch to determine the number of unused VCIs.
2. Are there enough VCIs for the new bootloader carousels?
   - If **yes**, go to Add a Bootloader Source to the DNCS.
   - If **no**, add more VCIs to the switch. Then, go to Add a Bootloader Source to the DNCS.

   **Note:** Having unused VCIs does not present any issues to your system; therefore, we recommend that you create 5 to 10 extra VCIs.

## Multiple Bootloader Settings

There are two specific areas of settings required to use multiple bootloaders in the DNCS:

- Bootloader Source Settings - For setting up and managing bootloader sources
- Specific Carousel Settings for DHCTs - For setting up set-tops to download images from a specific bootloader carousel

### Bootloader Source Settings

Use the following fields when you manage a bootloader source in the DNCS.

| Field | Description |
|---|---|
| Source Name | Enter a name to describe this source.<br>**Example:** Enter **Bootloader2**. |
| Source ID | We recommend that you select an even number that is not in use and that is greater than 200 to correspond with our naming convention. |
| Source Type | Select **Bootloader**. |
| Transport Type | Select the **In-band** option. |
| Data Rate | The data rate depends on several factors, including the DHCT type, the BFS QAM setting, and the available bandwidth. When you make this decision, select a rate between 1.00 and 3.00 Mbps.<br>For more information on carousel data rates, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377). |
| Block Size | Type **4000**. |
| Indication Interval | Type **100**. |
| Source | Select the **enable** option.<br>**Note:** If your system uses the RCS feature, skip this field. |
| Hosts | Select the same hosts that the main Bootloader source uses in the **Available Hosts** column and click the arrow to move those sources to the **Selected Hosts** column. |

### Related Topics

- Add a Bootloader Source to the DNCS
- Ways to Configure Multiple Bootloader Carousels

### Specific Carousel Settings for DHCTs

Use the following fields when you configure DHCTs to download images from a specific bootloader carousel.

| Field | Description |
|---|---|
| DHCT Type | The device that receives the new image. |
| Group | The file that corresponds to the new application platform release that you want to download. |
| Field Description | The group of devices to which you want to download the image. |
| Downloading Schedule | The download method you want to use. The following download methods are supported:<br>▪**Normal** - Causes the set-top to download the image after the set-top is powered on for two minutes.<br>▪**Immediate** - Causes the set-top to download the image in a relatively short amount of time.<br>**Important:** This method interrupts watching TV, PPV, VOD, and other services.<br>▪**Emergency** - Causes the set-top to download the image immediately, without displaying a barker for the subscriber. |
| Carousel | The bootloader carousel that the download device uses to download the image.<br>**Important:** When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source. |

### Related Topics

- Set Up DHCTs to Download Images from a Specific Bootloader Carousel
- Ways to Configure Multiple Bootloader Carousels

## Add a Bootloader Source to the DNCS

This section provides instructions for adding a bootloader source to the DNCS. The DNCS uses a default bootloader source (source ID 199); however, you can add bootloader sources to the DNCS. With multiple bootloader carousels, the BFS can send set-top software version images using more than one carousel. This enhancement gives operators the flexibility needed to reduce download times and maintain system performance by creating the optimal number of bootloader carousels for their system.

**Important:** If you are using our RCS solution, select **All Sites** to add this source to all existing sites as well as all future sites.

Before you begin, determine the data rate for each bootloader carousel. The rate is dependent on several factors, such as the BFS QAM setting and the available bandwidth. When making this decision, select a rate between 1.00 and 3.00 Mbps. For assistance, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377).

You also need to assign the new bootloader to the same hosts as the original bootloader. Refer to the configuration of the original bootloader and record which hosts it uses.

### Adding a Bootloader Source to the DNCS

1. On the DNCS Administrative Console, click the Application Interface Modules tab.
2. Click **BFS Admin**. Depending on your system configuration, the following window opens:
   - If you are using a typical network with no RCS, the BFS Administration window opens. If this window opens, go to step 4.
   - If you are using an RCS, the Please select a site window opens. If this window opens, go to step 3.
3. Select **File > All Sites**.
4. Click the **Sources** tab.
5. Click **File > New**. The Set Up BFS Source window opens.
6. Complete the fields on the screen as described in Bootloader Source Settings.

Use the following fields when you manage a bootloader source in the DNCS.

| Field | Description |
|---|---|
| Source Name | Enter a name to describe this source.<br>**Example:** Enter **Bootloader2**. |
| Source ID | We recommend that you select an even number that is not in use and that is greater than 200 to correspond with our naming convention. |
| Source Type | Select **Bootloader**. |
| Transport Type | Select the **In-band** option. |
| Data Rate | The data rate depends on several factors, including the DHCT type, the BFS QAM setting, and the available bandwidth. When you make this decision, select a rate between 1.00 and 3.00 Mbps.<br>For more information on carousel data rates, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377). |

| | |
|---|---|
| Block Size | Type **4000**. |
| Indication Interval | Type **100**. |
| Source | Select the **enable** option.<br>**Note:** If your system uses the RCS feature, skip this field. |
| Hosts | Select the same hosts that the main Bootloader source uses in the **Available Hosts** column and click the arrow to move those sources to the **Selected Hosts** column. |

7. Click **Save**. The system saves the carousel in the DNCS database and closes the Set Up BFS Source window.

8. Click the **Servers** tab and double-click the bootloader server. The Authorize BFS Server window opens for the bootloader server.

9. In the **Available Hosts** field, select the bootloader source that you just created and then click **Add**. The host you selected moves to the Selected Hosts list.

**Important:** Move only the server that you just created to the Selected Hosts list.

10. Click **Save**. The system saves this change and closes the Authorize BFS Server window.

11. Do you need to add another bootloader source this BFS?

- If **yes**, repeat this procedure from step 5.
- If **no**, you are ready to configure set-tops to use the correct bootloader carousel when downloading images. Go to Set Up DHCTs to Download Images from a Specific Bootloader Carousel.

## Add a Bootloader Source to the DNCS

This section provides instructions for adding a bootloader source to the DNCS. The DNCS uses a default bootloader source (source ID 199); however, you can add bootloader sources to the DNCS. With multiple bootloader carousels, the BFS can send set-top software version images using more than one carousel. This enhancement gives operators the flexibility needed to reduce download times and maintain system performance by creating the optimal number of bootloader carousels for their system.

**Important:** If you are using our RCS solution, select **All Sites** to add this source to all existing sites as well as all future sites.

Before you begin, determine the data rate for each bootloader carousel. The rate is dependent on several factors, such as the BFS QAM setting and the available bandwidth. When making this decision, select a rate between 1.00 and 3.00 Mbps. For assistance, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377).

You also need to assign the new bootloader to the same hosts as the original bootloader. Refer to the configuration of the original bootloader and record which hosts it uses.

### Adding a Bootloader Source to the DNCS

1. On the DNCS Administrative Console, click the Application Interface Modules tab.
2. Click **BFS Admin**. Depending on your system configuration, the following window opens:
   - If you are using a typical network with no RCS, the BFS Administration window opens. If this window opens, go to step 4.
   - If you are using an RCS, the Please select a site window opens. If this window opens, go to step 3.
3. Select **File > All Sites**.
4. Click the **Sources** tab.
5. Click **File > New**. The Set Up BFS Source window opens.
6. Complete the fields on the screen as described in Bootloader Source Settings.

Use the following fields when you manage a bootloader source in the DNCS.

| Field | Description |
|---|---|
| Source Name | Enter a name to describe this source.<br>**Example:** Enter **Bootloader2**. |
| Source ID | We recommend that you select an even number that is not in use and that is greater than 200 to correspond with our naming convention. |
| Source Type | Select **Bootloader**. |
| Transport Type | Select the **In-band** option. |
| Data Rate | The data rate depends on several factors, including the DHCT type, the BFS QAM setting, and the available bandwidth. When you make this decision, select a rate between 1.00 and 3.00 Mbps.<br>For more information on carousel data rates, refer to Recommendations for Data Carousel Rate Management Technical Bulletin (part number 716377). |

| | |
|---|---|
| Block Size | Type **4000**. |
| Indication Interval | Type **100**. |
| Source | Select the **enable** option.<br>**Note:** If your system uses the RCS feature, skip this field. |
| Hosts | Select the same hosts that the main Bootloader source uses in the **Available Hosts** column and click the arrow to move those sources to the **Selected Hosts** column. |

7. Click **Save**. The system saves the carousel in the DNCS database and closes the Set Up BFS Source window.

8. Click the **Servers** tab and double-click the bootloader server. The Authorize BFS Server window opens for the bootloader server.

9. In the **Available Hosts** field, select the bootloader source that you just created and then click **Add**. The host you selected moves to the Selected Hosts list.

**Important:** Move only the server that you just created to the Selected Hosts list.

10. Click **Save**. The system saves this change and closes the Authorize BFS Server window.

11. Do you need to add another bootloader source this BFS?

- If **yes**, repeat this procedure from step 5.
- If **no**, you are ready to configure set-tops to use the correct bootloader carousel when downloading images. Go to Set Up DHCTs to Download Images from a Specific Bootloader Carousel.

## Set Up DHCTs to Download Images from a Specific Bootloader Carousel

After you have added a bootloader source to the DNCS, set up DHCTs to download images from a specific bootloader carousel.

**Important:** When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source.

### Setting Up DHCTs to Download Images from a Specific Bootloader Carousel

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **DHCT Downloads** tab.
5. Click **File > New**. The Set Up DHCT Download window opens.
6. Complete the fields on the screen as described in Specific Carousel Settings for DHCTs.

Use the following fields when you configure devices (DHCTs and CableCARD modules) to download images from a specific bootloader carousel.

| Field | Description |
|---|---|
| Device Type | The device that receives the new image. |
| Group | The file that corresponds to the new application platform release that you want to download. |
| Field Description | The group of devices to which you want to download the image. |
| Downloading Schedule | The download method you want to use. The following download methods are supported:<br>▪ **Normal** - Causes the set-top to download the image after the set-top is powered on for two minutes.<br>▪ **Immediate** - Causes the set-top to download the image in a relatively short amount of time.<br>**Important:** This method interrupts watching TV, PPV, VOD, and other services.<br>▪ **Emergency** - Causes the set-top to download the image immediately, without displaying a barker for the subscriber. |
| Carousel | The bootloader carousel that the download device uses to download the image.<br>**Important:** When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error |

| | |
|---|---|
| | message when saving the image to the second bootloader source. |

7. Click **Save.** The Association Verification window opens.

8. Verify that the information shown is correct, and configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?** - Type **yes**.
- **Enter your name** - Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password** - Type the password you received from Cisco Services.

9. Click **OK**. The association Verification window closes and the Image List window is updated with the newly defined test download schedule. The emergency download begins instantaneously and no barker opens to the subscriber.

## Set Up DHCTs to Download Images from a Specific Bootloader Carousel

After you have added a bootloader source to the DNCS, set up DHCTs to download images from a specific bootloader carousel.

**Important:** When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error message when saving the image to the second bootloader source.

### Setting Up DHCTs to Download Images from a Specific Bootloader Carousel

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **DHCT Downloads** tab.
5. Click **File > New**. The Set Up DHCT Download window opens.
6. Complete the fields on the screen as described in Specific Carousel Settings for DHCTs.

Use the following fields when you configure devices (DHCTs and CableCARD modules) to download images from a specific bootloader carousel.

| Field | Description |
|---|---|
| Device Type | The device that receives the new image. |
| Group | The file that corresponds to the new application platform release that you want to download. |
| Field Description | The group of devices to which you want to download the image. |
| Downloading Schedule | The download method you want to use. The following download methods are supported:<br>▪ **Normal** - Causes the set-top to download the image after the set-top is powered on for two minutes.<br>▪ **Immediate** - Causes the set-top to download the image in a relatively short amount of time.<br>**Important:** This method interrupts watching TV, PPV, VOD, and other services.<br>▪ **Emergency** - Causes the set-top to download the image immediately, without displaying a barker for the subscriber. |
| Carousel | The bootloader carousel that the download device uses to download the image.<br>**Important:** When you set up multiple bootloader carousels, send each DHCT image using only one bootloader source. Attempting to send the same DHCT image to two different bootloader sources at the same time will cause the system to display a **Save Failed** error |

| | |
|---|---|
| | message when saving the image to the second bootloader source. |

7. Click **Save.** The Association Verification window opens.

8. Verify that the information shown is correct, and configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?** - Type **yes**.
- **Enter your name** - Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password** - Type the password you received from Cisco Services.

9. Click **OK**. The association Verification window closes and the Image List window is updated with the newly defined test download schedule. The emergency download begins instantaneously and no barker opens to the subscriber.

# OpenCable Compliance

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > DNCS System > Miscellaneous tab > OpenCable Compliant > Save**

If your system is designed to comply with OpenCable standards, you must set up certain additional parameters in the DNCS. However, you can do this **only after** you have set up all of your other network elements in the DNCS.

Our PowerKEY CableCARD Module is a point-of-deployment (POD) module that enables cable operators to fulfill the industry commitment to OpenCable. OpenCable is an initiative that is managed by CableLabs. The goal of OpenCable is to define a generation of DHCTs that can operate in various cable systems throughout North America, regardless of the DHCT manufacturer.

The procedures in this topic tell you how to configure the DNCS so that it recognizes these CableCARD modules as they are deployed in your network. For further information, refer to OpenCable™ CableCARD™ Interface Specification, OC-SP-CC-IF-I14-030905. To obtain a copy of this document, see Printed Resources.

## What do you want to do?

- Set up OpenCable compliance
- Define your system as OpenCable compliant
- Reboot the SI manager process

## Set Up OpenCable Compliance

The procedures in this topic tell you how to configure the DNCS so that it recognizes these CableCARD modules as they are deployed in your network. For further information, refer to OpenCable™ CableCARD™ Interface Specification, OC-SP-CC-IF-I14-030905. To obtain a copy of this document, see Printed Resources.

### Process Overview

After you have set up all of your other network elements in the DNCS, you can set up your system to comply with OpenCable standards by completing the following tasks. For step-by-step instructions for a particular task, click on that task.

1. Define the system as OpenCable compliant.
2. Reboot the SI Manager process on the DNCS workstation.

## Set Up OpenCable Compliance

The procedures in this topic tell you how to configure the DNCS so that it recognizes these CableCARD modules as they are deployed in your network. For further information, refer to OpenCable™ CableCARD™ Interface Specification, OC-SP-CC-IF-I14-030905. To obtain a copy of this document, see Printed Resources.

### Process Overview

After you have set up all of your other network elements in the DNCS, you can set up your system to comply with OpenCable standards by completing the following tasks. For step-by-step instructions for a particular task, click on that task.

1. Define the system as OpenCable compliant.
2. Reboot the SI Manager process on the DNCS workstation.

### Define Your System as OpenCable Compliant

The first step in setting up your network for OpenCable compliance is to define the system as such in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **DNCS System**. The DNCS System Configuration window opens with the DSM-CC tab in the forefront.
4. Click the **Miscellaneous** tab. The Miscellaneous window opens.
5. Click the **Open Cable Compliant** option.
6. Click **Save**. The system saves this setting in the DNCS database and the Open Cable Compliance Warning window opens.
7. Click **OK**. The warning window closes.
8. Click **Close**. The DNCS System Configuration window closes and returns you to the DNCS Administrative Console.
9. Your next step is to reboot the SI Manager process on the DNCS workstation. Go to Rebooting the SI Manager Process.

### Reboot the SI Manager Process

1. From the DNCS section of the DNCS Administrative Console Status window, click **Control**. The DNCS Control window opens.
2. From the list of processes, select **siManager**.
3. Click **Process** and select **Stop Process**. A confirmation window opens.
4. Click **Yes** to confirm that you want to stop the siManager process. The indicator next to siManager turns red to identify that the process is stopped.
5. With the siManager process selected, click **Process** and select **Start Process**. The indicator next to siManager turns green to identify that the process has started.

# Overlay

If your system uses our Overlay option, you have the ability to deploy certain models of Explorer DHCTs in an existing system (not manufactured by us).

Support for Overlay technology requires that you install and enable one of the following:

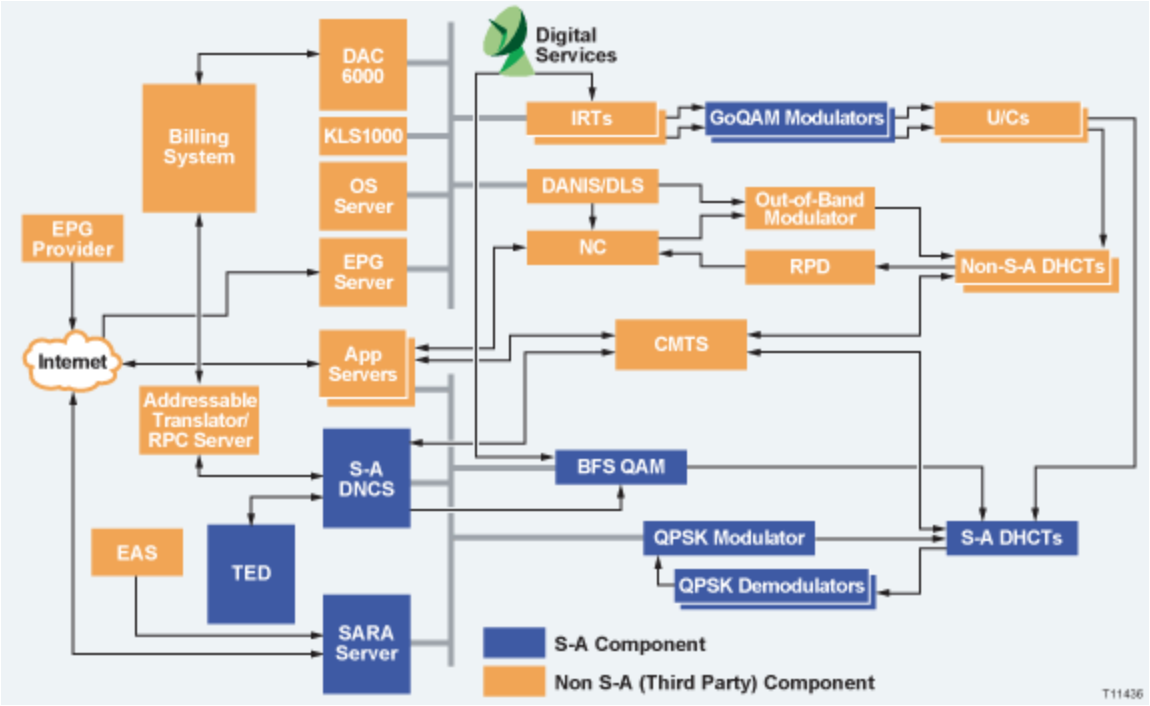
- Install SR 2.6 (or later) and enable the software license.
- Install SR 3.6 (or later) and enable the software license.

## What do you want to do?

- Examine a simplified network view of Overlay technology
- View a list of Explorer DHCTs that can be deployed in a system using Overlay technology
- Learn how content is processed in a system using Overlay technology
- Review a list of tasks required to prepare the DNCS to support Overlay technology

## Simplified Network View of Overlay Technology

The following diagram gives an example of a DBDS network that uses Overlay technology. In this diagram, our components are shown in blue.




### Related Topics

- DHCTs in an Overlay Environment
- Content in an Overlay Environment
- Configure the DNCS for Overlay Technology

## DHCTs in an Overlay Environment

With the Overlay option enabled on the DNCS, DHCTs from us and other manufacturers can be used in a network other than ours; independent of headend, hub, or node location.

The Overlay option currently supports the following Explorer DHCTs:

- **Explorer 3250 DHCT** - Supports video-on-demand (VOD), subscription VOD (SVOD), e-mail, chat services, Internet access, and other applications, such as games.
- **Explorer 3250HD DHCT** - Provides all the features of the Explorer 3250 DHCT, plus support for all 18 ATSC digital video formats, including the 6 high-definition digital formats for HDTV.
- **Explorer 8000 DHCT** - Includes a dual tuner and digital video recorder (DVR) with picture-in-picture (PIP) control, giving subscribers control, convenience, and choice in their TV viewing experience.
- **Explorer 8000HD DHCT** - Provides all the features of the Explorer 8000 DHCT, plus support for HD content.

**Important:** Pace, Panasonic, and Aptiv Digital set-tops are not currently supported by Overlay technology.

### Related Topics

- Content in an Overlay Environment
- Configure the DNCS for Overlay Technology
- Simplified Network View of Overlay Technology

## Content in an Overlay Environment

To allow your system to support encryption methods used by our equipment and by equipment from other manufacturers, Overlay technology uses partially encrypted broadcast sessions.

### Partially Encrypted Broadcast Sessions

Only partially encrypted broadcast sessions can be used to feed both our DHCTs and DHCTs from other manufacturers. Overlay technology uses GoQAM modulators to create partially encrypted sessions. These sessions consist mostly of unencrypted MPEG packets and a percentage of identical packets encrypted by us and by third-party systems. This encryption technique allows both types of DHCTs to function in the same network.

For assistance in setting up a partially encrypted broadcast session on a GoQAM modulator, see Add a Partially Encrypted Session.

### Related Topics

- Configure the DNCS for Overlay Technology
- Simplified Network View of Overlay Technology
- DHCTs in an Overlay Environment

## Configure the DNCS for Overlay Technology

These instructions summarize the steps required to configure your DNCS to support Overlay technology. Each step of these instructions provides a link to a more detailed procedure.

When using these procedures, keep in mind that because this technology "overlays" our system on top of your current system, you'll find that many of these procedures are used by operators of a typical system of ours. Others procedures, however, are required only by operators who manage a system that uses Overlay technology.

After enabling the Overlay option, follow these steps to configure your system for Overlay technology.

**Note:** All of these tasks are performed from the DNCS.

1. Add elements that process data to the DNCS.
2. Add elements that process content to the DNCS:
   - If you are using RF GoQAM modulators to process partially encrypted content streams, add content RF GoQAM modulators to the DNCS.
   - If you are using IF GoQAM modulators to process partially encrypted content streams, add content IF GoQAM modulators to the DNCS.
3. For each content IF GoQAM modulator in your system, add an UpConverter to the DNCS and link (connect) it to the IF GoQAM modulator that feeds the UpConverter.
4. Add sources to the DNCS Source List.
5. Set up partially encrypted sessions on GoQAM modulators to support broadcast services.

   **Note:** You set up partially encrypted sessions when defining a digital source as part of setting up a secure or PPV service.

6. If your system supports VOD services, add table-based third-party QAM modulators to the DNCS so that they are available for VOD service groups to use when creating VOD sessions

   **Important:** Make certain that when adding these modulators to the DNCS that you do not use our TSIDs for these modulators.

7. Set up VOD service groups.

   **Important:** VOD service groups can contain QAM modulators from most any manufacturer. However, they cannot contain our GoQAM modulators. GoQAM modulators are used only for broadcast services, not VOD services.

## RF GoQAM Modulators

Systems using the Overlay option require an RF GoQAM modulator or an IF GoQAM modulator. These modulators are required because they produce partially encrypted broadcast sessions, which feed DHCTs manufactured by us and by other vendors.

**Note:** Depending upon system architecture, GoQAM modulators can be used in headends or hubs.

- **RF GoQAM Modulators** are used only in a DBDS that uses Overlay technology. An RF GoQAM modulator receives both clear and encrypted content data in an MPEG format from two pairs of ASI inputs. Each pair consists of an encrypted stream and its corresponding clear stream. The RF GoQAM receives RF GoQAMs filter, modify, synchronize, and combine the two data streams into a single transport stream and send this stream to hubs. Once processed by the RF GoQAM, the transport stream can be used by DHCTs from third-party vendors, without regard to the type of encryption method that each DHCT uses. From the QAM List, you can add, modify, or delete an RF GoQAM modulator.
- **IF GoQAM Modulators** are used only in a DBDS that uses Overlay technology. An IF GoQAM modulator receives both a clear and an encrypted data stream. IF GoQAM modulators filter, modify, synchronize, and combine the two data steams into a single transport stream using an IF (intermediate frequency) of 44MHz. Once processed by the IF GoQAM, the transport stream can be fed to DHCTs from different manufacturers, without regard to the type of encryption method that the DHCTs use. Because the modulator uses an IF frequency, it supports applications that require operation below 55 MHz or above 860 MHz. From the QAM List, you can add, modify, or delete an IF GoQAM modulator.

**Related Topics**

- RF GoQAM Settings
- Add a Content RF GoQAM Modulator
- Modifying a QAM, MQAM, GQAM, or GoQAM Modulator
- Resetting a QAM, MQAM, GQAM, or GoQAM Modulator
- Deleting a QAM, MQAM, GQAM, or GoQAM Modulator
- Locate the MAC Address of a QAM

### RF GoQAM Settings

Use the Set Up GoQAM Modulator page on the DNCS Administrative Console to manage the RF GoQAM devices in your network. Two tabs in this window provide settings for the RF GoQAM:

- Basic Parameter settings: Use the settings on the Basic Parameters tab to configure the RF GoQAM.
- Connectivity settings: Use the settings on the Connectivity tab to configure the connections between the modulator and its associated MPEG source

**Note:** Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### RF GoQAM Basic Parameter Settings

Use the following fields when you manage an RF GoQAM in the DNCS.

| Field | Description | |
|---|---|---|
| Headend Name | The headend associated with this modulator. | |
| QAM Name | The name of this modulator.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1RFGoQ43 could represent an RF GoQAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. | |
| IP Address | The IP address of this modulator.<br>Be careful to properly place the dots (.) between numbers. | |
| Modulation Type | The type of modulation standard that the modulator uses.<br>**Example:** If this modulator uses the International Telecommunications Union standard ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6MHz)**. | |
| MAC Address | The MAC address for the modulator. | |
| Subnet Mask | The subnet mask where this modulator resides. | |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a modulator is rebooted. | |
| Input Block 1 ASI 1 Clear Transport Stream ID | The number identifying the transport stream for this input block.<br>(Complete for each input port on the GoQAM modulator) | |
| Input Block 2 ASI 2 Clear Transport Stream ID | A block accepts both a clear and an encrypted version of the same MPEG transport stream. | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters.<br>Specify a unique transport stream ID for each output port on the RF GoQAM modulator. |

| | |
|---|---|
| | **Note:** Make certain that you enter a TSID that is within the range reserved for our QAM modulators. This range is listed in the Ports area of the Basic Parameters tab for easy reference. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs<br>on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the modulator's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event when a<br>port fails. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>▪If this RF GoQAM modulator is sending data 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 that will receive data from this modulator.<br>▪If this RF GoQAM modulator is sending data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field.<br>**Note:** To remove a hub from the **Selected Hubs** field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field. |

**Related Topics**

- RF GoQAM Modulator Connection Settings
- Recommended Modulator Frequencies
- Add a Content RF GoQAM Modulator
- Modifying a QAM, MQAM, GQAM, or GoQAM Modulator
- Locate the MAC Address of a QAM

### RF GoQAM Modulator Connection Settings

Use the following fields when you manage connections for an RF GoQAM.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | The type of MPEG source device being used to send data to this modulator (for example, IRT, MDR and Service Group Object). |
| Device Name | The name of the source device. |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

### Related Topics

- Recommended Modulator Frequencies
- Add a Content RF GoQAM Modulator
- Modifying a QAM, MQAM, GQAM, or GoQAM Modulator
- Locate the MAC Address of a QAM

### Recommended Modulator Frequencies

Use the center frequencies shown in the following table to send data from your QAM modulators to the DHCTs on your system. Notice that these frequencies are separated by increments of 6 MHz.

**Note:** If you are experiencing signal interference, try offsetting your modulator frequencies by 250 kHz from the frequencies shown in the table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 153 | 159 | 165 | 171 | 177 | 183 | 189 | 195 | 201 | 207 |
| 213 | 219 | 225 | 231 | 237 | 243 | 249 | 255 | 261 | 267 |
| 273 | 279 | 285 | 291 | 297 | 303 | 309 | 315 | 321 | 327 |
| 333 | 339 | 345 | 351 | 357 | 363 | 369 | 375 | 381 | 387 |
| 393 | 399 | 405 | 411 | 417 | 423 | 429 | 435 | 441 | 447 |
| 453 | 459 | 465 | 471 | 477 | 483 | 489 | 495 | 501 | 507 |
| 513 | 519 | 525 | 531 | 537 | 543 | 549 | 555 | 561 | 567 |
| 573 | 579 | 585 | 591 | 597 | 603 | 609 | 615 | 621 | 627 |
| 633 | 639 | 645 | 651 | 657 | 663 | 669 | 675 | 681 | 687 |
| 693 | 699 | 705 | 711 | 717 | 723 | 729 | 735 | 741 | 747 |

### Add a Content RF GoQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > GOQAM >RF GOQAM**

If you are using an RF GoQAM modulator to send content to DHCTs and you have already added an MPEG source to the DNCS database, you are ready to add the RF GoQAM modulator to the DNCS database.

RF GoQAMs are a critical component of our Overlay solution. Overlay technology allows cable service providers to support DHCTs manufactured by us and by other vendors. RF GoQAM modulators can receive both clear and encrypted program and service data, such as, audio/video programming and Web services. They filter, modify, synchronize, and combine the two data streams into a single transport stream and send this stream to hubs. Once processed by the RF GoQAM, the transport stream can be used by DHCTs from different manufacturers, without regard to the type of encryption method that each DHCT uses.

**Important:** If you do not use Overlay technology, do not add an RF GoQAM modulator to your DBDS. Adding an RF GoQAM modulator in a system that does not use Overlay technology can cause your system to behave unpredictably.

#### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- Name of the headend containing the RF GoQAM modulator
- Name used to identify the RF GoQAM modulator
- IP address for the RF GoQAM modulator (from your system administrator)
- Type of modulation standard the RF GoQAM modulator uses, such as ITU J.83 Annex B
- MAC address for the RF GoQAM modulator
- Subnet mask for the RF GoQAM modulator (from your system administrator)
- If applicable, the default gateway that the RF GoQAM modulator uses
- Numbers identifying the input pairs that physically connect the modulator to the associated MPEG sources.
- The type of QAM used, such as 256 QAM or 64 QAM.
- Numbers identifying the transport streams going from the RF GoQAM modulator out to the hubs on your system
- Frequencies of the channels being used to send data from the RF GoQAM modulator to the hubs on your system
- Names of the hubs you want to receive data from this RF GoQAM modulator
- Name of the headend containing the MPEG sources that send content data to this RF GoQAM modulator
- Type of MPEG source devices being used to send data to this RF GoQAM modulator (for example, IRT, MDR, VOD server, and so forth)
- Names of the associated MPEG sources
- Numbers identifying the output ports of the associated MPEG sources that are physically connected to the input ports on this RF GoQAM modulator

**Notes:**

- All of this information should be recorded on your network map. However, if it is not, contact your

system administrator to obtain the information.

- For assistance installing the RF GoQAM, see GoQAM Modulator RF Output and IF Output Hardware Installation and Operation Guide (part number 4004834).

**Related Topics**

- Add a Content RF GoQAM Modulator
- Setting Up Basic Parameters for an RF GoQAM Modulator
- Setting Up Connections for an RF GoQAM Modulator
- Activating an RF GoQAM Modulator

### Setting Up Basic Parameters for an RF GoQAM Modulator

The first step in adding an RF GoQAM modulator is to set up the basic parameters for the modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > QAM > GOQAM > RF GOQAM**. The Set Up RF GOQAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in RF GoQAM Basic Parameter Settings.

Use the following fields when you manage an RF GoQAM in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1RFGoQ43 could represent an RF GoQAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| IP Address | The IP address of this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| Modulation Type | The type of modulation standard that the modulator uses.<br>**Example:** If this modulator uses the International Telecommunications Union standard ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6MHz)**. |
| MAC Address | The MAC address for the modulator. |
| Subnet Mask | The subnet mask where this modulator resides. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a modulator is rebooted. |
| Input Block 1 ASI 1 Clear Transport Stream ID | The number identifying the transport stream for this input block.<br>(Complete for each input port on the GoQAM modulator)<br>A block accepts both a clear and an encrypted version of the same MPEG transport stream. |
| Input Block 2 ASI 2 Clear Transport Stream ID | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. |
| RF OUT | **Modulation** - The type of Select the type of modulation this modulator |

| | |
|---|---|
| modulation this modulator uses | uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters.<br>Specify a unique transport stream ID for each output port on the RF GoQAM modulator.<br>**Note:** Make certain that you enter a TSID that is within the range reserved for our QAM modulators. This range is listed in the Ports area of the Basic Parameters tab for easy reference. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs<br>on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the modulator's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event when a<br>port fails. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>▪ If this RF GoQAM modulator is sending data 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 that will receive data from this modulator. |

| | |
|---|---|
| | ▪ If this RF GoQAM modulator is sending data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field.<br>**Note:** To remove a hub from the **Selected Hubs** field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field. |

**Related Topics**

- RF GoQAM Modulator Connection Settings
- Recommended Modulator Frequencies
- Add a Content RF GoQAM Modulator
- Modifying a QAM, MQAM, GQAM, or GoQAM Modulator
- Locate the MAC Address of a QAM

6.Click **Apply**. The system saves the RF GoQAM modulator information you have entered into the DNCS database and enables the Port to Hubs button.

7.Click **Port To Hubs**. The RF Output window opens. The Basic Parameters area of this window shows the data that you entered for key RF output fields. The Associate Hubs area shows the hubs that are available to receive content data from this RF GoQAM modulator.

8.Define which hubs will receive content data from this RF GoQAM modulator as follows:

- If this RF GoQAM modulator is sending data 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 that will receive data from this modulator.
- If this RF GoQAM modulator is sending data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field.

  **Note:** To remove a hub from the **Selected Hubs** field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field.

9.Click **Save**. The RF Output window closes.

**Important:** You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use. Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance.

10.Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to set up the connections between the RF GoQAM modulator and its associated MPEG source. Go to Setting Up Connections for an RF GoQAM Modulator.

### Setting Up Connections for an RF GoQAM Modulator

After you set up the basic parameters for an RF GoQAM modulator, complete these steps to set up the connections between the modulator and its associated MPEG source.

1. On the Set Up RF GoQAM window, click the **Connectivity** tab. The Connectivity window opens with a graphical representation of the devices already connected to this RF GoQAM modulator.
2. If not already selected, click to select the first **Input Port (Pair 1 Clear)** option.
3. Complete the fields on the screen as described in RF GoQAM Modulator Connection Settings.

Use the following fields when you manage connections for an RF GoQAM.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | The type of MPEG source device being used to send data to this modulator (for example, IRT, MDR and Service Group Object). |
| Device Name | The name of the source device. |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

#### Related Topics

- Recommended Modulator Frequencies
- Add a Content RF GoQAM Modulator
- Modifying a QAM, MQAM, GQAM, or GoQAM Modulator
- Locate the MAC Address of a QAM

4. Click **Apply**. The system saves this information in the DNCS database and updates the illustration so that it shows the information you entered.
5. Click to select the second input port and repeat this procedure from step 3 to set up the connectivity parameters for the second input port on the RF GoQAM modulator.
6. Your next step is to activate the RF GoQAM modulator by placing it online. Go to Activating an RF GoQAM Modulator.

### Activating an RF GoQAM Modulator

After you set up the connections between an RF GoQAM modulator and its associated MPEG source, complete these steps to activate the modulator by placing it online.

**Note:** You can activate an RF GoQAM modulator only after all parameters for the modulator have been saved to the DNCS database, and only after the modulator has finished its boot process. Therefore, you may have to wait a few minutes before you can complete this task.

1. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
2. At the **Administrative State** field, click the **Online** option.
3. Click **Save**. The system saves the RF GoQAM modulator information in the DNCS database and closes the Set Up RF GOQAM window. The QAM List window updates to include the new RF GoQAM modulator.
4. Add the new RF GoQAM modulator to your network map.
5. Do you need to add another RF GoQAM modulator?
   - If **yes**, go back to Setting Up Basic Parameters for an RF GoQAM Modulator.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.
6. Are you setting up your network for the first time?
   - If **yes**, go to step 7.
   - If **no**, continue making any other changes that you need to make to your network.
7. Are you using SONET interfaces in your network?
   - If **yes**, go to Setting Up SONET.
   - If **no**, go to step 8.
8. Does your network comply with OpenCable standards?
   - If **yes**, go to Setting Up OpenCable Compliance.
   - If **no**, continue making any other changes that you need to make to your network.

### Modifying a QAM, MQAM, GQAM, or GoQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM/MQAM Name] > File > Open**

After a QAM, MQAM, GQAM, or GoQAM modulator is saved in the DNCS database, you can modify any of its parameters except for the headend to which it is assigned.

**Note:** You can use this procedure to modify any type of content QAM modulator (for example, a GoQAM or an MQAM modulator).

**Important:** Contact us for assistance in changing a BFS QAM modulator.

Complete these steps to modify a QAM, MQAM, GQAM, or GoQAM modulator in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the QAM, MQAM, GQAM, or GoQAM modulator you want to modify.
5. Click **File > Open**. The Set Up QAM or Set Up MQAM window opens, as appropriate.
6. Make the desired changes. If you need help completing any fields, refer to the following procedures as appropriate:
   - Adding a BFS QAM Modulator
   - Adding a Content QAM Modulator
   - Adding a Content MQAM Modulator
   - Adding a Content GQAM Modulator
   - Adding an RF GoQAM Modulator
   - Adding an IF GoQAM Modulator

   **Note:** If you want to save your changes to the database without closing this window, you can click **Apply** at any time.
7. When you finish making changes, click **Save**. The system saves the new QAM or MQAM modulator information in the DNCS database and closes the Set Up QAM or Set Up MQAM window. The QAM List window updates to include the new modulator information.
8. Update your network map to reflect these changes.
9. Do you need to modify another QAM, MQAM, or GQAM modulator?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Select the QAM, MQAM, GQAM, or GoQAM modulator that you want to reboot.

**Notes:**

- Each MQAM modulator is listed four times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GQAM modulator is listed 16 times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GoQAM (RF or IF) is listed twice (once for each of the modulator's RF output channels), but select only the first occurrence.

5. Click **File > Reset**. The confirmation window appears with the question, "Are you sure you want to reset QAM modulator 'name of modulator'?"

6. Click **Yes**. The QAM List window displays the following message, "The reset request has been received by QAM modulator 'name of modulator'."

### Deleting a QAM, MQAM, GQAM, or GoQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM] > File > Delete**

**Note:** You can use this procedure to delete any type of QAM modulator that carries content.

Complete these steps to delete a QAM, MQAM, GQAM, or GoQAM modulator from the DNCS.

1. First tear down all sessions that are running on the modulator you want to delete.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List window opens.
5. Click once on the row containing the QAM, MQAM, GQAM, or GoQAM modulator that you want to delete.

   **Note:** Even though an MQAM modulator takes up four rows on the QAM List, you need to select only one of the rows to delete it. The same is true for the GQAM, which takes up to 16 rows on the QAM List, and for the GoQAM modulators (RF and IF), which take up two rows.

6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the selected modulator information from the DNCS database and from the QAM List window.
8. Delete the selected modulator from your network map.
9. Do you need to delete another QAM, MQAM, GQAM, or GoQAM modulator?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

### Locate the MAC Address of a QAM

You can look at the sticker on the side of the QAM, MQAM, SCS MQAM, GQAM, or GoQAM to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

## IF GoQAM Modulators

Systems using the Overlay option require an RF GoQAM modulator or an IF GoQAM modulator. These modulators are required because they produce partially encrypted broadcast sessions, which feed DHCTs manufactured by us and by other vendors.

**Note:** Depending upon system architecture, GoQAM modulators can be used in headends or hubs.

- **RF GoQAM Modulators** are used only in a DBDS that uses Overlay technology. An RF GoQAM modulator receives both clear and encrypted content data in an MPEG format from two pairs of ASI inputs. Each pair consists of an encrypted stream and its corresponding clear stream. The RF GoQAM receives RF GoQAMs filter, modify, synchronize, and combine the two data streams into a single transport stream and send this stream to hubs. Once processed by the RF GoQAM, the transport stream can be used by DHCTs from third-party vendors, without regard to the type of encryption method that each DHCT uses. From the QAM List, you can add, modify, or delete an RF GoQAM modulator.
- **IF GoQAM Modulators** are used only in a DBDS that uses Overlay technology. An IF GoQAM modulator receives both a clear and an encrypted data stream. IF GoQAM modulators filter, modify, synchronize, and combine the two data steams into a single transport stream using an IF (intermediate frequency) of 44MHz. Once processed by the IF GoQAM, the transport stream can be fed to DHCTs from different manufacturers, without regard to the type of encryption method that the DHCTs use. Because the modulator uses an IF frequency, it supports applications that require operation below 55 MHz or above 860 MHz. From the QAM List, you can add, modify, or delete an IF GoQAM modulator.

**Related Topics**

- IF GoQAM Settings
- Add a Content IF GoQAM Modulator
- Modifying a QAM, MQAM, GQAM, or GoQAM Modulator
- Resetting a QAM, MQAM, GQAM, or GoQAM Modulator
- Deleting a QAM, MQAM, GQAM, or GoQAM Modulator
- Locate the MAC Address of a QAM

### IF GoQAM Settings

Use the Set Up GoQAM Modulator page on the DNCS Administrative Console to manage the IF GoQAM devices in your network. Two tabs in this window provide settings for the IF GoQAM:

- Basic Parameter settings: Use the settings on the Basic Parameters tab to configure the IF GoQAM.
- Connectivity settings: Use the settings on the Connectivity tab to configure the connections between the modulator and its associated MPEG source

**Note:** Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### IF GoQAM Basic Parameter Settings

Use the following fields when you manage basic parameters for an IF GoQAM.

| Field | Description | |
|---|---|---|
| Headend Name | The headend associated with this modulator. | |
| QAM Name | The name of this modulator.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1RFGoQ43 could represent an RF GoQAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. | |
| IP Address | The IP address of this modulator.<br>Be careful to properly place the dots (.) between numbers. | |
| Modulation Type | The type of modulation standard that the modulator uses.<br>**Example:** If this modulator uses the International Telecommunications Union standard ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6MHz)**. | |
| MAC Address | The MAC address for the modulator. | |
| Subnet Mask | The subnet mask where this modulator resides. | |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a modulator is rebooted. | |
| Input Block 1 ASI 1 Clear Transport Stream ID | The number identifying the transport stream for this input block.<br>(Complete for each input port on the GoQAM modulator) | |
| Input Block 2 ASI 2 Clear Transport Stream ID | A block accepts both a clear and an encrypted version of the same MPEG transport stream. | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. | |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. | |
| RF OUT | **Modulation** - The type of modulation this modulator uses | Select the type of modulation this modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| | **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters.<br>Specify a unique transport stream ID for each output port on the RF GoQAM modulator. |

| | |
|---|---|
| | **Note:** Make certain that you enter a TSID that is within the range reserved for our QAM modulators. This range is listed in the Ports area of the Basic Parameters tab for easy reference. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs<br>on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the modulator's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event when a<br>port fails. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>▪If this RF GoQAM modulator is sending data 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 that will receive data from this modulator.<br>▪If this RF GoQAM modulator is sending data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field.<br>**Note:** To remove a hub from the **Selected Hubs** field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field. |

**Related Topics**

- IF GoQAM Connection Settings
- Recommended Modulator Frequencies
- Add a Content IF GoQAM Modulator
- Locate the MAC Address of a QAM

### IF GoQAM Connection Settings

Use the following fields when you manage connections for an IF GoQAM.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | The type of MPEG source device being used to send data to this modulator (for example, IRT, MDR and Service Group Object). |
| Device Name | The name of the source device. |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

### Related Topics

- Recommended Modulator Frequencies
- Add a Content IF GoQAM Modulator
- Locate the MAC Address of a QAM

### Recommended Modulator Frequencies

Use the center frequencies shown in the following table to send data from your QAM modulators to the DHCTs on your system. Notice that these frequencies are separated by increments of 6 MHz.

**Note:** If you are experiencing signal interference, try offsetting your modulator frequencies by 250 kHz from the frequencies shown in the table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 153 | 159 | 165 | 171 | 177 | 183 | 189 | 195 | 201 | 207 |
| 213 | 219 | 225 | 231 | 237 | 243 | 249 | 255 | 261 | 267 |
| 273 | 279 | 285 | 291 | 297 | 303 | 309 | 315 | 321 | 327 |
| 333 | 339 | 345 | 351 | 357 | 363 | 369 | 375 | 381 | 387 |
| 393 | 399 | 405 | 411 | 417 | 423 | 429 | 435 | 441 | 447 |
| 453 | 459 | 465 | 471 | 477 | 483 | 489 | 495 | 501 | 507 |
| 513 | 519 | 525 | 531 | 537 | 543 | 549 | 555 | 561 | 567 |
| 573 | 579 | 585 | 591 | 597 | 603 | 609 | 615 | 621 | 627 |
| 633 | 639 | 645 | 651 | 657 | 663 | 669 | 675 | 681 | 687 |
| 693 | 699 | 705 | 711 | 717 | 723 | 729 | 735 | 741 | 747 |

### Add a Content IF GoQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > GOQAM >IF GOQAM**

If you are using an IF GoQAM modulator to send content to DHCTs and you have already added an MPEG source to the DNCS database, you are ready to add the IF GoQAM modulator to the DNCS database.

IF GoQAMs are a critical component of our Overlay solution. Overlay allows cable service providers to support DHCTs manufactured by us and by other vendors. IF GoQAM modulators receive both a clear and an encrypted data stream. They filter, modify, synchronize, and combine the two data steams into a single transport stream using an IF (intermediate frequency) of 44MHz. Once processed by the IF GoQAM, the transport stream can be fed to DHCTs from different manufacturers, without regard to the type of encryption method that the DHCTs use.

Because the modulator uses an IF frequency, it supports applications that require operation below 55 MHz or above 860 MHz. For example, the IF output can be connected to the IF sampling port of a fiber interface unit, which sends the output transport stream to hubs that exceed the reach of standard AM (amplitude modulation) fiber.

**Important:** If you are not using Overlay technology, do not add an IF GoQAM modulator to your DBDS. Adding an IF GoQAM modulator to a system that does not use Overlay technology can cause your system to behave unpredictably.

#### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- Name of the headend containing the IF GoQAM modulator
- Name used to identify the IF GoQAM modulator
- IP address for the IF GoQAM modulator (from your system administrator)
- Type of modulation standard that the IF GoQAM modulator uses, such as ITU J.83 Annex B
- MAC address for the IF GoQAM modulator
- Subnet mask for the IF GoQAM modulator (from your system administrator)
- If applicable, the IP address of the default gateway that the network uses
- Number(s) identifying the input pair(s) that physically connect the modulator to the associated MPEG sources.
- Number(s) identifying the output transport stream(s) going from the IF GoQAM modulator to the UpConverters
- Name of the headend containing the associated MPEG sources
- Type of MPEG source devices being used to send data to this IF GoQAM modulator (for example, IRT, MDR, VOD server, and so forth)
- Names of the associated MPEG sources
- Numbers identifying the output ports of the associated MPEG sources that are physically connected to the input ports on this IF GoQAM modulator

**Notes:**

- All of this information should be recorded on your network map. However, if it is not, contact your

system administrator to obtain the information.

- For assistance installing the IF GoQAM, see GoQAM Modulator RF Output and IF Output Hardware Installation and Operation Guide (part number 4004834).

**Related Topics**

- Setting Up Basic Parameters for an IF GoQAM Modulator
- Setting Up Connections for an IF GoQAM Modulator
- Activating an IF GoQAM Modulator

### Setting Up Basic Parameters for an IF GoQAM Modulator

The first step in adding an IF GoQAM modulator is to set up the basic parameters for the modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > QAM > GOQAM > IF GOQAM**. The Set Up IF GOQAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in IF GoQAM Basic Parameter Settings.

Use the following fields when you manage basic parameters for an IF GoQAM.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this modulator. |
| QAM Name | The name of this modulator.<br>You can use up to 15 alphanumeric characters.<br>Be sure to use a name that allows you to easily identify the modulator and where it resides.<br>**Example:** A name of VODhub1RFGoQ43 could represent an RF GoQAM modulator whose IP address ends in 43 that processes VOD data for Hub 1. |
| IP Address | The IP address of this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| Modulation Type | The type of modulation standard that the modulator uses.<br>**Example:** If this modulator uses the International Telecommunications Union standard ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6MHz)**. |
| MAC Address | The MAC address for the modulator. |
| Subnet Mask | The subnet mask where this modulator resides. |
| Default Gateway | If your system uses a default gateway, the IP address of your default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a modulator is rebooted. |
| Input Block 1 ASI 1 Clear Transport Stream ID | The number identifying the transport stream for this input block.<br>(Complete for each input port on the GoQAM modulator)<br>A block accepts both a clear and an encrypted version of the same MPEG transport stream. |
| Input Block 2 ASI 2 Clear Transport Stream ID | |
| Input Port | The type of interface that will receive data from the modulator.<br>If the modulator will process VOD data, the modulator must have an ASI input interface. |
| INPUT Transport Stream ID | The system sets this value automatically when the corresponding transport stream ID is set up and the connection is established on the Connectivity tab. |
| RF OUT | **Modulation** - The type of Select the type of modulation this modulator |

| | |
|---|---|
| modulation this modulator uses | uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| **Transport Stream ID** - Identifies the transport stream | Type a unique number to identify the transport stream going from this modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters.<br>Specify a unique transport stream ID for each output port on the RF GoQAM modulator.<br>**Note:** Make certain that you enter a TSID that is within the range reserved for our QAM modulators. This range is listed in the Ports area of the Basic Parameters tab for easy reference. |
| **Channel Center Frequency (MHz**) - The channel frequency that you will use to send system information to DHCTs | Type the channel frequency that you will use to send system information to DHCTs<br>on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click to see a table of Recommended Modulator Frequencies. |
| **Continuous Wave Mode** - Determines whether the modulator produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output** - Determines whether the modulator's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled** - Determines whether you can set up additional sessions on an RF output port on the modulator | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event when a<br>port fails. |
| **Interleaver Depth** - Determines the depth of interleaving for the modulator | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs** - Allows you to see the hubs available to this modulator | Click to view the hubs that are available to receive content data from this modulator.<br>▪ If this RF GoQAM modulator is sending data 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 that will receive data from this modulator. |

| | |
|---|---|
| | ▪ If this RF GoQAM modulator is sending data to all hubs in the headend, make sure no hubs appear in the Selected Hubs field.<br>**Note:** To remove a hub from the **Selected Hubs** field, select the hub name, and then click **Remove**. The hub name moves to the Available Hubs field. |

**Related Topics**

- IF GoQAM Connection Settings
- Recommended Modulator Frequencies
- Add a Content IF GoQAM Modulator
- Locate the MAC Address of a QAM

6. Click **Apply**. The system saves the IF GoQAM modulator information you have entered into the DNCS database and enables the Connectivity tab.

7. Click **Port To Hubs**. The IF Output window opens. The Basic Parameters area of this window shows the data that you entered for key IF output fields. The Associate Hubs area shows the hubs that are available to receive content data from this IF GoQAM modulator.

8. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to set up the connections between the IF GoQAM modulator and its associated MPEG source. Go to Setting Up Connections for an IF GoQAM Modulator.

### Setting Up Connections for an IF GoQAM Modulator

After you set up the basic parameters for an IF GoQAM modulator, complete these steps to set up the connections between the modulator and its associated MPEG source.

1. On the Set Up IF GoQAM window, click the **Connectivity** tab. The Connectivity window opens with a graphical representation of the devices already connected to this IF GoQAM modulator.
2. If not already selected, click to select the first **Input Port (Pair 1 Clear)** option.
3. Complete the fields on the screen as described in IF GoQAM Connection Settings.

Use the following fields when you manage connections for an IF GoQAM.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives data from the modulator resides. |
| Device Type | The type of MPEG source device being used to send data to this modulator (for example, IRT, MDR and Service Group Object). |
| Device Name | The name of the source device. |

The options that appear on this window after Device Name depend upon what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with this modulator.

**Example:** If your MPEG source were a VOD server, you would have selected a Device Type of **Service Group Object**. Then, in addition to the Device Name, you would need to specify the number that identifies the output port on the MPEG source (the VOD server) that is physically connected to the input port on this modulator.

#### Related Topics

- Recommended Modulator Frequencies
- Add a Content IF GoQAM Modulator
- Locate the MAC Address of a QAM

4. Click **Apply**. The system saves this information in the DNCS database and updates the illustration so that it shows the information you entered.
5. Click to select the second input port and repeat this procedure from step 3 to set up the connectivity parameters for the second input port on the IF GoQAM modulator.
6. Your next step is to activate the IF GoQAM modulator by placing it online. Go to Activating an IF GoQAM Modulator.

### Activating an IF GoQAM Modulator

After you set up the connections between an IF GoQAM modulator and its associated MPEG source, complete these steps to activate the modulator by placing it online.

**Note:** You can activate an IF GoQAM modulator only after all parameters for the modulator have been saved to the DNCS database, and only after the modulator has finished its boot process. Therefore, you may have to wait a few minutes before you can complete this task.

1. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
2. At the **Administrative State** field, click the **Online** option.
3. Click **Save**. The system saves the IF GoQAM modulator information in the DNCS database and closes the Set Up IF GOQAM window. The QAM List window updates to include the new IF GoQAM modulator.
4. Add the new IF GoQAM modulator to your network map.
5. Add the UpConverter that this IF GoQAM feeds to the DNCS database.
6. Do you need to add another IF GoQAM modulator?
   - If **yes**, go back to Setting Up Basic Parameters for an IF GoQAM Modulator.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.
7. Are you setting up your network for the first time?
   - If **yes**, go to step 8.
   - If **no**, continue making any other changes that you need to make to your network.
8. Are you using SONET interfaces in your network?
   - If **yes**, go to Setting Up SONET.
   - If **no**, go to step 9.
9. Does your network comply with OpenCable standards?
   - If **yes**, go to Setting Up OpenCable Compliance.
   - If **no**, continue making any other changes that you need to make to your network.

### Modifying a QAM, MQAM, GQAM, or GoQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM/MQAM Name] > File > Open**

After a QAM, MQAM, GQAM, or GoQAM modulator is saved in the DNCS database, you can modify any of its parameters except for the headend to which it is assigned.

**Note:** You can use this procedure to modify any type of content QAM modulator (for example, a GoQAM or an MQAM modulator).

**Important:** Contact us for assistance in changing a BFS QAM modulator.

Complete these steps to modify a QAM, MQAM, GQAM, or GoQAM modulator in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the QAM, MQAM, GQAM, or GoQAM modulator you want to modify.
5. Click **File > Open**. The Set Up QAM or Set Up MQAM window opens, as appropriate.
6. Make the desired changes. If you need help completing any fields, refer to the following procedures as appropriate:
   - Adding a BFS QAM Modulator
   - Adding a Content QAM Modulator
   - Adding a Content MQAM Modulator
   - Adding a Content GQAM Modulator
   - Adding an RF GoQAM Modulator
   - Adding an IF GoQAM Modulator

   **Note:** If you want to save your changes to the database without closing this window, you can click **Apply** at any time.
7. When you finish making changes, click **Save**. The system saves the new QAM or MQAM modulator information in the DNCS database and closes the Set Up QAM or Set Up MQAM window. The QAM List window updates to include the new modulator information.
8. Update your network map to reflect these changes.
9. Do you need to modify another QAM, MQAM, or GQAM modulator?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Select the QAM, MQAM, GQAM, or GoQAM modulator that you want to reboot.

**Notes:**

- Each MQAM modulator is listed four times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GQAM modulator is listed 16 times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GoQAM (RF or IF) is listed twice (once for each of the modulator's RF output channels), but select only the first occurrence.

5. Click **File > Reset**. The confirmation window appears with the question, "Are you sure you want to reset QAM modulator 'name of modulator'?"

6. Click **Yes**. The QAM List window displays the following message, "The reset request has been received by QAM modulator 'name of modulator'."

### Deleting a QAM, MQAM, GQAM, or GoQAM Modulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [QAM] > File > Delete**

**Note:** You can use this procedure to delete any type of QAM modulator that carries content.

Complete these steps to delete a QAM, MQAM, GQAM, or GoQAM modulator from the DNCS.

1. First tear down all sessions that are running on the modulator you want to delete.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List window opens.
5. Click once on the row containing the QAM, MQAM, GQAM, or GoQAM modulator that you want to delete.

   **Note:** Even though an MQAM modulator takes up four rows on the QAM List, you need to select only one of the rows to delete it. The same is true for the GQAM, which takes up to 16 rows on the QAM List, and for the GoQAM modulators (RF and IF), which take up two rows.

6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the selected modulator information from the DNCS database and from the QAM List window.
8. Delete the selected modulator from your network map.
9. Do you need to delete another QAM, MQAM, GQAM, or GoQAM modulator?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console.

### Locate the MAC Address of a QAM

You can look at the sticker on the side of the QAM, MQAM, SCS MQAM, GQAM, or GoQAM to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

## UpConverters

This section contains information and procedures for adding, modifying, and deleting UpConverters using the DNCS.

## What do you want to do?

- View UpConverter settings
- Add an UpConverter
- Modify an UpConverter
- Delete an UpConverter

### UpConverter Settings

Use the Set Up UpConverter page on the DNCS Administrative Console to manage the UpConverter devices in your network. Three sections of this window provide settings for the UpConverter:

- UpConverter basic settings: Use the settings on the Basic Parameters tab to configure the UpConverter.
- RF output settings: Use the RF output settings to manage the RF output ports for the UpConverter.
- Connection settings: Use the Connectivity tab to manage the connections for the UpConverter.

### UpConverter RF Output Port Settings

Use the following fields when you manage the RF output ports for an UpConverter in the DNCS.

| Field | Description |
|---|---|
| Transport Stream ID | A unique number that identifies the transport stream going from this UpConverter to select hubs. |
| Modulation | The modulation that the UpConverter modulator uses.<br>**Example:** If the UpConverter uses 64 QAM modulation, select **64-QAM**. |
| Channel Center Frequency (MHz) | The frequency of the channel that you will use to send content from this UpConverter to select hubs.<br>Click to see a table of Recommended Modulator Frequencies. |
| Available Hubs | The hubs available to this UpConverter.<br>Select a hub in the **Available Hubs** list and then click **Add**. The hub you selected moves from the Available Hubs list to the Selected Hubs list.<br>Repeat this process until all of the hubs that will receive the output of this UpConverter appear in the **Selected Hubs** list. |

### Related Topics

- Upconverter Connection Settings

Use the following fields when you manage the connections for an UpConverter in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds the UpConverter resides. |
| Device Type | The type of device being used to send data to this UpConverter (for example, IF GoQAM modulator). |
| Device Name | The name previously defined for the device being used to send data to this UpConverter. |
| The options that appear depend on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the IF GoQAM modulator that feeds this UpConverter. | |

### Related Topics

- Add an UpConverter
- Modifying an UpConverter


- Add an UpConverter
- Modifying an UpConverter

### UpConverter Connection Settings

Use the following fields when you manage the connections for an UpConverter in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds the UpConverter resides. |
| Device Type | The type of device being used to send data to this UpConverter (for example, IF GoQAM modulator). |
| Device Name | The name previously defined for the device being used to send data to this UpConverter. |
| The options that appear depend on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the IF GoQAM modulator that feeds this UpConverter. | |

### Related Topics

- Add an UpConverter
- Modifying an UpConverter

### Add an UpConverter

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

After you add an IF GoQAM modulator to the DNCS, next add the UpConverter that the IF GoQAM modulator feeds. UpConverters are used for special applications that have IF outputs, such as the IF GoQAM modulator.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- Name used to identify the UpConverter
- Number identifying the transport stream going from the IF GoQAM modulator to the UpConverter
- Type of modulation the UpConverter modulator uses, such as 256 QAM or 64 QAM
- Number(s) identifying the transport stream(s) going from the UpConverter out to the hubs on your system
- Frequencies of the channels being used to send data from the UpConverter to the hubs on your system
- The hubs that the UpConverter feeds
- Name of the headend containing the IF GoQAM modulator that feeds the UpConverter
- Name of the IF GoQAM modulator sending data to the UpConverter
- Number identifying the output port of the IF GoQAM modulator that is physically connected to the input port on this UpConverter

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Related Topics

- Setting Up Basic Parameters for an UpConverter
- Setting Up RF Outputs for an UpConverter
- Setting Up Connections for an UpConverter

### Setting Up Basic Parameters for an UpConverter

The first step in adding an UpConverter is to set up the basic parameters for the UpConverter.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **UpConverter**. The UpConverter List window opens.
4. Click **File > New**. The Set Up UpConverter window opens with the Basic Parameters tab in the forefront.
5. Click in the **UpConverter Name** field and type the name of this UpConverter. You can use up to 15 alphanumeric characters.

   **Note:** We recommend that you establish a naming scheme that allows you to easily identify the UpConverter and where it resides.

   **Example:** A name of UpConIFGoQ43 could represent an IF QAM modulator whose IP address ends in 43 that processes data for Hub 1.

6. Click in the **Input UpConverter Stream ID** field and type the number identifying the transport stream going from the IF GoQAM modulator to the UpConverter.
7. Click **Apply**. The system applies your changes and makes the RF Output Ports fields and the Connectivity tab available for you to select.
8. You are now ready to set up the RF outputs for the UpConverter. Go to Setting Up RF Outputs for an UpConverter.

### Setting Up RF Outputs for an UpConverter

1.On the Set Up UpConverter window, in the **RF Output Ports** area, click **Add**. The RF Output Port window appears.

2.Complete the fields on the screen as described in UpConverter RF Output Port Settings.

Use the following fields when you manage the RF output ports for an UpConverter in the DNCS.

| Field | Description |
|---|---|
| Transport Stream ID | A unique number that identifies the transport stream going from this UpConverter to select hubs. |
| Modulation | The modulation that the UpConverter modulator uses.<br>**Example:** If the UpConverter uses 64 QAM modulation, select **64-QAM**. |
| Channel Center Frequency (MHz) | The frequency of the channel that you will use to send content from this UpConverter to select hubs.<br>Click to see a table of Recommended Modulator Frequencies. |
| Available Hubs | The hubs available to this UpConverter.<br>Select a hub in the **Available Hubs** list and then click **Add**. The hub you selected moves from the Available Hubs list to the Selected Hubs list.<br>Repeat this process until all of the hubs that will receive the output of this UpConverter appear in the **Selected Hubs** list. |

#### Related Topics

- Upconverter Connection Settings

Use the following fields when you manage the connections for an UpConverter in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds the UpConverter resides. |
| Device Type | The type of device being used to send data to this UpConverter (for example, IF GoQAM modulator). |
| Device Name | The name previously defined for the device being used to send data to this UpConverter. |
| The options that appear depend on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the IF GoQAM modulator that feeds this UpConverter. | |

#### Related Topics

- Add an UpConverter
- Modifying an UpConverter


- Add an UpConverter
- Modifying an UpConverter


3.Click **Save**. The RF Output Port window closes and the Set Up UpConverter window now displays the data you just entered about the RF output of this UpConverter.

4.Are there other RF output ports on this UpConverter that will feed hubs in your system?

- If **yes**, repeat this procedure to set up these RF output ports.
- If **no**, click **Apply**. The system saves the information you have just entered.

5. Your next step is set up the connections between the UpConverter and the IF GoQAM modulator that connects to the UpConverter. Go to Setting Up Connections for an UpConverter.

### Setting Up Connections for an UpConverter

After you set up the UpConverter modulator basic parameters, complete these steps to set up the connections between the UpConverter and the IF GoQAM modulator that feeds the UpConverter.

1. On the Set Up UpConverter window, click the **Connectivity** tab. The Connectivity window opens with a graphical representation of this UpConverter.
2. If not already selected, click the **Input Port** option to select it.
3. Complete the fields on the screen as described in Upconverter Connection Settings.

Use the following fields when you manage the connections for an UpConverter in the DNCS.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds the UpConverter resides. |
| Device Type | The type of device being used to send data to this UpConverter (for example, IF GoQAM modulator). |
| Device Name | The name previously defined for the device being used to send data to this UpConverter. |

The options that appear depend on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the IF GoQAM modulator that feeds this UpConverter.

#### Related Topics

- Add an UpConverter
- Modifying an UpConverter

4. Click **Apply**. The system saves this information in the DNCS database and updates the illustration so that it shows the information you entered.
5. Add the new UpConverter to your network map.
6. Click **File > Close** to close the Set Up UpConverter window and display the UpConverter List window.
7. Do you need to add another UpConverter?
   - If **yes**, go back to Setting Up Basic Parameters for an UpConverter.
   - If **no**, go to step 8.
8. From the UpConverter List window, click **File > Close** to close the UpConverter List window.

### Modifying an UpConverter

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > UpConverter > [UpConverter Name] > File > Open**

After an UpConverter is saved in the DNCS database, you can modify any of its parameters except for the headend to which it is assigned.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **UpConverter**. The UpConverter List window opens.
4. Click once on the row containing the UpConverter you want to modify.
5. Click **File > Open**. The Set Up UpConverter window opens, as appropriate.
6. Make the desired changes. If you need help completing any fields, refer to Add an UpConverter.

   **Note:** If you would like to save your changes to the database without closing this window, you can click **Apply** at any time.

7. When you finish making changes, click **Save**. The system saves the new UpConverter information in the DNCS database and closes the Set Up UpConverter window. The QAM List window updates to include the new modulator information.
8. Update your network map to reflect these changes.
9. Do you need to modify another UpConverter modulator?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the UpConverter List window and return to the DNCS Administrative Console.

### Deleting an UpConverter

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > UpConverter > [UpConverter] > File > Delete**

You can use this procedure to delete an UpConverter from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **UpConverter**. The UpConverter List window opens.
4. Click once on the row containing the UpConverter that you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the UpConverter information from the DNCS database and from the UpConverter List window.
7. Delete the UpConverter from your network map.
8. Do you need to delete another UpConverter?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the UpConverter List window and return to the DNCS Administrative Console.

# Partially Encrypted Sessions

## Set Up Partially Encrypted Sessions for Secure or PPV Services

Overlay technology uses a special encryption method that partially encrypts broadcast sessions to deliver content to DHCTs. Partially encrypted sessions consist mostly of unencrypted MPEG packets and a percentage of identical packets encrypted by our systems and by systems manufactured by other vendors. This technique allows both our DHCTs and DHCTs from other manufacturers to function in the same network.

After setting up a partially encrypted session, you can use the session to provide secure or PPV services to subscribers who have a DHCT from us or from another manufacturer.

**Important:** Because only GoQAM modulators provide partially encrypted sessions, set up partially encrypted sessions on only GoQAM modulators.

### You Need to Know

Before You Begin

Before you set up partially encrypted sessions, first make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Configure the DNCS for Overlay Technology.

You might also want to have your network map readily available.

Time To Complete

Setting up a partially encrypted session takes approximately 5 minutes to complete. However, setting up a secure or PPV service from this partially encrypted session takes from 45 minutes to an hour to complete.

Performance Impact

Setting up a partially encrypted session and using it to provide a secure or PPV service does not impact network performance. You can complete this procedure at any time.

### Setting Up Partially Encrypted Sessions

The following steps summarize the tasks required to set up partially encrypted sessions. Each step provides a link to a more detailed procedure.

1. Make sure you have completed all of the necessary steps specified in Configure the DNCS for Overlay Technology.
2. If you have not already done so, add the non-SA source to the DNCS Source List.
3. Create a source definition from a source in the Source List and use it to build a partially encrypted session.
4. Now that you have built a partially encrypted session, use this session to provide a secure or PPV service to subscribers:
   - To create a secure service from this partially encrypted session, go to **step 4** of Setting Up Secure Services.
   - To create a PPV service from this partially encrypted session, go to **step 4** of Setting Up PPV Services.

## Set Up Partially Encrypted Sessions for Secure or PPV Services

Overlay technology uses a special encryption method that partially encrypts broadcast sessions to deliver content to DHCTs. Partially encrypted sessions consist mostly of unencrypted MPEG packets and a percentage of identical packets encrypted by our systems and by systems manufactured by other vendors. This technique allows both our DHCTs and DHCTs from other manufacturers to function in the same network.

After setting up a partially encrypted session, you can use the session to provide secure or PPV services to subscribers who have a DHCT from us or from another manufacturer.

**Important:** Because only GoQAM modulators provide partially encrypted sessions, set up partially encrypted sessions on only GoQAM modulators.

### You Need to Know

▸ Before You Begin

Before you set up partially encrypted sessions, first make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Configure the DNCS for Overlay Technology.

You might also want to have your network map readily available.

▸ Time To Complete

Setting up a partially encrypted session takes approximately 5 minutes to complete. However, setting up a secure or PPV service from this partially encrypted session takes from 45 minutes to an hour to complete.

▸ Performance Impact

Setting up a partially encrypted session and using it to provide a secure or PPV service does not impact network performance. You can complete this procedure at any time.

# Partially Encrypted Sessions

## Set Up Partially Encrypted Sessions for Secure or PPV Services

Overlay technology uses a special encryption method that partially encrypts broadcast sessions to deliver content to DHCTs. Partially encrypted sessions consist mostly of unencrypted MPEG packets and a percentage of identical packets encrypted by our systems and by systems manufactured by other vendors. This technique allows both our DHCTs and DHCTs from other manufacturers to function in the same network.

After setting up a partially encrypted session, you can use the session to provide secure or PPV services to subscribers who have a DHCT from us or from another manufacturer.

**Important:** Because only GoQAM modulators provide partially encrypted sessions, set up partially encrypted sessions on only GoQAM modulators.

### You Need to Know

▸ Before You Begin

Before you set up partially encrypted sessions, first make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Configure the DNCS for Overlay Technology.

You might also want to have your network map readily available.

▸ Time To Complete

Setting up a partially encrypted session takes approximately 5 minutes to complete. However, setting up a secure or PPV service from this partially encrypted session takes from 45 minutes to an hour to complete.

▸ Performance Impact

Setting up a partially encrypted session and using it to provide a secure or PPV service does not impact network performance. You can complete this procedure at any time.

### Setting Up Partially Encrypted Sessions

The following steps summarize the tasks required to set up partially encrypted sessions. Each step provides a link to a more detailed procedure.

1. Make sure you have completed all of the necessary steps specified in Configure the DNCS for Overlay Technology.
1. If you have not already done so, add the non-SA source to the DNCS Source List.
1. Create a source definition from a source in the Source List and use it to build a partially encrypted session.
1. Now that you have built a partially encrypted session, use this session to provide a secure or PPV service to subscribers:
    - To create a secure service from this partially encrypted session, go to **step 4** of Setting Up Secure Services.
    - To create a PPV service from this partially encrypted session, go to **step 4** of Setting Up PPV Services.

### Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

#### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

#### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

### Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

#### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

#### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

### Add a Partially Encrypted Session

**Important:** Follow this procedure only if your system uses Overlay technology and uses GoQAM modulators. Only GoQAM modulators produce partially encrypted sessions.

After you add a content source to the Source List, define the source and use it to build a partially encrypted session. A partially encrypted session can be delivered to DHCTs.

**Note:** Sessions define and allocate the resources that your network uses to deliver content. When you build a session, you identify the equipment where the content originates, such as an IRT. You also identify the GoQAM modulator that places the content onto the HFC network.

### You Need to Know

▸ Before You Begin

Before you create a partially encrypted session, you must have the following information:

- Name and Source ID that you gave the source when you added the content source to the Source List
- Number of the channel where the service will be displayed
- MPEG program number from your content service provider
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)

▸ Time To Complete

Building a partially encrypted session takes approximately 20 minutes to complete.

▸ Performance Impact

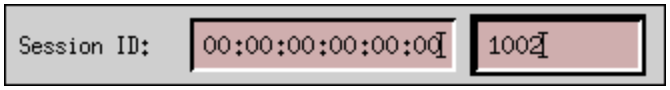
Building a partially encrypted session does not impact network performance. You can complete this procedure at any time.

### Related Topics

- Partially Encrypted Session Settings
- Adding a Partially Encrypted Session

### Partially Encrypted Session Settings

Use the following fields when you manage a partially encrypted session in the DNCS.

| Field | Description | |
|---|---|---|
| Session ID | **Left window** - The session MAC address. Type 12 zeros (the system inputs the colons for you). | |
| | **Right Session ID field** - The source ID you used when you added the content source. | |
| | Your final entry will look similar to the following example:<br>  | |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source. | |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year. **Example:** You would type July 4, 2007, as **07042007**. The system inputs the slashes for you and displays 07/04/2007.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. | |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** You would type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. | |
| Define Session | Define the session programming.<br>Select the **Broadcast** programming option because this source will provide broadcast (audio/video) programming rather than system information. | |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br>You defined the MPEG source when you set up your network. | |
| Select Outputs | The carrier that will receive content from this source. | |
| Wrap-up | **Input MPEG Program Number** | The MPEG program number of the clear stream that the GoQAM modulator receives. |
| | **Incumbent MPEG Program Number** | The MPEG program number of the non-SA encrypted stream that the GoQAM modulator receives. |
| | **Bandwidth** | The amount of bandwidth (in Mbps) that the system should allow for this service.<br>This value is usually defined by your content service provider. Requirements vary from |

| | |
|---|---|
| | system to system. |
| **Audio Encryption Percentage** | Leave the default value of **5** so that the modulator will use our encryption method to partially encrypt the audio portion of the clear stream. |
| **Video Encryption Percentage** | Leave the default value of **2** so that the modulator will use our encryption method to partially encrypt the video portion of the clear stream. |

## Related Topics

- Adding a Partially Encrypted Session

### Adding a Partially Encrypted Session

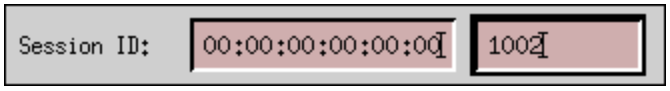
**Notes:**

- This procedure applies to systems that use Overlay technology and GoQAM modulators.
- If you are sending the same source content through more than one GoQAM modulator,you must define the source for each modulator.

**Example:** If you are sending the same source content through six GoQAM modulators, you must define the source six times once for each modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define.
5. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
6. Click **File > New Digital**. The Digital Source Set Up window opens.
7. Complete the fields on the screen as described in Partially Encrypted Session Settings. Be sure to click **Next** to move to the next screen in the sequence.

Use the following fields when you manage a partially encrypted session in the DNCS.

| Field | Description |
|---|---|
| Session ID | **Left window** - The session MAC address. Type 12 zeros (the system inputs the colons for you). |
| | **Right Session ID field** - The source ID you used when you added the content source. |
| | Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year. **Example:** You would type July 4, 2007, as **07042007**. The system inputs the slashes for you and displays 07/04/2007.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** You would type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>Displays only if you select the **Specify effective date and time** option or if you select the **Custom** option in Date/Time. |

| | | |
|---|---|---|
| Define Session | Define the session programming.<br><br>Select the **Broadcast** programming option because this source will provide broadcast (audio/video) programming rather than system information. | |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br><br>You defined the MPEG source when you set up your network. | |
| Select Outputs | The carrier that will receive content from this source. | |
| Wrap-up | **Input MPEG Program Number** | The MPEG program number of the clear stream that the GoQAM modulator receives. |
| | **Incumbent MPEG Program Number** | The MPEG program number of the non-SA encrypted stream that the GoQAM modulator receives. |
| | **Bandwidth** | The amount of bandwidth (in Mbps) that the system should allow for this service.<br><br>This value is usually defined by your content service provider. Requirements vary from system to system. |
| | **Audio Encryption Percentage** | Leave the default value of **5** so that the modulator will use our encryption method to partially encrypt the audio portion of the clear stream. |
| | **Video Encryption Percentage** | Leave the default value of **2** so that the modulator will use our encryption method to partially encrypt the video portion of the clear stream. |

8. Click **Save** on the Save Source Definition window. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

9. Will other GoQAM modulators deliver this content to different portions of your network?

   - If **yes**, for each additional GoQAM modulator that carries this content, repeat this procedure from step 5 to build partially encrypted sessions on each modulator.
   - If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

10. Now that you have built a partially encrypted session, use this session to provide a secure or PPV service to subscribers:

    - To create a secure service from this partially encrypted session, go to step 4 of Setting Up Secure Services.
    - To create a PPV service from this partially encrypted session, go to step 4 of Setting Up PPV Services.

## Table-Based QAM Modulators for VOD

This window lists the table-based QAMs that are part of your DBDS. Table-based QAMs from us are known as Continuum DVP™ eXtra Dense QAM Array (XDQA) QAMs. If your system uses Overlay technology, your third-party QAMs are also listed in this window.

Table-based QAMs are used to provide VOD service, and, for this reason, are part of a service group. By adding table-based QAMs to the DNCS, you ensure that set-tops receive information about service groups that contain table-based QAMs. If your system uses table-based QAMs and these QAMs have not been added to the DNCS, set-tops may be unable to tune to the correct channel to receive a VOD event.

## What do you want to do?

- Review settings for table-based QAMs
- Add a table-based QAM to the DNCS
- Use the Filter to display table-based QAMs
- Modify a table-based QAM
- Delete a table-based QAM
- Manage sessions on table-based QAMs

### Table-Based QAM Settings

Use the Table-Based QAM window on the DNCS Administrative Console to manage the table-based QAM devices in your network. Three tabs in this window provide settings for the table-based QAM:

- Basic Parameters - Table-Based QAM
- RF Parameter Settings - Table-Based QAM
- Session Data Parameter Settings - Table-Based QAM

### Table-Based QAM Basic Parameter Settings

Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM.<br>You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

### Related Topics

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

### Table-Based QAM RF Parameter Settings

Use the following fields when you manage RF parameters for a table-based QAM.

| Field | Description |
|---|---|
| TSID | A unique number to identify the transport stream going from this table-based QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365.<br>**Note:** TSID ranges are defined from DNCS System Configuration. If you receive a range error message, you can change values from the following location: **DNCS tab > System Provisioning tab > DNCS System Configuration > Advanced Parameters tab** |
| Frequency | The frequency (in MHz) of the channel you will use to send data from this table-based QAM to the hubs in your system.<br>You can enter a value in 6 MHz increments from 91 to 861. |
| Modulation Type | The type of modulation this QAM uses. |
| Bandwidth | The bandwidth (in Mbps) that the system should reserve for the QAM. |
| Port Number | The carrier output port associated with the frequency you entered. |

### Related Topics

- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

### Table-Based QAM Session Data Parameter Settings

These parameters are typically loaded from a data file to automatically populate the fields. The file containing the session data uses the following format: **udp port,output port,program,low pid,high pid,optional tsid**

**Important:** If the TSID is not provided, the TSID must be derivable based on the UDP port.

After you add a table-based QAM to your system, you can modify session data for the QAM whenever needed. You can continue to upload new files with new session information or you can make changes to session information directly from the Table-Based QAMs List window. To make changes manually, directly from the Table-Based QAMs List window, see Modify Session Data for a Table-Based QAM.

### Related Topics

- Add a Table-Based QAM
- Upload Session Data File to a Table-Based QAM

### Table-Based QAM Filter

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > Filter**

From the Filter area on the Table-Based QAMs List window, you can quickly retrieve information about the table-based QAMs in your system.

### Related Topics

- Learn about Filter settings for table-based QAMs
- Use the Filter to search and display specific Table-Based QAMs in your system
- Learn about the data that the Filter displays

### Table-Based QAM Filter Settings

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > Filter**

This section describes Table-Based QAM Filter options and provides examples to show how the Filter searches for table-based QAM data based on your selections.

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field.<br>**Note:** This field accepts only numbers. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125<br>172.1**4**.5.32<br>172.17.5.5**4** |

### Table-Based QAM Filter Options

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125 |

| | | |
|---|---|---|
| | **Note:** This field accepts only numbers. | 172.1**4**.5.32<br>172.17.5.5**4** |

## Related Topics

- Table-Based QAMs Filter Data
- Use the Filter to Display Table-Based QAMs

### Table-Based QAM Filter Settings

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > Filter**

This section describes Table-Based QAM Filter options and provides examples to show how the Filter searches for table-based QAM data based on your selections.

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field.<br>**Note:** This field accepts only numbers. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125<br>172.1**4**.5.32<br>172.17.5.5**4** |

### Table-Based QAM Filter Options

The following table describes the Filter options for searching table-based QAMs.

| By Field | By Value | Examples |
|---|---|---|
| **QAM Name** | Enter any part of a QAM name in the By Value field to have the filter display QAMs whose names match any portion of the text entered in this field.<br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **te** in the By Value field, the Filter finds and displays QAMs with any of the following names:<br>▪**te**n<br>▪**te**stqam<br>However, a QAM named **Testqam** would not be shown, since the search is case-sensitive. |
| **Headend** | Select any of the headends shown in the list. | The Filter finds all the table-based QAMs assigned to the selected headend. |
| **IP** | Enter any part of an IP address in the By Value field to have the filter display QAMs with IP addresses that match any portion of the text entered in this field. | If you enter **4** in the By Value field, the Filter finds and displays QAMs that<br>have any of the following IP addresses:<br>172.17.**4**.125 |

| | | |
|---|---|---|
| | **Note:** This field accepts only numbers. | 172.1**4**.5.32<br>172.17.5.5**4** |

**Related Topics**

- Table-Based QAMs Filter Data
- Use the Filter to Display Table-Based QAMs

### Use the Filter to Display Table-Based QAMs

1. Click the **By Field** arrow and select one of the following options:
   - Headend
   - IP
   - Name

**Note:** For a description of these options, see Table-Based QAM Filter Settings.

2. Click in the **By Value** field and enter data in this field, or when filtering by Headend, click the Headend arrow and select the headend containing the QAM.

**Note:** For examples of how By Value data affects searches, see Table-Based QAMs Filter Settings.

3. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Table-Based QAMs List window.

**Note:** For information about the data displayed, see Table-Based QAM Filter Data.

**Table-Based QAM Filter Data**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM**

When you use the Filter to search for and display service groups, search results are shown in the Table-Based QAMs List window, which lists the following information:

- **QAM Name** - Shows the name of the table-based QAM
- **IP Address** - Shows the GigE IP address of the table-based QAM
- **MAC Address** - Shows the GigE MAC address for the table-based QAM
- **Online** - Determines whether the QAM is active (Online enabled) or inactive (Online disabled)
- **Headend** - Shows the name of the headend containing the table-based QAM

**Related Topics**

- Add a Table-Based QAM
- Modify a Table-Based QAM Modulator
- Delete a Table-Based QAM Modulator
- Manage Table-Based QAM Sessions

### Add a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs**

From the Table-Based QAMs interface, you can add our Continuum DVP™ eXtra Dense QAM Array (XDQA) QAMs. If your system uses Overlay technology, you also add third-party QAMs using this interface.

Table-based QAMs are used to provide VOD service, and, for this reason, are part of a service group. By adding table-based QAMs to the DNCS, you ensure that DHCTs receive information about service groups that contain table-based QAMs. If your system uses table-based QAMs and these QAMs have not been added to the DNCS, DHCTs may be unable to tune to the correct channel to receive a VOD event.

#### You Need to Know

Process Overview

To add table-based QAM modulators to the DNCS, you must complete the following tasks in the order presented.

1. Record your planned associations between service groups and table-based QAMs. You will need a service group ID for each table-based QAM you add.
2. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

**Notes:**

- The file uses the following format:

udp port,output port,program,low pid,high pid,optional tsid

- If the TSID is not provided, the TSID must be derivable based on the UDP port.

3. Add the table-based QAMs to the DNCS.
4. Configure RF parameters for the table-based QAMs.

#### Related Topics

- Configure session data for Table-Based QAM Modulators

#### Adding a Table-Based QAM Modulator

Follow these steps to add table-based QAM to the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. Click **Add**. The Add Table-Based QAM window opens.
5. Complete the fields on the screen as described in Table-Based QAM Basic Parameter Settings.

Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM. |

| | |
|---|---|
| | You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

**Related Topics**

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

6. Click **Save**. The Add Table-Based QAM window closes and the QAM you added displays in the Table-Based QAMs List window.

7. Select the QAM from the list and click **Configure RF Parameters**. The RF Parameters window opens for the QAM you selected.

8. Click **Add**. Empty data fields appear in the window.

9. Complete the fields on the screen as described in Table-Based QAM RF Parameter Settings.

Use the following fields when you manage RF parameters for a table-based QAM.

| Field | Description |
|---|---|
| TSID | A unique number to identify the transport stream going from this table-based QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365.<br>**Note:** TSID ranges are defined from DNCS System Configuration. If you receive a range error message, you can change values from the following location: **DNCS tab > System Provisioning tab > DNCS System Configuration > Advanced Parameters tab** |
| Frequency | The frequency (in MHz) of the channel you will use to send data from this table-based QAM to the hubs in your system.<br>You can enter a value in 6 MHz increments from 91 to 861. |
| Modulation Type | The type of modulation this QAM uses. |
| Bandwidth | The bandwidth (in Mbps) that the system should reserve for the QAM. |
| Port Number | The carrier output port associated with the frequency you entered. |

**Related Topics**

- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

10. Click **Save**. The system saves the information you have entered and updates the RF Parameters

window with this information. The status area of the window displays the message, "RF Parameters saved successfully.

11. Click **Exit** to close the window.

**Related Topics**

- Upload Session Data for Table-Based QAMs

### Add a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs**

From the Table-Based QAMs interface, you can add our Continuum DVP™ eXtra Dense QAM Array (XDQA) QAMs. If your system uses Overlay technology, you also add third-party QAMs using this interface.

Table-based QAMs are used to provide VOD service, and, for this reason, are part of a service group. By adding table-based QAMs to the DNCS, you ensure that DHCTs receive information about service groups that contain table-based QAMs. If your system uses table-based QAMs and these QAMs have not been added to the DNCS, DHCTs may be unable to tune to the correct channel to receive a VOD event.

#### You Need to Know

Process Overview

To add table-based QAM modulators to the DNCS, you must complete the following tasks in the order presented.

1. Record your planned associations between service groups and table-based QAMs. You will need a service group ID for each table-based QAM you add.
2. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

**Notes:**

- The file uses the following format:

  udp port,output port,program,low pid,high pid,optional tsid

- If the TSID is not provided, the TSID must be derivable based on the UDP port.

3. Add the table-based QAMs to the DNCS.
4. Configure RF parameters for the table-based QAMs.

#### Related Topics

- Configure session data for Table-Based QAM Modulators

#### Adding a Table-Based QAM Modulator

Follow these steps to add table-based QAM to the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. Click **Add**. The Add Table-Based QAM window opens.
5. Complete the fields on the screen as described in Table-Based QAM Basic Parameter Settings.

Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM. |

| | |
|---|---|
| | You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

**Related Topics**

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

6. Click **Save**. The Add Table-Based QAM window closes and the QAM you added displays in the Table-Based QAMs List window.

7. Select the QAM from the list and click **Configure RF Parameters**. The RF Parameters window opens for the QAM you selected.

8. Click **Add**. Empty data fields appear in the window.

9. Complete the fields on the screen as described in Table-Based QAM RF Parameter Settings.

Use the following fields when you manage RF parameters for a table-based QAM.

| Field | Description |
|---|---|
| TSID | A unique number to identify the transport stream going from this table-based QAM out to the hubs in your system.<br>You can use any number from 0 to 66,365.<br>**Note:** TSID ranges are defined from DNCS System Configuration. If you receive a range error message, you can change values from the following location: **DNCS tab > System Provisioning tab > DNCS System Configuration > Advanced Parameters tab** |
| Frequency | The frequency (in MHz) of the channel you will use to send data from this table-based QAM to the hubs in your system.<br>You can enter a value in 6 MHz increments from 91 to 861. |
| Modulation Type | The type of modulation this QAM uses. |
| Bandwidth | The bandwidth (in Mbps) that the system should reserve for the QAM. |
| Port Number | The carrier output port associated with the frequency you entered. |

**Related Topics**

- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

10. Click **Save**. The system saves the information you have entered and updates the RF Parameters window with this information. The status area of the window displays the message, "RF Parameters

saved successfully.

11. Click **Exit** to close the window.

**Related Topics**

- Upload Session Data for Table-Based QAMs

### Upload Session Data to a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data > File Upload**

This procedure describes how to upload session data from a file because this is the preferred method for populating this data on the DNCS. If you want to enter session data manually, be sure to obtain documentation listing the standard values for UDP Port, Program Number, High PID, and Low PID for the type of table-based QAM you are configuring.

Follow these steps to configure session data for new table-based QAMs.

1. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

   **Important:**

   - The file uses the following format: udp port,output port,program,low pid,high pid,optional tsid
   - If the TSID is not provided, the TSID must be derivable based on the UDP port.

   **Note:** To ensure that this file is saved during a system backup, place this file in the appropriate directory on the DNCS. For assistance, refer to Recommendations for Installing Applications on the DNCS and Application Server (part number 749638). To obtain a copy of this document, see Printed Resources.

2. On the DNCS Administrative Console, click the **DNCS** tab.
3. On the DNCS tab, click the **Network Element Provisioning** tab.
4. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
5. Select a newly added table-based QAM.
6. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
7. Click **File load**.
8. Click the **Browse** button.
9. From the File Upload window, navigate to the location where the session data file for this table-based QAM is stored and click **Open**. The path and the file you selected is populated in the **Select the file to be uploaded** field.
10. Click the **Load** button.
11. Wait for confirmation that all of the records were loaded with 0 errors. Click **OK** in the confirmation window.
12. Click **Save changes**.

    **Important:** You must click **Save changes** to save the session data. Clicking **OK** in the previous step does not automatically save the session data.

13. Click **Exit** to close the window.

#### Related Topics

- Modify Session Data for a Table-Based QAM

### Reset a Table-Based QAM

**Quick Path: DNCS > Network Element Provisioning > QAM > [Select QAM] > File > Reset**

Resetting a QAM, MQAM, GQAM, or GoQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

**Important:** You can reset only our modulators from the DNCS. Generic QAM modulators cannot be reset from the DNCS. To reset a generic QAM modulator, refer to the documentation provided by the manufacturer of the modulator.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Select the QAM, MQAM, GQAM, or GoQAM modulator that you want to reboot.

**Notes:**

- Each MQAM modulator is listed four times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GQAM modulator is listed 16 times (once for each of the modulator's RF output channels), but select only the first occurrence.
- Each GoQAM (RF or IF) is listed twice (once for each of the modulator's RF output channels), but select only the first occurrence.

5. Click **File > Reset**. The confirmation window appears with the question, "Are you sure you want to reset QAM modulator 'name of modulator'?"
6. Click **Yes**. The QAM List window displays the following message, "The reset request has been received by QAM modulator 'name of modulator'."

## Reset a Table-Based QAM

### Modify a Table-Based QAM

Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table- Based QAMs > [Select QAM] > Edit

You can modify several aspects of the table-based QAM:

- Modify Basic Parameters for a Table-Based QAM
- Modifying RF Parameters for a Table-Based QAM
- Modify Session Data for a Table-Based QAM

### Modify Basic Parameters for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAM > [Filter and Select QAM] > Edit**

After you add a table-based QAM to your system, you can modify any of its basic parameters whenever needed. Follow this procedure to modify the basic parameters for table-based QAMs.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. Use the Filter to display the QAM that you want to modify.

   **Note:** For assistance using the Filter, see Table-Based QAM Filter.

5. Select the QAM that you want to modify. A check mark appears in the box to the left of the QAM.
6. Click **Edit**. The Edit Table-Based QAM window opens for the QAM you selected.
7. Make changes to the fields as described in Table-Based QAM Basic Parameter Settings.

   Use the following fields when you manage a table-based QAM in the DNCS.

| Field | Description |
|---|---|
| QAM Name | The name of this table-based QAM.<br>You are limited to 20 alpha numeric characters.<br>We recommend that you establish a naming scheme that allows you to easily identify the QAM and where it resides. |
| IP Address | The GigE IP address of this table-based QAM.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| MAC Address | The GigE MAC address for this table-based QAM. |
| Online | Determines whether the QAM is active or inactive. |
| Headend | The headend associated with this table-based QAM. |

**Related Topics**

- Table-Based QAM RF Parameter Settings
- Table-Based QAM Session Data Parameter Settings
- Add a Table-Based QAM

8. Click **Save** to save your changes. The Edit Table-Based QAM window closes and the changes you made are shown in the Table-Based QAMs List window.
9. Click **Exit** to close the Table-Based QAMs List window.

**Related Topics**

- Modifying RF Parameters for a Table-Based QAM

- Modify Session Data for a Table-Based QAM

### Modify RF Parameters for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure RF Parameters**

After you add a table-based QAM to your system, you can modify any of its RF parameters whenever needed.

Follow these steps to modify RF Parameters for table-based QAMs.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAM**.
4. From the Table-Based QAMs List window, select a table-based QAM.
5. Click **Configure RF Parameters**. The RF Parameters window opens for the QAM you selected.
6. Complete one of the following steps.
   - To edit existing parameters, click in the fields you want to edit and make changes. Then, click **Save** to save your changes.
   - To add a new RF parameter, click **Add** and complete the new data fields that appear. Then, click **Save** to save your changes.
   - To delete an existing parameter, click **Delete**. When asked to confirm, click **OK**.

   **Note:** If necessary, upload a new session data file to match the RF parameter changes you have made.
7. Click **Exit** to close the window.

**Related Topics**

- Modify Session Data for a Table-Based QAM
- Table-Based QAM RF Parameter Settings

### Modify Session Data for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data**

After you upload session data for a table-based QAM, you can modify the session data whenever needed. When entering session data manually, be sure to obtain documentation listing the standard values for UDP Port, Program Number, High PID, and Low PID for the type of table-based QAM you are configuring.

Follow these steps to manually modify session data for table-based QAMs from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM whose sessions you want to modify.
5. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
6. Select the session and click **Edit**. The Edit Session Data window opens.
7. Update the information as needed, and click **Save** to save your changes. The Edit Session Data window closes and the Session Data window updates with the new data.

   **Note:** For assistance see Table-Based QAM Session Data Parameters.

   These parameters are typically loaded from a data file to automatically populate the fields. The file containing the session data uses the following format: **udp port,output port,program,low pid,high pid,optional tsid**

   **Important:** If the TSID is not provided, the TSID must be derivable based on the UDP port.

   After you add a table-based QAM to your system, you can modify session data for the QAM whenever needed. You can continue to upload new files with new session information or you can make changes to session information directly from the Table-Based QAMs List window. To make changes manually, directly from the Table-Based QAMs List window, see Modify Session Data for a Table-Based QAM.

   **Related Topics**

   - Add a Table-Based QAM
   - Upload Session Data File to a Table-Based QAM

8. Click **Exit** to close the window.

**Related Topics**

- Delete Sessions from a Table-Based QAM
- Upload Session Data to a Table-Based QAM

### Upload Session Data File for Table-Based QAM Modulators

Uploading session data from a file is the preferred method for populating this data on the DNCS.

Follow these steps to upload a new session data file for new table-based QAM modulators.

1. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.
2. From the Table-Based QAMs List window, select the table-based QAM you need to edit.
3. Click **Configure Session Data**. The Table-Based Session Data window opens.
4. Click **File load**.
5. Click the **Browse** button.
6. From the File Upload window, navigate to the location where the session data file for this table-based QAM is stored and click **Open**. The path and the file you selected is populated in the **Select the file to be uploaded** field.
7. Click the **Load** button.
8. Wait for confirmation that all of the records were loaded with 0 errors. Click **OK** in the confirmation window.
9. Click **Save changes**.

   **Important:** You must click **Save changes** to save the session data. Clicking **OK** in the previous step does not automatically save the session data.

10. Do you need to upload new session data for another table-based QAM?
    - If **yes**, click **Table-Based QAMs List** from the navigation path at the top of the window. Then repeat this procedure from step 2.
    - If **no**, you have completed this procedure. If necessary, change the RF parameters (TSIDs) for the QAM sessions you edited.

### Delete a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Delete**

Follow these steps to delete a table-based QAM from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM you want to delete.
5. Click **Delete**. A confirmation window opens.
6. Click **OK**. The table-based QAM is removed from the list.
7. Do you want to delete additional table-based QAMs?
   - If **yes**, repeat steps 4 and 5 for each table-based QAM you want to delete.
   - If **no**, click **Exit**.

**Manage Table-Based QAM Sessions**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Filter to show QAMs] > [Select QAM] > Configure Session Data**

From the Session Data window, you can manage sessions for your table-based QAMs.

**Related Topics**

- Upload session data to a table-based QAM
- Modify session data for a table-based QAM
- Delete sessions on a table-based QAM

### Upload Session Data to a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data > File Upload**

This procedure describes how to upload session data from a file because this is the preferred method for populating this data on the DNCS. If you want to enter session data manually, be sure to obtain documentation listing the standard values for UDP Port, Program Number, High PID, and Low PID for the type of table-based QAM you are configuring.

Follow these steps to configure session data for new table-based QAMs.

1. Ensure the comma-delimited text file containing the session data for table-based QAMs is loaded on the DNCS. Make sure you know the path to this file.

   **Important:**

   - The file uses the following format: udp port,output port,program,low pid,high pid,optional tsid
   - If the TSID is not provided, the TSID must be derivable based on the UDP port.

   **Note:** To ensure that this file is saved during a system backup, place this file in the appropriate directory on the DNCS. For assistance, refer to Recommendations for Installing Applications on the DNCS and Application Server (part number 749638). To obtain a copy of this document, see Printed Resources.

2. On the DNCS Administrative Console, click the **DNCS** tab.
3. On the DNCS tab, click the **Network Element Provisioning** tab.
4. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
5. Select a newly added table-based QAM.
6. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
7. Click **File load**.
8. Click the **Browse** button.
9. From the File Upload window, navigate to the location where the session data file for this table-based QAM is stored and click **Open**. The path and the file you selected is populated in the **Select the file to be uploaded** field.
10. Click the **Load** button.
11. Wait for confirmation that all of the records were loaded with 0 errors. Click **OK** in the confirmation window.
12. Click **Save changes**.

    **Important:** You must click **Save changes** to save the session data. Clicking **OK** in the previous step does not automatically save the session data.

13. Click **Exit** to close the window.

**Related Topics**

- Modify Session Data for a Table-Based QAM

### Modify Session Data for a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data**

After you upload session data for a table-based QAM, you can modify the session data whenever needed. When entering session data manually, be sure to obtain documentation listing the standard values for UDP Port, Program Number, High PID, and Low PID for the type of table-based QAM you are configuring.

Follow these steps to manually modify session data for table-based QAMs from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM whose sessions you want to modify.
5. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
6. Select the session and click **Edit**. The Edit Session Data window opens.
7. Update the information as needed, and click **Save** to save your changes. The Edit Session Data window closes and the Session Data window updates with the new data.

   **Note:** For assistance see Table-Based QAM Session Data Parameters.

   These parameters are typically loaded from a data file to automatically populate the fields. The file containing the session data uses the following format: **udp port,output port,program,low pid,high pid,optional tsid**

   **Important:** If the TSID is not provided, the TSID must be derivable based on the UDP port.

   After you add a table-based QAM to your system, you can modify session data for the QAM whenever needed. You can continue to upload new files with new session information or you can make changes to session information directly from the Table-Based QAMs List window. To make changes manually, directly from the Table-Based QAMs List window, see Modify Session Data for a Table-Based QAM.

   **Related Topics**

   - Add a Table-Based QAM
   - Upload Session Data File to a Table-Based QAM

8. Click **Exit** to close the window.

**Related Topics**

- Delete Sessions from a Table-Based QAM
- Upload Session Data to a Table-Based QAM

### Delete Sessions from a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Configure Session Data > [Select Sessions to be deleted] > Delete > OK**

This procedure describes either of the following ways to delete sessions from a table-based QAM:

- Individual sessions on a table-based QAM
- All sessions on a table-based QAM so that you can then upload new session data to the table-based QAM

Follow these steps to delete sessions from a table-based QAM.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM whose sessions you want to modify.
5. Click **Configure Session Data**. The Session Data window opens for the QAM you selected.
6. Select the sessions that you want to delete.

   **Tip:** To delete all sessions on this QAM, click the topmost selection box. Check marks appear in all selection boxes.

7. Click **Delete**. A confirmation message appears.
8. Click **OK**. The message closes and the Session Data window updates and shows that the selected sessions have been removed from the window.
9. Click **Exit** to close the window.

**Related Topics**

- Upload Session Data for a Table-Based QAM (Delete Sessions from a Table-Based QAM, Upload Session Data to a Table-Based QAM)

## Delete a Table-Based QAM

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Table-Based QAMs > [Select QAM] > Delete**

Follow these steps to delete a table-based QAM from the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **Table-Based QAMs**. The Table-Based QAMs List window displays any table-based QAMs that have already been added to the DNCS.
4. Select the table-based QAM you want to delete.
5. Click **Delete**. A confirmation window opens.
6. Click **OK**. The table-based QAM is removed from the list.
7. Do you want to delete additional table-based QAMs?
   - If **yes**, repeat steps 4 and 5 for each table-based QAM you want to delete.
   - If **no**, click **Exit**.

# PowerKEY Conditional Access

**Important:** Only sites that provide secure (encrypted) services to subscribers need to setup Conditional Access. If your site provides only clear (unencrypted) services, you do need to set up Conditional Access.

After you set up the two-way communication path for your network, if you are going to provide secure services, you must set up the PowerKEY Conditional Access (CA) system or enable the Open Conditional Access. This topic describes the PowerKEY CA system, the benefits it offers to cable operators, and how it works to protect secure services.

This topic does not provide step-by-step instructions for setting up the PowerKEY CA system. Refer to the Transaction Encryption Device FX Server Installation and Operation Guide (part number 736138) for that information.

## What do you want to do?

- Learn about conditional access
- Learn how conditional access works
- Set up PowerKEY conditional access

## What Is Conditional Access?

Conditional Access (CA) refers to the system, software, and components necessary to provide or deny subscribers selective access to specific services.

Because these services are available only to those subscribers who are authorized to receive them, you must encrypt these services to keep them secure from theft by unauthorized users. Consequently, these services are often called **secure** services. Our DNCS uses the PowerKEY CA system to provide secure services.

### Related Topics

- Benefits of PowerKEY CA
- How Conditional Access Works
- Set Up PowerKEY Conditional Access

## Benefits of PowerKEY CA

The PowerKEY CA system offers the following benefits to system operators:

- Enhanced encryption and decryption techniques to secure the transmission of sensitive applications, such as IPPV, Internet service, and VOD
- Increased number of secured services that can be offered to and purchased by subscribers
- Increased revenue due to the increased number of secured services offered for purchase

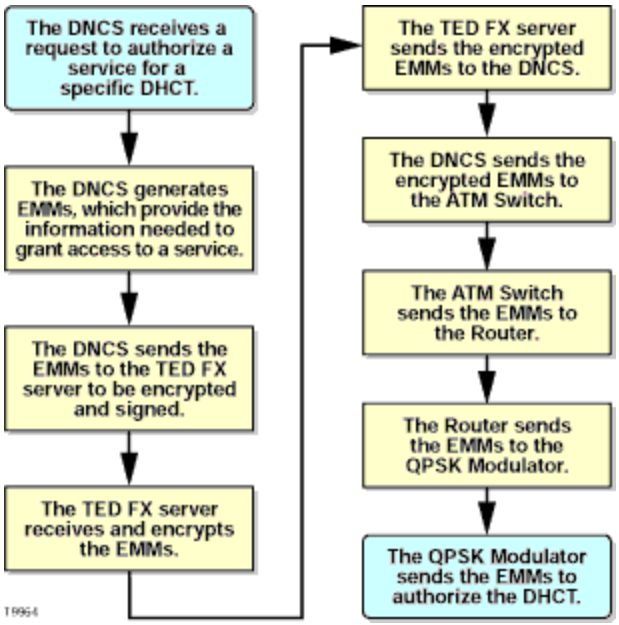
### Related Topics

- How Conditional Access Works
- Set Up PowerKEY Conditional Access
- What Is Conditional Access?

## How Conditional Access Works

The PowerKEY CA system uses either the Transaction Encryption Device (TED) server or the TED FX server. Both servers ensure that secure applications remain secure as they are transported throughout the DBDS. However, the TED FX server is able to encrypt more Entitlement Management Messages (EMMs) per second than the TED server.

The TED/TED FX server is connected directly to the DNCS using a short Ethernet connection. As shown in the following diagram, when the DNCS receives a request to authorize a service to a specific DHCT, the DNCS generates EMMs. EMMs contain information for a specific DHCT that enables that DHCT to access specific secure services.




After the DNCS generates the EMMs, it sends them to the TED/TED FX server to be encrypted. After the TED/TED FX server encrypts the EMMs, it sends the encrypted EMMs to the DNCS. The DNCS then sends the encrypted EMMs through the DBDS to the DHCT.

These encrypted EMMs enable DHCTs to decrypt premium broadcasts that have been encrypted to keep subscribers who have not purchased the broadcasts from accessing them. In other words, EMMs deliver the "keys" by which an authorized DHCT can access secure services.

For more information about the TED FX server and procedures for setting up the PowerKEY CA system, see the Transaction Encryption Device FX Server Installation and Operation Guide (part number 736138).

### Related Topics

- Set Up PowerKEY Conditional Access
- What Is Conditional Access?
- Benefits of PowerKEY CA

## Set Up PowerKEY Conditional Access

For specific instructions on installing the TED, installing the TED files, initializing the PowerKEY CA system, and supporting the TED server, refer to Transaction Encryption Device 3.0 Installation and Operation Guide (part number 4031371).

### Related Topics

- What Is Conditional Access?
- Benefits of PowerKEY CA
- How Conditional Access Works

# Stat Mux Dejitter Groups (SMDGs)

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

**Quick Path from GQAM: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [select GQAM] > Advanced Parameters tab > Stat Mux Dejitter Groups: Set up**

This topic describes how to use the Stat Mux Dejitter Groups window to set up stat mux dejitter groups (SMDGs) on GQAM modulators that receive multiplexed sources.

Setting up SMDGs enables a GQAM modulator to appropriately process multiplexed sources. Failing to set up SMDGs on GQAM modulators that receive multiplexed sources may result in tiling of the video on set-tops. SMDGs identify each GQAM input and output that will carry the multiplex and they also allow the modulator to appropriately process the multiplexed sources.

### Related Topics

- Set up stat mux dejitter groups
- Set up multicast sessions on GQAM SMDGs
- View stat mux dejitter group settings

## Stat Mux Dejitter Group Settings

Use the following fields when you manage SMDGs.

| Field | Description |
|---|---|
| ID | An identifier to indicate the SMDG. This must be a numerical value from 1 to 65535. |
| QAM Name | The QAM that carries this SMDG. |
| Bandwidth | The bandwidth that the modulator uses:<br>▪QAM-64<br>▪QAM-256 |
| Input Port | The input port that this SMDG uses. |
| Destination IP Address | The IP address of the receiving device, based on the following criteria:<br>▪If a GbE port receives the source, enter the IP multicast address for the GQAM modulator.<br>▪If an ASI port receives the source, do not enter data in this field.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Destination UDP Port | The UDP port of the receiving device, based on the following criteria:<br>▪If a GbE port receives the source, enter the UDP port on the GQAM modulator that receives the multiplexed source.<br>▪If an ASI port receives the source, do not enter data in this field. |
| Output Port | The output port that this SMDG uses. |

Related Topics

- Information Needed to Set up Stat Mux Dejitter Groups
- Set Up Stat Mux Dejitter Groups

## Set Up Stat Mux Dejitter Groups Overview

You can set up a maximum of 16 SMDGs on a GQAM modulator  one SMDG for each RF output port on the GQAM modulator. Each SMDG can accommodate a maximum of 60 sessions.

If you are using a GQAM modulator that receives sources from a statistical multiplexor (stat mux) and you have already added the GQAM modulator to the DNCS, you can set up SMDGs on the modulator. SMDGs identify each GQAM input and output that will carry the multiplex and they also allow the modulator to appropriately process the multiplexed sources. After setting up SMDGs on the GQAM modulator, you can set up sessions for groups to carry.

**Important:** Setting up an SMDG enables the GQAM modulator to appropriately process multiplexed sources. Failing to set up SMDGs on GQAM modulators that receive multiplexed sources may result in tiling of the video on DHCTs.

### Related Topics

- Information Needed to Set Up Stat Mux Dejitter Groups
- Set Up Stat Mux Dejitter Groups
- Stat Mux Dejitter Groups Settings

### Information Needed to Set Up Stat Mux Dejitter Groups

Before you begin, make certain that you have the following software installed on your system:

- GQAM software release 4.0 or later
- DNCS SR 2.7/3.7/4.2 SP2 or later

You will also need the following information:

- Your network map
- The input ports that receive the multiplexed source (ASI inputs, Ethernet inputs, or both)
- If a GbE port is used for multicasting, the destination multicast IP address (IP multicast address) for the GQAM modulator
- If a GbE port is used for unicasting, the destination UDP port number on the GQAM modulator that receives the source
- GQAM output port number that modulates the source onto the network

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Related Topics

- Set Up Stat Mux Dejitter Groups
- Stat Mux Dejitter Group Settings

### Setting Up Stat Mux Dejitter Groups

Complete these instructions to set up SMDGs by mapping the input port that receives the multiplexed source to the output port that modulates the source onto the network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. Click **GQAM**. The GQAM List window opens.
4. Select the GQAM modulator on which you want to set up an SMDG. Then select **File > Open**. The Set Up GQAM window opens with the Basic Parameters tab in the forefront.
5. Click the **Advanced Parameters** tab.
6. Click the **Set Up** button for Stat Mux Dejitter Groups. The Stat Mux Dejitter Groups window opens for the selected GQAM modulator.
7. Click **Add**. Empty fields appear at the top of the window.
8. Complete the fields on the screen as described in Stat Mux Dejitter Group Settings.

Use the following fields when you manage SMDGs.

| Field | Description |
|---|---|
| ID | An identifier to indicate the SMDG. This must be a numerical value from 1 to 65535. |
| QAM Name | The QAM that carries this SMDG. |
| Bandwidth | The bandwidth that the modulator uses:<br>▪ QAM-64<br>▪ QAM-256 |
| Input Port | The input port that this SMDG uses. |
| Destination IP Address | The IP address of the receiving device, based on the following criteria:<br>▪ If a GbE port receives the source, enter the IP multicast address for the GQAM modulator.<br>▪ If an ASI port receives the source, do not enter data in this field.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Destination UDP Port | The UDP port of the receiving device, based on the following criteria:<br>▪ If a GbE port receives the source, enter the UDP port on the GQAM modulator that receives the multiplexed source.<br>▪ If an ASI port receives the source, do not enter data in this field. |
| Output Port | The output port that this SMDG uses. |

Related Topics

- Information Needed to Set up Stat Mux Dejitter Groups
- Set Up Stat Mux Dejitter Groups

9. Click **Save**. Parameters for the SMDG are listed in the Stat Mux Dejitter Group window.

10. Do you need to add another SMDG to this GQAM modulator?

- If **yes**, repeat this procedure from step 7.
- If **no**, go to step 11.

11. Do you need to add SMDGs to another GQAM modulator?

- If **yes**, repeat this procedure from step 4.
- If **no**, you have successfully added SMDGs to the GQAM modulators that receive multiplexed sources and are ready to set up sessions for these SMDGs. For assistance setting up multicast sessions, see Set Up Multicast Sessions on a GQAM. For assistance setting up CF sessions, see Define a Digital Source and Session.

## Related Topics

- Content GQAM Modulator Settings
- Reset a Content GQAM
- Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

## Multicast Sessions

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > GQAM > Advanced Parameters tab > Multicast Sessions: Set up**

This section describes how to use the Multicast Digital Session Definition window to set up multicast sessions on a GQAM modulator and on any stat mux dejitter groups (SMDGs) that have been set up for a GQAM modulator:

- **GQAM modulator** - If you are using a GQAM modulator to send multicast sessions to the network and you already added a GQAM modulator to the DNCS and created a source for the session, you can follow the procedure in this topic to set up multicast sessions on the GQAM modulator.
- **GQAM SMDGs** - If you are using a GQAM modulator that receives input from a statistical multiplexor (stat mux) to send multicast sessions to the network and you already added SMDGs to the DNCS and created a source for the session, you can follow the procedure in this topic to set up multicast sessions on the GQAM SMDGs. You can set up a maximum of 60 sessions on an SMDG.

  **Important:** SMDG sessions must use the same input port and output port that the SMDG uses. Otherwise, the session may fail.

### Related Topics

- Multicast Session Settings - GQAM Modulator
- Information Needed for Multicast Sessions
- Set Up Multicast Sessions on a GQAM

### Multicast Session Settings - GQAM Modulator

Use the following fields when you manage multicast sessions on a GQAM modulator.

| Field | Description |
|---|---|
| Source ID | Source that the session will use. |
| Session ID | Left Session ID field.<br>Enter 12 zeros (**00:00:00:00:00:00**).<br>Right Session ID field.<br>The Source ID you used when you added the source to the DNCS. |
| Bandwidth | The maximum amount of bandwidth (in Mbps) that the system should allow for this device.<br>This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>▪Standard MPEG video streams use **2** or **3** Mbps.<br>▪HDTV streams use **13** Mbps.<br>▪Audio streams use **0.2** Mbps.<br>▪Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| Output Carrier | The output destination of the source. |
| Program Number | The MPEG program number being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Source IP Address 1 | The IP address of the first device. |
| Source IP Address 2 | The IP address of the second device (if used). |
| Source IP Address 3 | The IP address of the third device (if used). |
| Input Destination Multicast IP Address | The multicast IP address on the GQAM modulator where sources are input. |
| UDP Port | The port number on the modulator where the sources are input.<br>**Important:** If you are using GQAMs, and the multicast session is being set up as an SMDG session, the session's input port must match the input port of the SMDG. Otherwise, the session may fail. |

Related Topics

- Information Needed for Multicast Sessions
- Set Up Multicast Sessions on a GQAM
- Stat Mux Dejitter Groups

### Information Needed for Multicast Sessions

You need the following information to set up a multicast session on the GQAM modulator:

- Source ID as you defined it when you added the content source to the DNCS
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the content from the source (refer to your network map)
- MPEG program number (from your content service provider)
- IP addresses of source devices (up to 3 different source devices can be used)
- Input destination multicast ID address on the GQAM modulator
- Destination UDP port on the GQAM modulator

**Important:** To support multicast sessions, GQAM software version 4.0 or later must be installed on the GQAM modulator.

### Related Topics

- Multicast Session Settings
- Set Up Multicast Sessions on a GQAM

### Set Up Multicast Sessions on a GQAM

**Important:** To support multicast sessions, GQAM software version 4.0 or later must be installed on the GQAM modulator.

### Set Up Multicast Sessions on a GQAM

1. You should have already gathered the information needed to set up a multicast session.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List opens.
5. Select the GQAM modulator on which you want to set up a multicast session. Then choose the **File > Open**.
6. Click the **Advanced Parameters** tab.
7. Click **Multicast Sessions: Set up**. The Multicast Digital Session Definition window opens.
8. Click **Add**. The Multicast Digital Session for [GQAM name] window opens.
9. Complete the fields on the screen as described in Multicast Session Settings - GQAM Modulator.

Use the following fields when you manage multicast sessions on a GQAM modulator.

| Field | Description |
|---|---|
| Source ID | Source that the session will use. |
| Session ID | Left Session ID field.<br>Enter 12 zeros (**00:00:00:00:00:00**). |
| | Right Session ID field.<br>The Source ID you used when you added the source to the DNCS. |
| Bandwidth | The maximum amount of bandwidth (in Mbps) that the system should allow for this device.<br>This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>▪ Standard MPEG video streams use **2** or **3** Mbps.<br>▪ HDTV streams use **13** Mbps.<br>▪ Audio streams use **0.2** Mbps.<br>▪ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>▪ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| Output Carrier | The output destination of the source. |
| Program Number | The MPEG program number being fed into the transport stream.<br>This number must match the program number of the MPEG source as defined by your content provider. |
| Source IP Address 1 | The IP address of the first device. |
| Source IP Address 2 | The IP address of the second device (if used). |

| | |
|---|---|
| Source IP Address 3 | The IP address of the third device (if used). |
| Input Destination Multicast IP Address | The multicast IP address on the GQAM modulator where sources are input. |
| UDP Port | The port number on the modulator where the sources are input.<br><br>**Important:** If you are using GQAMs, and the multicast session is being set up as an SMDG session, the session's input port must match the input port of the SMDG. Otherwise, the session may fail. |

Related Topics

- Information Needed for Multicast Sessions
- Set Up Multicast Sessions on a GQAM
- Stat Mux Dejitter Groups

10. Click **Save**. The system saves the multicast session in the DNCS database and starts the session you built for it. The Multicast Digital Session Definition window updates to include the new session information.

11. Do you need to create another multicast session on this GQAM modulator?

- If **yes**, repeat this procedure from step 7 for each additional multicast session that this GQAM modulator will carry.
- If **no**, click **Exit** to close the Multicast Digital Session Definition window.

## Related Topics

- Multicast Sessions
- Encrypt a Service
- Register a Service
- Determine and Convert a Package EID
- Add a Service Package

# SONET

Synchronous optical network (SONET) is an industry standard for carrying many signals with different capacities over a fiber optics network. In a SONET ring topology, if a fiber cable is cut, the SONET add/drop multiplexers (ADMs) are intelligent enough to send the affected services over an alternate path. Service remains uninterrupted, so subscribers are never aware that a problem exists.

SONET rings also allow you to transport signals over longer distances than in traditional distribution networks. However, you must use SONET converters (interfaces) to move MPEG-2 data from the MPEG source (usually a BIG) through the ring to your DHCTs. You can connect SONET rings to other SONET rings, SONET rings to SONET interfaces, and SONET interfaces to SONET interfaces to extend the signal capability of your network.

## Process Overview

After you have installed the equipment that makes up the SONET ring, you must set up the ring and the interfaces in the DNCS so that the DNCS will process signals correctly through the ring. This is a three-step process in which you must complete the following tasks:

- Add the SONET ring
- Add the SONET interfaces
- Set up the connections between the SONET ring, the elements that are sending data to it, and the elements that are receiving data from it.

## Add a SONET Ring

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > File > New**

The first step in setting up SONET in the DNCS is to set up a SONET ring. A SONET ring is similar to a headend in that it represents a group of devices that send signals to a particular group of DHCTs. However, a SONET ring uses fiber optics instead of coaxial cable. Setting up a SONET ring in the DNCS simply tells the DNCS that you are using a SONET ring with a specific name somewhere in your network.

### Adding a SONET Ring to the DNCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click **File > New**. The Set Up SONET Network window opens with the Basic Parameters tab in the forefront.
5. Click in the **SONET Network Name** field and type the name you will use to identify this SONET ring (for example, **EastsideSONRng**). You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

6. Click **Save**. The system saves the SONET ring name in the DNCS database and closes the Set Up SONET Network window. The SONET Network List window updates to include the new SONET ring.
7. Add the new SONET ring to your network map.
8. Do you need to add another SONET ring?
   - If **yes**, go repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.
9. Your next step is to add the SONET interfaces that will transport the MPEG data through the SONET ring and ultimately to your DHCTs. Go to Add a SONET-to-ASI Interface.

## Add a SONET Ring

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > File > New**

The first step in setting up SONET in the DNCS is to set up a SONET ring. A SONET ring is similar to a headend in that it represents a group of devices that send signals to a particular group of DHCTs. However, a SONET ring uses fiber optics instead of coaxial cable. Setting up a SONET ring in the DNCS simply tells the DNCS that you are using a SONET ring with a specific name somewhere in your network.

### Adding a SONET Ring to the DNCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click **File > New**. The Set Up SONET Network window opens with the Basic Parameters tab in the forefront.
5. Click in the **SONET Network Name** field and type the name you will use to identify this SONET ring (for example, **EastsideSONRng**). You can use up to 15 alphanumeric characters.

   **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.

6. Click **Save**. The system saves the SONET ring name in the DNCS database and closes the Set Up SONET Network window. The SONET Network List window updates to include the new SONET ring.
7. Add the new SONET ring to your network map.
8. Do you need to add another SONET ring?
   - If **yes**, go repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.
9. Your next step is to add the SONET interfaces that will transport the MPEG data through the SONET ring and ultimately to your DHCTs. Go to Add a SONET-to-ASI Interface.

## SONET-to-ASI (STA) Interface Settings

Use the Set Up STA window on the DNCS Administrative Console to manage the SONET-to-ASI interfaces in your network. Two tabs in this window provide settings for the STA interface:

- Basic Parameters
- Connection Settings

### STA Interface Basic Parameter Settings

Use the following fields when you manage basic parameters for a SONET interface.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this STA interface. |
| STA Name | The name of the STA interface.<br>**Example: HE1_STA1**.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme on your network map. |
| IP Address | The IP address for the STA interface.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the STA interface. |
| Subnet Mask | The number identifying the subnet mask where this STA interface resides, based on the following criteria:<br>▪If your system uses a class B IP network configuration, type **255.255.0.0**.<br>▪If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Direction | Select the appropriate signal direction option, based on the following criteria:<br>▪If you are using this STA interface to convert SONET signals into ASI signals, click the **SONET to ASI** option.<br>▪If you are using this STA interface to convert ASI signals into SONET signals, click the **ASI to SONET** option. |

### Advanced Parameters

**CAUTION:** Do **NOT** change anything on the Advanced Parameters tab without first consulting Cisco Services.

### STA Interface Connection Settings

**Caution:** Do NOT change anything on the Advanced Parameters tab without first consulting Cisco Services.

Use the following fields when you manage connections for a SONET interface.

| Field | Description |
|---|---|
| Input Port | **Connect To** - The headend that contains the device that will send data to the STA interface. |
| | **Device Type** - The type of device sending data to the STA interface (for example, BIG, SONET ring, or another STA interface). |
| | **Device Name** - The name of the input device. |
| Output Port | **Headend Name** - The headend that contains the device receiving data from the STA interface. |
| | **Device Type** - The type of device receiving data from the STA interface (for example, MQAM modulator or another STA interface). |
| | **Device Name** - The name of the output device. |

The options that appear on this window depend on what you selected for the **Device Type**. As you finish completing this window, keep in mind that the information being requested is about the device that will be sending data **to** the STA interface.

## Add a SONET-to-ASI Interface

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > STA > File > New**

After you add a SONET ring to the DNCS, you must add the SONET interfaces to that ring. We use the SONET-to-ASI (STA) interface to move MPEG data through networks that use a SONET ring topology. This interface converts ASI data from an MPEG source (usually a BIG or an MDR) and converts it to SONET data.

The interface can also take SONET data and convert it into ASI data. For this reason, the interface is often called the STA (SONET-to-ASI) interface. For more information on our SONET interface, refer to the ASI-SONET Interface Model D9462 Installation and Operation Guide (part number 593500).

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- Name of the headend containing the STA interface
- Name used to identify the STA interface
- IP address for the STA interface (click here for the procedure to locate)
- MAC address for the STA interface (click here for the procedure to locate)
- Number for the subnet mask where the STA interface resides
- Name(s) of the headend(s) containing the devices that will be sending data to and receiving data from the STA interface
- Names of the devices that will be sending data to and receiving data from the STA interface
- Number identifying the output port on the device that will be sending data to the STA interface
- Number identifying the input port on the device that will be receiving data from the STA interface

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

**Caution:** The STA interface has a maximum throughput rate of 128 Mbps. Make sure you have configured the device that will be sending data to the STA interface in such a way that the MPEG input does not exceed 128 Mbps. Otherwise, there will be random data loss that results in macro-blocking on all programs carried by the SONET link.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add an STA interface to the DNCS, you must complete the following tasks. For step-by-step instructions for a particular task, click on that task.

- Set up the basic parameters for the STA interface.
- Set up the connections between the STA interface, the device sending data to the interface (input device), and the device receiving signals from the interface (output device).

### Setting Up Basic Parameters for an STA Interface

The first step in adding an STA interface is to complete these steps to set up the basic parameters for that interface.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **STA**. The STA List opens.
4. Click **File > New**. The Set Up STA window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in STA Interface Basic Parameter Settings.

Use the following fields when you manage basic parameters for a SONET interface.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this STA interface. |
| STA Name | The name of the STA interface.<br>**Example: HE1_STA1**.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme on your network map. |
| IP Address | The IP address for the STA interface.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the STA interface. |
| Subnet Mask | The number identifying the subnet mask where this STA interface resides, based on the following criteria:<br>▪ If your system uses a class B IP network configuration, type **255.255.0.0**.<br>▪ If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Direction | Select the appropriate signal direction option, based on the following criteria:<br>▪ If you are using this STA interface to convert SONET signals into ASI signals, click the **SONET to ASI** option.<br>▪ If you are using this STA interface to convert ASI signals into SONET signals, click the **ASI to SONET** option. |
| **Advanced Parameters** | |
| **CAUTION:** Do **NOT** change anything on the Advanced Parameters tab without first consulting Cisco Services. | |

6. Click **Apply**. The system saves the basic parameters for this STA interface in the DNCS database.

**Important:** Do NOT change anything on the Advanced Parameters tab without first consulting Cisco Services.

7.Your next step is to set up the connections between the STA interface, the input device, and the output device. Go to Setting Up Connections for an STA Interface.

### Setting Up Connections for an STA Interface

After you set up the basic parameters for an STA interface, complete these steps to set up the connections between the interface, the input device, and the output device.

**Caution:** Do **NOT** change anything on the Advanced Parameters tab without first consulting Cisco Services.

1. On the Set Up STA window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the STA interface and any devices already connected to it. (If no devices are yet connected, the illustration field will be empty.)

   **Note:** You might have to click the maximize button  in the upper-right corner of the window (or use the scroll bars) to see the whole window.

2. If not already selected, click the **Input Port** option.

3. Complete the fields on the screen as described in ▸ STA Interface Connection Settings.

   **Caution:** Do NOT change anything on the Advanced Parameters tab without first consulting Cisco Services.

   Use the following fields when you manage connections for a SONET interface.

| Field | Description |
|---|---|
| Input Port | **Connect To** - The headend that contains the device that will send data to the STA interface. |
| | **Device Type** - The type of device sending data to the STA interface (for example, BIG, SONET ring, or another STA interface). |
| | **Device Name** - The name of the input device. |
| Output Port | **Headend Name** - The headend that contains the device receiving data from the STA interface. |
| | **Device Type** - The type of device receiving data from the STA interface (for example, MQAM modulator or another STA interface). |
| | **Device Name** - The name of the output device. |
| The options that appear on this window depend on what you selected for the **Device Type**. As you finish completing this window, keep in mind that the information being requested is about the device that will be sending data **to** the STA interface. | |

4. Click **Apply**. The system saves the Connectivity parameters for the output port on the STA interface in the DNCS database and updates the illustration to include the output device.

5. Click **Save**. The system saves all of the STA interface information in the DNCS database and closes the Set Up STA window. The STA List window updates to include the new STA interface.

6. Add the new STA interface to your network map.

7. Do you need to add another STA interface?
   - If **yes**, go back to Setting Up Basic Parameters for an STA Interface.
   - If **no**, click **File > Close** to close the STA List window and return to the DNCS Administrative Console. Go to step 8.

8. Your next step is to set up the connections between the SONET ring, the elements that are sending

data to it, and the elements that are receiving data from it. Go to Set Up SONET Ring Connections.

## Set Up SONET Ring Connections

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > [SONET Network Name] > File > Open**

After you have added all of the SONET interfaces, you must set up the connections between the SONET ring, the elements that are sending data to it, and the elements that are receiving data from it.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- Numbers identifying the input ports on the SONET ring where it will be receiving data from the input device
- Numbers identifying the output ports on the SONET ring where it will be sending data to the output device
- Names of the input devices that will be sending data to the SONET ring
- Names of the output devices that will be receiving data from the SONET ring
- If this SONET ring will be receiving data from another SONET ring, the number identifying the output port on the other SONET ring
- If this SONET ring will be sending data to another SONET ring, the number identifying the input port on the other SONET ring

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

To set up SONET ring connections you must complete the following tasks.

1. Set up the input ports on the SONET ring.
2. Set up the output ports on the SONET ring.

### SONET Ring Connection Settings

Use the following topics to set up the port settings for your SONET ring:

- SONET Ring Input Port Settings
- SONET Ring Output Port Settings

### SONET Ring Input Port Settings

Use the following fields when you manage the SONET ring input ports.

| Field | Description |
|---|---|
| Input Port | Select the input port.<br>In the SONET Network Name area, click on the box to select an input port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the input port. |
| Create Port | Add an input port to the SONET ring.<br>Click **Create Port** to add an input port to the SONET ring, if it does not already exist. |
| Port Number | Identifies the input port on this SONET ring where it will receive data from the input device.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Input** option. |
| Device Type | The type of input device sending data to this SONET ring through the input port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the input device. |

The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will send data to this SONET ring.

### SONET Ring Output Port Settings

Use the following fields when you manage the SONET ring output ports.

| Field | Description |
|---|---|
| Output Port | Select the output port.<br>In the SONET Network Name area, click on the box to select an output port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the output port. |
| Create Port | Add an output port to the SONET ring.<br>Click **Create Port** to add an output port to the SONET ring, if the output port does not already exist. |
| Port Number | Identifies the output port on this SONET ring where it will send data to the output device.<br>Available only if you click **Create Port**.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Output** option. |
| Device Type | The type of output device receiving data from the SONET ring through the output port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the output device |

The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will receive data from this SONET ring.

### Setting Up SONET Ring Input Ports

The first step in setting up connections for a SONET ring is to complete these steps to set up the input ports on the SONET ring. Setting up the input ports establishes connectivity between the SONET ring and the network elements (input devices) that send data to it.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click once on the row containing the SONET ring whose connections you want to set up.
5. Click **File > Open**. The Set Up SONET Network window opens for the SONET ring you selected.
6. Click the **Connectivity** tab. The Connectivity window opens with an illustration of the SONET ring and any devices already connected to it. (If no devices are yet connected, only the SONET ring will appear in the illustration field.)

   **Note:** You might have to click the maximize button in the upper right corner of the window to be able to see all of the elements on the window.

7. Complete the fields on the screen as described in SONET Ring Input Port Settings.

   Use the following fields when you manage the SONET ring input ports.

| Field | Description |
|---|---|
| Input Port | Select the input port.<br>In the SONET Network Name area, click on the box to select an input port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the input port. |
| Create Port | Add an input port to the SONET ring.<br>Click **Create Port** to add an input port to the SONET ring, if it does not already exist. |
| Port Number | Identifies the input port on this SONET ring where it will receive data from the input device.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Input** option. |
| Device Type | The type of input device sending data to this SONET ring through the input port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the input device. |
| The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will send data to this SONET ring. | |

8. Click **Apply**. The system saves the Connectivity parameters for this input port in the DNCS database. The input port box that you checked changes color to green to show that the port is connected. The

illustration field updates to show the device to which that port is connected.

9. Do you need to set up any other input ports for this SONET ring?

- If **yes**, repeat this procedure from step 7.
- If **no**, your next step is to set up the output ports for this SONET ring. Go to Setting Up SONET Ring Output Ports.

### Setting Up SONET Ring Output Ports

After you set up the SONET ring input ports, complete these steps to set up the output ports on the SONET ring. Setting up the output ports establishes connectivity between the SONET ring and the network elements (output devices) that receive data from it.

1. On the **Connectivity** tab of the Set Up SONET Network window, is the output port that you need to set up already present in the Output Ports column?
   - If **yes**, go to step 5.
   - If **no**, click **Create Port**. The Port Number Prompt window opens.
2. Complete the fields on the screen as described in SONET Ring Output Port Settings.

Use the following fields when you manage the SONET ring output ports.

| Field | Description |
|---|---|
| Output Port | Select the output port.<br>In the SONET Network Name area, click on the box to select an output port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the output port. |
| Create Port | Add an output port to the SONET ring.<br>Click **Create Port** to add an output port to the SONET ring, if the output port does not already exist. |
| Port Number | Identifies the output port on this SONET ring where it will send data to the output device.<br>Available only if you click **Create Port**.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Output** option. |
| Device Type | The type of output device receiving data from the SONET ring through the output port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the output device |
| The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will receive data from this SONET ring. | |

3. Click **Apply**. The system saves the Connectivity parameters for this output port in the DNCS database. The input port box that you checked changes color to green to show that the port is connected. The illustration field updates to show the device to which that port is connected.
4. Do you need to set up any other output ports for this SONET ring?
   - If **yes**, repeat this procedure.
   - If **no**, click **Save**. The system saves all of the SONET ring information in the DNCS database, closes the Set Up SONET Network window, and returns you to the SONET Network List window.
5. Add the new SONET ring connection information to your network map.

6. Do you need to set up connections for another SONET ring?
   - If **yes**, go back to Set Up SONET Ring Connections.
   - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.
7. Are you setting up your network for the first time?
   - If **yes**, go to step 8.
   - If **no**, continue making any other changes that you need to make to your network.
8. Does your network comply with OpenCable standards?
   - If **yes**, go to Setting Up OpenCable Compliance.
   - If **no**, continue making any other changes that you need to make to your network.

## Locating an STA Interface IP Address

You can look at the sticker on the side of an STA interface to locate its IP address. Or, if the device is already in operation, you can complete these steps to use its front panel to locate the IP address.

1. Go to the front panel of the STA interface.
2. Press **OPTIONS** until you see **Main Menu** appear in the LCD.
3. Press the right or left arrow button until you see **Unit/Status** appear in the LCD.
4. Press **ENTER**.
5. Press the right or left arrow button until you see **IP Addr** appear in the LCD.
6. Press **OPTIONS** to return to the Main Menu.

## Locating an STA Interface MAC Address

You can look at the sticker on the side of an STA interface to locate its MAC address. Or, if the device is already in operation, you can complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the STA interface in question.
2. Press **OPTIONS** until you see **Main Menu** appear in the LCD.
3. Press the right or left arrow button until you see **Unit/Status** appear in the LCD.
4. Press **ENTER**.
5. Press the right or left arrow button until you see **MAC Addr** appear in the LCD.
6. Press **OPTIONS** to return to the Main Menu.

## Modify a SONET Ring

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > [SONET Ring Name] > File > Open**

After a SONET ring is saved in the DNCS, you can modify any of its parameters.

### Modifying a SONET Ring

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click once on the SONET ring you want to modify.
5. Click **File > Open**. The Set Up SONET Network window opens for the SONET ring you selected with the Basic Parameters tab in the forefront.
6. Make changes to the fields as described in SONET Ring Input Port Settings or SONET Ring Output Port Settings.

Use the following fields when you manage the SONET ring output ports.

| Field | Description |
|---|---|
| Output Port | Select the output port.<br>In the SONET Network Name area, click on the box to select an output port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the output port. |
| Create Port | Add an output port to the SONET ring.<br>Click **Create Port** to add an output port to the SONET ring, if the output port does not already exist. |
| Port Number | Identifies the output port on this SONET ring where it will send data to the output device.<br>Available only if you click **Create Port**.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Output** option. |
| Device Type | The type of output device receiving data from the SONET ring through the output port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the output device |
| The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will receive data from this SONET ring. | |

Use the following

fields when you manage the SONET ring input ports.

| Field | Description |
|---|---|
| Input Port | Select the input port.<br>In the SONET Network Name area, click on the box to select an input port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the input port. |
| Create Port | Add an input port to the SONET ring.<br>Click **Create Port** to add an input port to the SONET ring, if it does not already exist. |
| Port Number | Identifies the input port on this SONET ring where it will receive data from the input device.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Input** option. |
| Device Type | The type of input device sending data to this SONET ring through the input port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the input device. |
| The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will send data to this SONET ring. | |

7. When you finish making changes, click **Save**. The system saves the new SONET ring information in the DNCS database and closes the Set Up SONET Network window. If you changed the name of the SONET ring, the SONET Network List window updates to include the new name.
8. Update your network map to reflect these changes.
9. Do you need to modify another SONET ring?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.

## Modify a SONET Ring

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > [SONET Ring Name] > File > Open**

After a SONET ring is saved in the DNCS, you can modify any of its parameters.

### Modifying a SONET Ring

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click once on the SONET ring you want to modify.
5. Click **File > Open**. The Set Up SONET Network window opens for the SONET ring you selected with the Basic Parameters tab in the forefront.
6. Make changes to the fields as described in SONET Ring Input Port Settings or SONET Ring Output Port Settings.

Use the following fields when you manage the SONET ring output ports.

| Field | Description |
|---|---|
| Output Port | Select the output port.<br>In the SONET Network Name area, click on the box to select an output port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the output port. |
| Create Port | Add an output port to the SONET ring.<br>Click **Create Port** to add an output port to the SONET ring, if the output port does not already exist. |
| Port Number | Identifies the output port on this SONET ring where it will send data to the output device.<br>Available only if you click **Create Port**.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Output** option. |
| Device Type | The type of output device receiving data from the SONET ring through the output port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the output device |
| The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will receive data from this SONET ring. | |

Use the

following fields when you manage the SONET ring input ports.

| Field | Description |
|---|---|
| Input Port | Select the input port.<br>In the SONET Network Name area, click on the box to select an input port. A check mark appears in the box, and the box changes color to yellow.<br>**Important:** If the port you want to use is not in the list, you will need to create the input port. |
| Create Port | Add an input port to the SONET ring.<br>Click **Create Port** to add an input port to the SONET ring, if it does not already exist. |
| Port Number | Identifies the input port on this SONET ring where it will receive data from the input device.<br>You can use up to 5 numeric characters. |
| Port Type | Type of port on this SONET ring<br>Select the **Input** option. |
| Device Type | The type of input device sending data to this SONET ring through the input port you created.<br>**Example:** An STA interface or another SONET ring. |
| Device Name | The name of the input device. |
| The options that appear on this window are dependent on what you selected for the Device Type. As you finish completing this window, keep in mind that the information being requested is about the device that will send data to this SONET ring. | |

7. When you finish making changes, click **Save**. The system saves the new SONET ring information in the DNCS database and closes the Set Up SONET Network window. If you changed the name of the SONET ring, the SONET Network List window updates to include the new name.
8. Update your network map to reflect these changes.
9. Do you need to modify another SONET ring?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.

## Modify an STA Interface

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > STA > [STA Interface Name] > File > Open**

After an STA interface is saved in the DNCS, you can modify any of its parameters except for the headend to which it is assigned.

### Modifying an STA Interface

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **STA**. The STA List window opens.
4. Click once on the STA interface you want to modify.
5. Click **File > Open**. The Set Up STA window opens for the STA interface you selected with the Basic Parameters tab in the forefront.
6. Make changes to the fields as described in STA Interface Basic Parameter Settings and STA Interface Connection Settings.

**Caution:** Do NOT change anything on the Advanced Parameters tab without first consulting Cisco Services.

Use the following fields when you manage connections for a SONET interface.

| Field | Description |
|---|---|
| Input Port | **Connect To** - The headend that contains the device that will send data to the STA interface. |
| | **Device Type** - The type of device sending data to the STA interface (for example, BIG, SONET ring, or another STA interface). |
| | **Device Name** - The name of the input device. |
| Output Port | **Headend Name** - The headend that contains the device receiving data from the STA interface. |
| | **Device Type** - The type of device receiving data from the STA interface (for example, MQAM modulator or another STA interface). |
| | **Device Name** - The name of the output device. |
| The options that appear on this window depend on what you selected for the **Device Type**. As you finish completing this window, keep in mind that the information being requested is about the device that will be sending data **to** the STA interface. | |

Use the following fields when you manage basic parameters for a

SONET
interface.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this STA interface. |
| STA Name | The name of the STA interface.<br>**Example: HE1_STA1**.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme on your network map. |
| IP Address | The IP address for the STA interface.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the STA interface. |
| Subnet Mask | The number identifying the subnet mask where this STA interface resides, based on the following criteria:<br>▪ If your system uses a class B IP network configuration, type **255.255.0.0**.<br>▪ If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Direction | Select the appropriate signal direction option, based on the following criteria:<br>▪ If you are using this STA interface to convert SONET signals into ASI signals, click the **SONET to ASI** option.<br>▪ If you are using this STA interface to convert ASI signals into SONET signals, click the **ASI to SONET** option. |

### Advanced Parameters

**CAUTION:** Do **NOT** change anything on the Advanced Parameters tab without first consulting Cisco Services.

7. When you finish making changes, click **Save**. The system saves the new STA interface information in the DNCS database and closes the Set Up STA window. The STA List window updates to include the new STA interface information.

8. Update your network map to reflect these changes.

9. Do you need to modify another STA interface?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **File > Close** to close the STA List window and return to the DNCS Administrative Console.

## Modify an STA Interface

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > STA > [STA Interface Name] > File > Open**

After an STA interface is saved in the DNCS, you can modify any of its parameters except for the headend to which it is assigned.

### Modifying an STA Interface

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **STA**. The STA List window opens.
4. Click once on the STA interface you want to modify.
5. Click **File > Open**. The Set Up STA window opens for the STA interface you selected with the Basic Parameters tab in the forefront.
6. Make changes to the fields as described in STA Interface Basic Parameter Settings and STA Interface Connection Settings.

**Caution:** Do NOT change anything on the Advanced Parameters tab without first consulting Cisco Services.

Use the following fields when you manage connections for a SONET interface.

| Field | Description |
|---|---|
| Input Port | **Connect To** - The headend that contains the device that will send data to the STA interface. |
| | **Device Type** - The type of device sending data to the STA interface (for example, BIG, SONET ring, or another STA interface). |
| | **Device Name** - The name of the input device. |
| Output Port | **Headend Name** - The headend that contains the device receiving data from the STA interface. |
| | **Device Type** - The type of device receiving data from the STA interface (for example, MQAM modulator or another STA interface). |
| | **Device Name** - The name of the output device. |
| The options that appear on this window depend on what you selected for the **Device Type**. As you finish completing this window, keep in mind that the information being requested is about the device that will be sending data **to** the STA interface. | |

Use the following fields when you manage basic parameters

for a SONET interface.

| Field | Description |
|---|---|
| Headend Name | The headend associated with this STA interface. |
| STA Name | The name of the STA interface.<br>**Example: HE1_STA1**.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme on your network map. |
| IP Address | The IP address for the STA interface.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Physical Address | The MAC address for the STA interface. |
| Subnet Mask | The number identifying the subnet mask where this STA interface resides, based on the following criteria:<br>▪ If your system uses a class B IP network configuration, type **255.255.0.0**.<br>▪ If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator. |
| Direction | Select the appropriate signal direction option, based on the following criteria:<br>▪ If you are using this STA interface to convert SONET signals into ASI signals, click the **SONET to ASI** option.<br>▪ If you are using this STA interface to convert ASI signals into SONET signals, click the **ASI to SONET** option. |

### Advanced Parameters

**CAUTION:** Do **NOT** change anything on the Advanced Parameters tab without first consulting Cisco Services.

7. When you finish making changes, click **Save**. The system saves the new STA interface information in the DNCS database and closes the Set Up STA window. The STA List window updates to include the new STA interface information.
8. Update your network map to reflect these changes.
9. Do you need to modify another STA interface?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the STA List window and return to the DNCS Administrative Console.

## Delete a SONET Ring

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > [SONET Ring Name] > File > Delete**

Use this procedure to delete a SONET ring from the DNCS.

### Deleting a SONET Ring

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click once on the row containing the SONET ring you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the SONET ring information from the DNCS database and from the SONET Network List window.
7. Delete the SONET ring from your network map.
8. Do you need to delete another SONET ring?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.

## Delete a SONET Ring

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SONET > [SONET Ring Name] > File > Delete**

Use this procedure to delete a SONET ring from the DNCS.

### Deleting a SONET Ring

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **SONET**. The SONET Network List window opens.
4. Click once on the row containing the SONET ring you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the SONET ring information from the DNCS database and from the SONET Network List window.
7. Delete the SONET ring from your network map.
8. Do you need to delete another SONET ring?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the SONET Network List window and return to the DNCS Administrative Console.

## Delete an STA Interface

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > STA > [STA Interface Name] > File > Delete**

Use this procedure to delete an STA interface from the DNCS.

### Deleting an STA Interface

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **STA**. The STA List window opens.
4. Click once on the STA interface you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the STA interface information from the DNCS database and from the STA List window.
7. Delete the STA interface from your network map.
8. Do you need to delete another STA interface?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the STA List window and return to the DNCS Administrative Console.

## Delete an STA Interface

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > STA > [STA Interface Name] > File > Delete**

Use this procedure to delete an STA interface from the DNCS.

### Deleting an STA Interface

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **STA**. The STA List window opens.
4. Click once on the STA interface you want to delete.
5. Click **File > Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the STA interface information from the DNCS database and from the STA List window.
7. Delete the STA interface from your network map.
8. Do you need to delete another STA interface?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the STA List window and return to the DNCS Administrative Console.

# Two-Way Communication

If your system uses two-way communication, set up the two-way communication path for your network after you have set up the elements that process system data. In addition to sending information to DHCTs, the DNCS must be able to receive information from them. This is especially true if you provide PPV, VOD, or interactive services, which require a reverse data path. The QPSK modulator and the QPSK demodulator work together to provide this two-way communication over the out-of-band data path.

Using an out-of-band data path offers the following advantages:

- DHCTs can receive system data when they are tuned to an analog channel, so you can make system changes without interfering with the subscriber's viewing experience
- The volume of  data is reduced, so you have more space to provide programming
- A QPSK modulator can be connected to as many as eight demodulators. When a QPSK modulator and demodulator(s) are connected to each other, they are referred to collectively as a QPSK modem

**Note:** We offer a software product that you can purchase separately to enable the DNCS to also transport DOCSIS-compliant CMTS data. For more information about this software product, contact the representative who handles your account.

### You Need to Know

Before You Begin

Before you begin, you must have your network map.

Process Overview

To set up two-way communication, you must complete the following steps.

1. Add a QPSK modulator.
2. Add a QPSK demodulator.

## QPSK Modulator

A QPSK modulator processes data going downstream from the DNCS to the DHCTs, as well as data going upstream from the DHCTs to the DNCS.

For example, a QPSK modulator takes programming data for a PPV event from the DNCS, processes it onto an RF signal, and then sends it to the DHCTs. When a subscriber chooses to buy that event by using their remote control to send a signal to the DHCT, the DHCT passes that signal back to the DNCS, first through a QPSK demodulator, and then through a QPSK modulator.

For more information on QPSK modulators, refer to DAVIC QPSK Demodulator Model D9492 Installation and Operation Guide (part number 545617).

**Note:** We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data to DHCTs. For more information about this software product, contact the representative who handles your account.

## What do you want to do?

- Review QPSK modulator settings
- Add a QPSK modulator
- Modify a QPSK modulator
- Reset the QPSK modulator database
- Delete a QPSK modulator

### Information to Add a QPSK Modulator

You need the following information to add a QPSK modulator to the DNCS:

- IP address for the QPSK modulator
- MAC address for the QPSK modulator (click here for the procedure to locate)
- Subnet mask for the QPSK modulator
- IP address of the default router associated with the modulator
- Base IP address for all DHCTs within the domain of the modulator
- Subnet mask for all DHCTs within the domain of the modulator
- RF output frequency assigned to this modulator

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Locate a QPSK Modulator MAC Address

You can look at the sticker on the side of the QPSK modulator to locate its MAC address. Or, if the QPSK modulator is already in operation, you can complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the QPSK modulator.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

### QPSK Modulator Settings

Use the Set Up QPSK Modulator page on the DNCS Administrative Console to manage the QPSK modulators in your network. Two tabs in this window provide settings for the QAM:

- Basic Parameters settings: Use the settings on the Basic Parameters tab to configure key settings of the QPSK modulator.
- Advanced Parameters settings: Use the settings on the Advanced Parameters tab to to view the default setting for the QPSK modulator. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab.

### Basic Parameter Settings - QPSK Modulator

Use the following fields when you manage the basic parameters for a QPSK modulator.

| Field | Description |
|---|---|
| Hub Name | The hub associated with this content QPSK (if you have more than one defined). |
| Name | The name of this QPSK.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that allows you to easily identify the QPSK modulator and where it resides. |
| IP Address | The IP address for this QPSK.<br>Be careful to properly place the dots (.) between numbers. |
| Physical Address | The MAC address for the QPSK. |
| Subnet Mask | The subnet mask where this QPSK modulator resides. |
| Default Router | The IP address for the router associated with this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| DHCT Base IP Address | The base IP address for all DHCTs within the domain of this modulator. |
| DHCT Subnet Mask | The subnet mask for all DHCTs within the domain of this modulator. |
| Frequency | The RF output frequency assigned to this modulator.<br>This value can be from 70 MHz to 130 MHz in increments of 0.25 MHz. |
| DCM (DHCT Communications Mode) | Determines the DCM for the QPSK.<br>**Important:** Currently all DSG-capable DHCTs use a Mixed DOCSIS/DAVIC DCM. Unique code on Explorer 8300 DHCTs enables them to recognized a DCM of Mixed DOCSIS/DAVIC as DOCSIS. QPSK modulators that provide the BRF to hubs with Explorer 8300 DHCTs use a DCM of Mixed DOCSIS/DAVIC.<br>Select the appropriate DCM from one of the following choices:<br>▪**DAVIC** - Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel.<br>▪**Mixed DOCSIS/DAVIC** - Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel.<br>▪**DOCSIS** - Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.) |
| Options | **Continuous Wave Mode -** Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK. |

**Front Panel Lock -** Determines whether changes can be made from the front panel.

**Broadcast Only Mode -** Determines whether the QPSK sends priority broadcast transmissions.

**Database Persistence -** Determines whether the QPSK stores the IP addresses of DHCTs in RAM.

**Note:** Occasionally, you may need to clear the IP addresses that DHCTs are currently using and replace them with new IP addresses. To accomplish this, use the Reset and Clear DB selection on the QPSK File menu. For more information, see Reset the QPSK Modulator Persistent Database.

### Advanced Parameter Settings - QPSK Modulator

In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any advanced parameters after you have set up the basic parameters, keep in mind the following guidelines and contact Cisco Services if you need further assistance.

**Important:** If you change any of the default parameters, you must stay within the signal capacity of your plant design. Otherwise, the DHCTs might not be able to communicate with the DBDS. In addition, you must reboot the QPSK modulator and wait for all corresponding DHCTs to sign on again before any changes take effect.

| Field | Description |
|---|---|
| Configuration File Name | Do not change this parameter without first consulting Cisco Services. |
| Service Channel Frequency | Enter a value from 8 to 26.5 MHz based on your plant design.<br>This parameter establishes the frequency that the DHCTs use to broadcast to the demodulators on this hub. |
| Backup Service Channel Frequency | If you are **NOT** using a backup service channel, enter the same value in this field that you entered for the Service Channel Frequency parameter on the basic parameters tab. Otherwise, enter a value from 8 to 26.5 MHz based on your plant design.<br>**Important:** We recommend that you not use a backup service channel. The backup service channel is used when the service channel fails. All reverse channel messaging is sent over the channel on which the DHCT achieves initial sign-on. If a backup service channel is in use, the DHCT may not be able to achieve initial sign-on. |
| Tuner Input Attenuator | The DHCT calibration setting based on the design targets of your RF plant and the combining networks. If you need assistance, contact Cisco Services.<br>The system will not connect to any levels that are in the fail range. |

### Add a QPSK Modulator

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

### Process Overview

The first step in setting up the two-way communication path for your network is to add a QPSK modulator. To add a content modulator to the DNCS, complete the following tasks.

1. Set up the modulator's basic parameters.
2. Set up the modulator's advanced parameters.

**Note:** For a list of information needed to add the modulator to the DNCS, go to Information to Add a QPSK Modulator.

### Add a QPSK Modulator

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

### Process Overview

The first step in setting up the two-way communication path for your network is to add a QPSK modulator. To add a content modulator to the DNCS, complete the following tasks.

1. Set up the modulator's basic parameters.
2. Set up the modulator's advanced parameters.

**Note:** For a list of information needed to add the modulator to the DNCS, go to Information to Add a QPSK Modulator.

### Add Basic Parameters

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click **File > New > QPSK**. The Set Up QPSK Modulator window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameter Settings - QPSK Modulator.

Use the following fields when you manage the basic parameters for a QPSK modulator.

| Field | Description |
|---|---|
| Hub Name | The hub associated with this content QPSK (if you have more than one defined). |
| Name | The name of this QPSK.<br>You can use up to 15 alphanumeric characters. Be sure to use a name that allows you to easily identify the QPSK modulator and where it resides. |
| IP Address | The IP address for this QPSK.<br>Be careful to properly place the dots (.) between numbers. |
| Physical Address | The MAC address for the QPSK. |
| Subnet Mask | The subnet mask where this QPSK modulator resides. |
| Default Router | The IP address for the router associated with this modulator.<br>Be careful to properly place the dots (.) between numbers. |
| DHCT Base IP Address | The base IP address for all DHCTs within the domain of this modulator. |
| DHCT Subnet Mask | The subnet mask for all DHCTs within the domain of this modulator. |
| Frequency | The RF output frequency assigned to this modulator.<br>This value can be from 70 MHz to 130 MHz in increments of 0.25 MHz. |
| DCM (DHCT Communications Mode) | Determines the DCM for the QPSK.<br>**Important:** Currently all DSG-capable DHCTs use a Mixed DOCSIS/DAVIC DCM. Unique code on Explorer 8300 DHCTs enables them to recognized a DCM of Mixed DOCSIS/DAVIC as DOCSIS. QPSK modulators that provide the BRF to hubs with Explorer 8300 DHCTs use a DCM of Mixed DOCSIS/DAVIC.<br>Select the appropriate DCM from one of the following choices:<br>▪ **DAVIC** - Select if DHCTs receive all communications (out-of-band and unicast data) on a DAVIC channel.<br>▪ **Mixed DOCSIS/DAVIC** - Select if DHCTs receive out-of-band data on a DAVIC channel, and unicast communications on a DOCSIS channel. |

| | |
|---|---|
| | ▪ **DOCSIS** - Select if DHCTs receive out-of-band data and unicast data on a DOCSIS channel. (The DAVIC channel may be used for out-of-band data if the DOCSIS channel is impaired.) |
| Options | **Continuous Wave Mode -** Determines whether the QPSK produces an unmodulated RF carrier. This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QPSK's RF output port is muted. This is helpful when installing the QPSK. |
| | **Front Panel Lock -** Determines whether changes can be made from the front panel. |
| | **Broadcast Only Mode -** Determines whether the QPSK sends priority broadcast transmissions. |
| | **Database Persistence -** Determines whether the QPSK stores the IP addresses of DHCTs in RAM.<br>**Note:** Occasionally, you may need to clear the IP addresses that DHCTs are currently using and replace them with new IP addresses. To accomplish this, use the Reset and Clear DB selection on the QPSK File menu. For more information, see Reset the QPSK Modulator Persistent Database. |

6. To continue adding a QPSK modulator to the DNCS, set up the advanced parameters for the QPSK modulator. Go to Add Advanced Parameters.

### Add Advanced Parameters

Complete these steps to set up the QPSK modulator advanced parameters.

1. On the Set Up QPSK Modulator window, click the **Advanced Parameters** tab. The Advanced Parameters window opens.
2. In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any of these parameters, refer to the guidelines listed in Advanced Parameter Settings - QPSK Modulator.

   In general, the system sets up the QPSK modulator advanced parameters automatically, and you should not change them. However, if you need to change any advanced parameters after you have set up the basic parameters, keep in mind the following guidelines and contact Cisco Services if you need further assistance.

   **Important:** If you change any of the default parameters, you must stay within the signal capacity of your plant design. Otherwise, the DHCTs might not be able to communicate with the DBDS. In addition, you must reboot the QPSK modulator and wait for all corresponding DHCTs to sign on again before any changes take effect.

| Field | Description |
|---|---|
| Configuration File Name | Do not change this parameter without first consulting Cisco Services. |
| Service Channel Frequency | Enter a value from 8 to 26.5 MHz based on your plant design.<br>This parameter establishes the frequency that the DHCTs use to broadcast to the demodulators on this hub. |
| Backup Service Channel Frequency | If you are **NOT** using a backup service channel, enter the same value in this field that you entered for the Service Channel Frequency parameter on the basic parameters tab. Otherwise, enter a value from 8 to 26.5 MHz based on your plant design.<br>**Important:** We recommend that you not use a backup service channel. The backup service channel is used when the service channel fails. All reverse channel messaging is sent over the channel on which the DHCT achieves initial sign-on. If a backup service channel is in use, the DHCT may not be able to achieve initial sign-on. |
| Tuner Input Attenuator | The DHCT calibration setting based on the design targets of your RF plant and the combining networks. If you need assistance, contact Cisco Services.<br>The system will not connect to any levels that are in the fail range. |

3. Click **Save**. The system saves the advanced parameters for this modulator in the DNCS database and closes the Set Up QPSK Modulator window. The QPSK List window updates to include the new QPSK modulator.
4. Cick **File > Close** to close the QPSK List window and return to the DNCS Administrative Console.
5. Add the new QPSK modulator to your network map.

### Related Topics

- Add a QPSK Demodulator
- Register the BRF With the BFS Client - for assistance multicasting out-of-band data to Explorer 8300 DHCTs in support of DOCSIS
- Set Up PowerKEY Conditional Access - for assistance supporting secure services, such as PPV, VOD, or

Web applications

**Modify a QPSK Modulator**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Open**

After a QPSK modulator has been saved in the DNCS, you can modify any of its parameters, except for the hub to which it is assigned.

1. On the DNCS Administrative Console, click the DNCS tab.
2. Click the Network **Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator you want to modify.
5. Click **File > Open**. The Set Up QPSK Modulator window opens for the QPSK modulator you selected.
6. @ either of the following topics:
   - Basic Parameter Settings - QPSK Modulator
   - Advanced Parameter Settings - QPSK Modulator
7. When you finish making changes, click **Save**. The system saves the new QPSK modulator information in the DNCS database and closes the Set Up QPSK Modulator window. The QPSK/CMTS List window updates to include the new QPSK modulator information.
8. Update your network map to reflect these changes.
9. Click **File > Close** to close the QPSK/CMTS List window and return to the DNCS Administrative Console.

Related Topics

- Set Up Your Network
- Locate the MAC Address of a QPSK Modulator

## Reset the QPSK Modulator Persistent Database

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > Reset and Clear DB**

### Why Reset QPSK Modulator Persistent Database?

Under normal circumstances, persistent database records should not be cleared. Clearing these causes DHCTs to disconnect from the QPSK modulator. Until the DHCTs sign back on, a process that may take hours, subscribers will be unable to use interactive services, such as VOD.

There are, however, some situations when it is necessary to clear and reset the QPSK the database, for example, if you need to reallocate the IP addresses of DHCTs. In other situations, it can be helpful to clear and reset the QPSK database, for example, when moving some DHCTs from one QPSK modulator to another. This page describes how to use the Reset and Clear DB selection on the QPSK File menu to reset and clear the QPSK persistent database.

Selecting this menu option clears the persistent database records for all associated DHCT IP addresses. All package and billing information remains intact and the persistent database function is maintained for future QPSK modulator resets.

### You Need to Know

Performance Impact

During this process no DHCTs for the QPSK modulator are rebooted. As a result, you can perform this procedure at any time. However, interactive services will be unavailable to subscribers until the DHCTs on the corresponding QPSK sign back on, a process that can take from a few minutes to a few hours, depending on several factors. For this reason, you may prefer to clear the database records during a maintenance period.

### Resetting the QPSK Modulator Persistent Database

Follow this procedure to clear the persistent database records for all associated DHCT IP addresses.

1. Make sure that you are aware of how resetting database records can impact system performance.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
5. Select the QPSK modulator that you want to reset.
6. Click **File > Reset and Clear DB**. A confirmation window displays prompting you to confirm that you want to reset the QPSK modulator, associated demodulator, and clear the status of all DHCTs that the modulator feeds.
7. Click **Yes**. The persistent database records for this QPSK modulator are cleared and the persistent database function for future QPSK modulator resets is maintained.
8. Do you have additional modulators to reset?
    - If **yes**, repeat this procedure from step 4 as many times as is necessary to reset additional modulators.
    - If **no**, go to step 9.
9. Click **File > Close** to close the QPSK/CMTS List window.

## Why Reset QPSK Modulator Persistent Database?

Under normal circumstances, persistent database records should not be cleared. Clearing these causes DHCTs to disconnect from the QPSK modulator. Until the DHCTs sign back on, a process that may take hours, subscribers will be unable to use interactive services, such as VOD.

There are, however, some situations when it is necessary to clear and reset the QPSK the database, for example, if you need to reallocate the IP addresses of DHCTs. In other situations, it can be helpful to clear and reset the QPSK database, for example, when moving some DHCTs from one QPSK modulator to another. This page describes how to use the Reset and Clear DB selection on the QPSK File menu to reset and clear the QPSK persistent database.

Selecting this menu option clears the persistent database records for all associated DHCT IP addresses. All package and billing information remains intact and the persistent database function is maintained for future QPSK modulator resets.

## You Need to Know

Performance Impact

During this process no DHCTs for the QPSK modulator are rebooted. As a result, you can perform this procedure at any time. However, interactive services will be unavailable to subscribers until the DHCTs on the corresponding QPSK sign back on, a process that can take from a few minutes to a few hours, depending on several factors. For this reason, you may prefer to clear the database records during a maintenance period.

## Reset the QPSK Modulator Persistent Database

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > File > Reset and Clear DB**

### Why Reset QPSK Modulator Persistent Database?

Under normal circumstances, persistent database records should not be cleared. Clearing these causes DHCTs to disconnect from the QPSK modulator. Until the DHCTs sign back on, a process that may take hours, subscribers will be unable to use interactive services, such as VOD.

There are, however, some situations when it is necessary to clear and reset the QPSK the database, for example, if you need to reallocate the IP addresses of DHCTs. In other situations, it can be helpful to clear and reset the QPSK database, for example, when moving some DHCTs from one QPSK modulator to another. This page describes how to use the Reset and Clear DB selection on the QPSK File menu to reset and clear the QPSK persistent database.

Selecting this menu option clears the persistent database records for all associated DHCT IP addresses. All package and billing information remains intact and the persistent database function is maintained for future QPSK modulator resets.

### You Need to Know

Performance Impact

During this process no DHCTs for the QPSK modulator are rebooted. As a result, you can perform this procedure at any time. However, interactive services will be unavailable to subscribers until the DHCTs on the corresponding QPSK sign back on, a process that can take from a few minutes to a few hours, depending on several factors. For this reason, you may prefer to clear the database records during a maintenance period.

### Resetting the QPSK Modulator Persistent Database

Follow this procedure to clear the persistent database records for all associated DHCT IP addresses.

1. Make sure that you are aware of how resetting database records can impact system performance.
1. On the DNCS Administrative Console, click the **DNCS** tab.
1. Click the **Network Element Provisioning** tab.
1. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
1. Select the QPSK modulator that you want to reset.
1. Click **File > Reset and Clear DB**. A confirmation window displays prompting you to confirm that you want to reset the QPSK modulator, associated demodulator, and clear the status of all DHCTs that the modulator feeds.
1. Click **Yes**. The persistent database records for this QPSK modulator are cleared and the persistent database function for future QPSK modulator resets is maintained.
1. Do you have additional modulators to reset?
    - If **yes**, repeat this procedure from step 4 as many times as is necessary to reset additional modulators.
    - If **no**, go to step 9.
1. Click **File > Close** to close the QPSK/CMTS List window.

**Delete a QPSK Modulator**

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Delete**

Use this procedure to delete a QPSK modulator from the DNCS database.

**Important:** If there are any QPSK demodulators connected to a QPSK modulator when you delete the modulator, the system automatically deletes those demodulators from the DNCS database.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator you want to delete.
5. Click **File > Delete Bridge.** A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the QPSK modulator information from the DNCS database and from the QPSK/CMTS List window. If there were any QPSK demodulators connected to this QPSK modulator, the system deletes those demodulators from the DNCS database.
7. Delete the QPSK modulator from your network map.
8. Click **File > Close** to close the QPSK/CMTS List window and return to the DNCS Administrative Console.

## QPSK Demodulator

A QPSK demodulator performs data error correction, and then passes the ATM cells upstream to the QPSK modulator. The QPSK demodulator also monitors power levels and slot timing of incoming DHCT signals. You can assign up to eight QPSK demodulators to one QPSK modulator.

**Note:** We offer a software product that enables the DNCS to also transport DOCSIS-compliant CMTS data. For more information about this software product, contact the representative who handles your account.

## What do you want to do?

- Review QPSK demodulator settings
- Add a QPSK demodulator
- Modify a QPSK demodulator
- Delete a QPSK demodulator

### QPSK Demodulator Settings

Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br><br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br><br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your plant design.<br><br>**Important:** We recommend the following guidelines:<br><br>▪Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)<br><br>▪Set all demodulators associated with the same modulator to the same frequency. |

## Add a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select Modulator] > File > Demodulators > File > New Demod**

### Information to Add a QPSK Demodulator

Before you add a QPSK demodulator to a QPSK modulator, you need the following information:

- Name of the modulator physically connected to this demodulator
- Port number where this demodulator is physically connected to the modulator
- Name of the node set you want to associate with this demodulator

**Important:** We recommend that you assign each demodulator to a unique node set.

- RF input frequency assigned to this demodulator

**Important:** We recommend the following:

- That you set this value to equal the service channel frequency of the associated modulator.
- That you set all demodulators associated with the same modulator to the same frequency.

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Process Overview

After you have added a QPSK modulator to the DNCS database, add all QPSK demodulators that are connected to that modulator. To add a QPSK demodulator to a QPSK modulator, follow this process.

1. If you have not already done so, add a node set for the demodulator. A node set represents the point where a group of reverse signals generated from DHCTs are combined and fed into a single QPSK demodulator.
2. Add a QPSK demodulator to a QPSK modulator by assigning each demodulator to the port number on the modulator that matches the actual physical connections between the modulator and demodulator.

   **Important:** We recommend that you set all demodulators associated with the same modulator to the same frequency.

**Note:** For a list of information needed to add the demodulator to the DNCS, go to Information to Add a QPSK Demodulator.

### Information to Add a QPSK Demodulator

Before you add a QPSK demodulator to a QPSK modulator, you need the following information:

- Name of the modulator physically connected to this demodulator
- Port number where this demodulator is physically connected to the modulator
- Name of the node set you want to associate with this demodulator

**Important:** We recommend that you assign each demodulator to a unique node set.

- RF input frequency assigned to this demodulator

**Important:** We recommend the following:

- That you set this value to equal the service channel frequency of the associated modulator.
- That you set all demodulators associated with the same modulator to the same frequency.

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Add a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Select Modulator] > File > Demodulators > File > New Demod**

### Information to Add a QPSK Demodulator

Before you add a QPSK demodulator to a QPSK modulator, you need the following information:

- Name of the modulator physically connected to this demodulator
- Port number where this demodulator is physically connected to the modulator
- Name of the node set you want to associate with this demodulator

**Important:** We recommend that you assign each demodulator to a unique node set.

- RF input frequency assigned to this demodulator

**Important:** We recommend the following:

- That you set this value to equal the service channel frequency of the associated modulator.
- That you set all demodulators associated with the same modulator to the same frequency.

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

### Process Overview

After you have added a QPSK modulator to the DNCS database, add all QPSK demodulators that are connected to that modulator. To add a QPSK demodulator to a QPSK modulator, follow this process.

1. If you have not already done so, add a node set for the demodulator. A node set represents the point where a group of reverse signals generated from DHCTs are combined and fed into a single QPSK demodulator.
1. Add a QPSK demodulator to a QPSK modulator by assigning each demodulator to the port number on the modulator that matches the actual physical connections between the modulator and demodulator.

   **Important:** We recommend that you set all demodulators associated with the same modulator to the same frequency.

**Note:** For a list of information needed to add the demodulator to the DNCS, go to Information to Add a QPSK Demodulator.

### Adding a QPSK Demodulator

**Important:** Be very careful when you add a QPSK demodulator to the DNCS. Incorrectly configuring demodulators causes large numbers of DHCTs to be classified as non-responding units. In addition, the network management system will falsely log errors originating from incorrectly configured QPSK demodulators.

After you add a QPSK modulator to the DNCS, complete these steps to add all QPSK demodulators that are connected to that modulator.

1. Does a node set exist for this demodulator.
   - If **yes**, go to step 2.
   - If **no**, add a node set and then go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
5. Select the modulator to which you need to assign this demodulator.
6. Click **File > Demodulators**. The QPSK Modem window opens with an illustration of the modulator and its eight possible port connections.
7. Click **File > New Demod**. The Set Up QPSK Demodulator window opens.
8. Complete the fields on the screen as described in QPSK Demodulator Settings.

Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your plant design.<br>**Important:** We recommend the following guidelines:<br>▪ Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)<br>▪ Set all demodulators associated with the same modulator to the same frequency. |

9. Check the associated modulator service channel frequency (on the Advanced Parameters tab of the QPSK modulator window). The QPSK modulator's service channel frequency must match the frequency

of at least one of the associated demodulators. If at least one of the demodulator's frequencies does not match the service channel frequency of the associated modulator, change the frequency of one of the demodulators accordingly. For assistance changing the frequency, go to Modify a QPSK Demodulator.

10. Click **Save**.
    - The system saves the demodulator information in the DNCS database and closes the Set Up QPSK Demodulator window.
    - Then, the QPSK Modem window opens with the new demodulator appearing in the illustration.
    - An information window opens.
11. Click **OK** to close the information window.
12. Add the new QPSK demodulator to your network map.

### Modify a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator] > File > Open Demod**

After a QPSK demodulator has been saved in the DNCS, you can modify only the node set and RF output frequency assigned to that demodulator. To change any other parameters, you must delete the QPSK demodulator and then re-add it to the DNCS, using the new information.

**Important:** We recommend that you assign each demodulator to a unique node set. In addition, set all demodulators associated with the same modulator to the same frequency as the service channel for that modulator.

### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

### Modifying a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to modify.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the picture of the demodulator you want to modify, and then click **File > Open Demod**. The Set Up QPSK Demodulator window opens for the demodulator you selected.

   **Note:** You could also open this window by clicking the right mouse button on the demodulator picture on the QPSK Modem window, and then selecting **Open** from the menu that appears.

7. Make changes to the fields as described in QPSK Demodulator Settings.

   Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br><br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br><br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your |

plant design.

**Important:** We recommend the following guidelines:

- Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)
- Set all demodulators associated with the same modulator to the same frequency.

8. When you finish making changes, click **Save**. The system saves the demodulator information in the DNCS database. The Set Up QPSK Demodulator window closes. The QPSK Modem window opens with the new demodulator appearing in the illustration. An information window opens and directs you to check the associated modulator service channel frequency. The service channel frequency must match the frequency of at least one of the associated demodulators.

9. Click **OK** to close the information window.

10. Update your network map to reflect these changes.

### Modify a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator] > File > Open Demod**

After a QPSK demodulator has been saved in the DNCS, you can modify only the node set and RF output frequency assigned to that demodulator. To change any other parameters, you must delete the QPSK demodulator and then re-add it to the DNCS, using the new information.

**Important:** We recommend that you assign each demodulator to a unique node set. In addition, set all demodulators associated with the same modulator to the same frequency as the service channel for that modulator.

### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

### Modifying a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to modify.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the picture of the demodulator you want to modify, and then click **File > Open Demod**. The Set Up QPSK Demodulator window opens for the demodulator you selected.

   **Note:** You could also open this window by clicking the right mouse button on the demodulator picture on the QPSK Modem window, and then selecting **Open** from the menu that appears.

7. Make changes to the fields as described in QPSK Demodulator Settings.

   Use the following fields when you manage a QPSK demodulator in the DNCS.

| Field | Description |
|---|---|
| Port | The port on the QPSK modulator from which this demodulator receives data.<br><br>**Note:** This field is not editable. The only time you can change this field is when creating a QPSK demodulator. |
| Node Set Name | The node set that you want to associate with this demodulator.<br><br>**Important:** We recommend that you assign each demodulator to a unique node set. |
| Frequency | The RF input frequency assigned to this modulator. You can enter a value from 8 to 26.5 MHz, based on your |

plant design.

**Important:** We recommend the following guidelines:

- Set this value to equal the service channel frequency of the associated modulator. (The service channel frequency of the QPSK modulator is shown in the Advanced Parameters tab of the Set Up QPSK modulator window.)
- Set all demodulators associated with the same modulator to the same frequency.

8. When you finish making changes, click **Save**. The system saves the demodulator information in the DNCS database. The Set Up QPSK Demodulator window closes. The QPSK Modem window opens with the new demodulator appearing in the illustration. An information window opens and directs you to check the associated modulator service channel frequency. The service channel frequency must match the frequency of at least one of the associated demodulators.

9. Click **OK** to close the information window.

10. Update your network map to reflect these changes.

### Delete a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator Name] > File > Delete Demod**

Use this procedure to delete a QPSK demodulator from the DNCS.

#### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

#### Deleting a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to delete.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the demodulator you want to delete, and then click **File > Delete Demod**. A confirmation window opens.

   **Note:** You could also click the right mouse button on the demodulator picture, and then select **Delete** from the menu that appears.

7. Click **Yes**. The confirmation window closes. The system removes the QPSK demodulator information from the DNCS database and from the QPSK Modem window.
8. Remove the QPSK demodulator from your network map.

### Delete a QPSK Demodulator

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS > [Modulator Name] > File > Demodulators > [Demodulator Name] > File > Delete Demod**

Use this procedure to delete a QPSK demodulator from the DNCS.

#### You Need to Know

Before You Begin

Before you begin, you must know which QPSK modulator is associated with the QPSK demodulator you want to modify. In addition, you must have your network map available.

#### Deleting a QPSK Demodulator

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS**. The QPSK/CMTS List window opens.
4. Click once on the row containing the QPSK modulator associated with the demodulator you want to delete.
5. Click **File > Demodulators**. The QPSK Modem window opens for the QPSK modulator you selected. This window shows the demodulator(s) associated with this QPSK modulator.
6. Click on the demodulator you want to delete, and then click **File > Delete Demod**. A confirmation window opens.

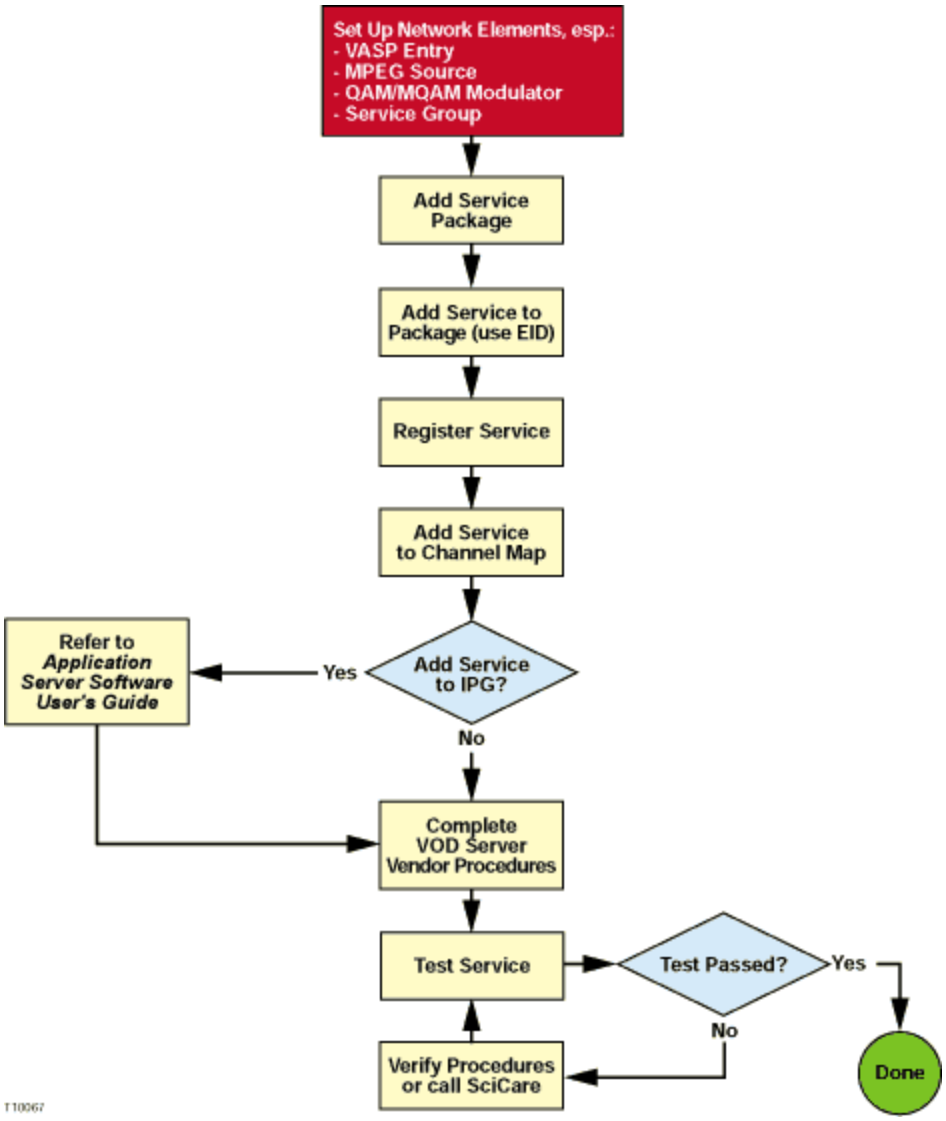
   **Note:** You could also click the right mouse button on the demodulator picture, and then select **Delete** from the menu that appears.

7. Click **Yes**. The confirmation window closes. The system removes the QPSK demodulator information from the DNCS database and from the QPSK Modem window.
8. Remove the QPSK demodulator from your network map.

# Video-On-Demand (VOD)

## Setting Up VOD Services Flow Diagram

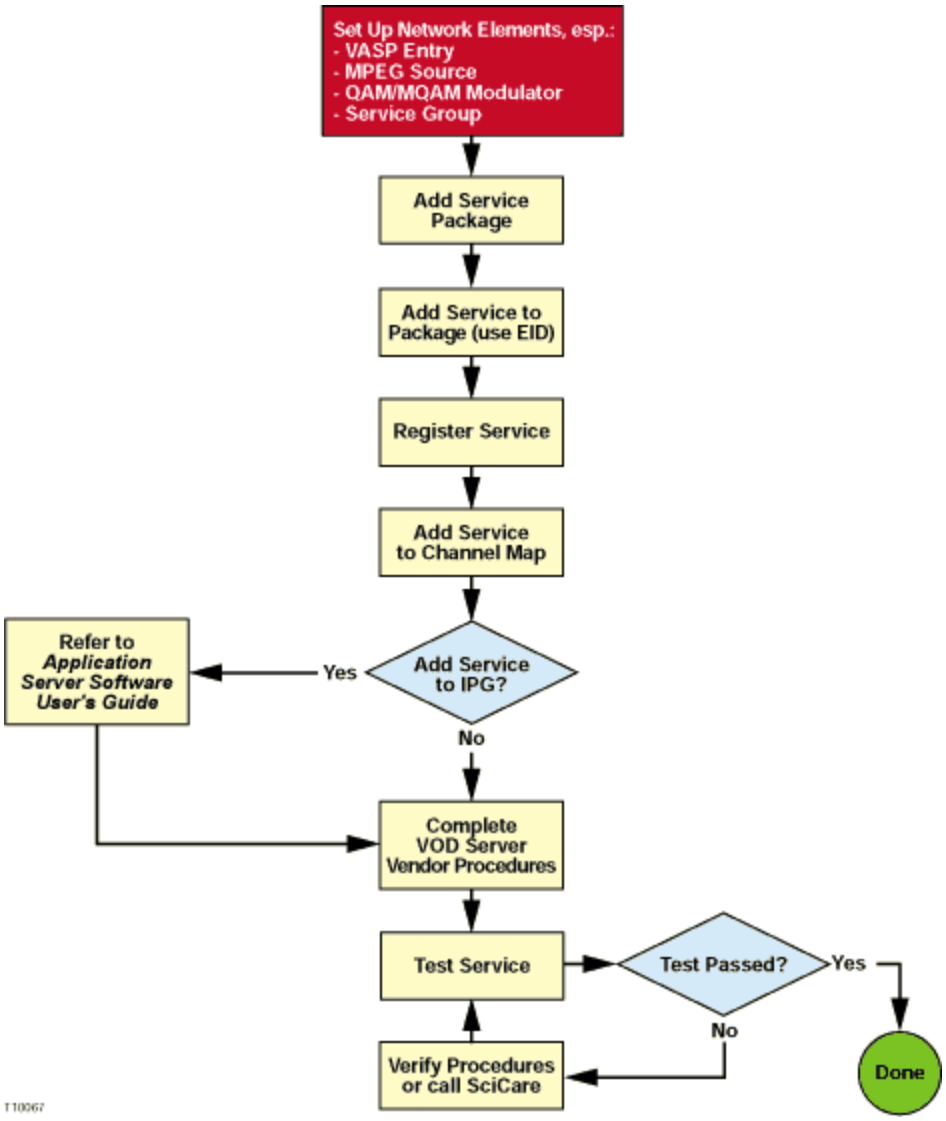
The following diagram illustrates the process of setting up a VOD service.



# Video-On-Demand (VOD)

## Setting Up VOD Services Flow Diagram

The following diagram illustrates the process of setting up a VOD service.



## Types of Service Groups

A service group is a set of QAM, MQAM, or GQAM modulator channels that provide narrowcast services, most frequently VOD services, to a unique group of DHCTs. Service groups enable a VOD server to determine which VOD QAM modulator resources a DHCT can access.

You can add the following types of service groups to the DNCS:

- Parent service groups, which contain one or more child service groups
- **Child service groups**, which belong to a parent service group
- **Standalone service groups**, which are independent: they contain no child service groups nor do they belong to a parent service group

Allowing one service group to belong to another enables you to more effectively manage the different types of content that your VOD server provides.

Related Topics

- Why Use Different Types of Service Groups?
- Service Groups for VOD Services
- Add a Service Group

### Why Use Different Types of Service Groups?

Your ability to better manage content increases when using parent and child service groups because you can share the VOD QAM channels of a parent service group with those of its children. Sharing QAM channels gives you the ability to provide services without consuming a large portion of the available RF spectrum.

For example, because child service groups have access to all of the QAM modulator channels of their parent, a parent service group typically provides content that is infrequently accessed, such as classic films or documentaries. Low demand for this type of content means that it can be made available to a larger group of DHCTs (those fed by a child and its parent) without impacting the ability of subscribers to access the content. However, content that is in high demand, such as recent movie releases, is typically provided by child service groups. Child service groups better serve this purpose because they feed a smaller number of DHCTs than parent service groups.

**Note:** VOD providers often refer to low-demand content as "library content."

### Related Topics

- Types of Service Groups
- Service Groups for VOD Services
- Add a Service Group
- Modify a Service Group
- Delete a Service Group

### Service Groups for VOD Services

If you are going to provide VOD services, add a service group for each unique group of VOD QAM modulators. To provide low-demand (library) content, identify this service group as a parent service group and then add child service groups, which provide high-demand content, to the parent service group. If you do not want to manage content by distinguishing between content types, simply add a service group and do not identify it as a parent service group. (Standalone service groups contain no child service groups nor do they belong to parent service groups.)

### Related Topics

- Types of Service Groups
- Why Use Different Types of Service Groups
- Add a Service Group
- Modify a Service Group
- Delete a Service Group

## Service Group Settings

The following settings allow you to manage the service groups in your network:

- Add Service Group Settings
- Edit Service Group Settings

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

### Add Service Group Settings

Use the Add Service Group window on the DNCS Administrative Console to add service groups to the DNCS.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and that processes VOD data for Hub 1. |
| Parent Group | Allows this service group to function as a parent service group.<br><br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Groups/Selected Groups | Determines the child groups associated with this parent group. Select groups from this list only when adding a parent service group to the DNCS.<br><br>To add a child to this parent service group, select a service group in the Available Group list and click **Add**.<br><br>The selected service group moves from the Available Groups list to the Selected Groups list.<br><br>**Notes:**<br><br>▪If you make a mistake, you can remove ports from the Selected Groups list by clicking on the name of the group you want to remove in the Selected Groups list, and then clicking **Remove**. The selected group moves from the Selected Groups list into the Available Groups list.<br><br>▪These lists display only when you select the **Parent Group** setting. For more information on parent service groups, see Types of Service Groups. |
| Available Ports/Selected Ports | Determines the ports associated with the service group.<br><br>Select the port of the QAM, MQAM, or GQAM modulator that will provide VOD data for this service group and click **Add**.<br><br>The selected port moves from the Available Ports list into the Selected Ports list.<br><br>Repeat for each QAM, MQAM, or GQAM modulator that will provide VOD data for this service group.<br><br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

**Related Topics**

- Service Groups
- Edit Service Group Settings

### Edit Service Group Settings

Use the Edit Service Group window on the DNCS Administrative Console to modify the settings of a service groups.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| Service Group ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Service Group Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and that processes VOD data for Hub 1. |
| Parent ID | A 0 in this field indicates that this is a parent or standalone service group.<br><br>If this is a child service group, you can change it to a parent or standalone service group, by entering a 0 in this field.<br><br>If this is a child service group, you can change the Parent ID and make this service group the child of another parent service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable.<br><br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Children | If this is a parent service group, the child groups associated with this parent group are listed here. |
| Parent Group | Allows this service group to function as a parent service group.<br><br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Ports/Selected Ports | For a parent, standalone, or child service group, you can change the RF ports that the service group uses by adding or removing RF ports:<br><br>▪To add RF ports to the service group, select a port in the **Available Ports** and click **Add**. The selected port moves from the Available Ports list to the Selected Ports list.<br><br>▪To remove RF ports from the service group, select a port in the **Selected Ports** list and click **Remove**. The selected port moves from the Selected Ports list to the Available Ports list.<br><br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in |

| | |
|---|---|
| | the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

## Related Topics

- Service Groups
- Add Service Group Settings

### Session Signaling Parameter Settings

The following table describes each field in the DSM-CC tab and provides the range of values that we recommend.

| Field | Description |
|---|---|
| **DHCT Session Signaling Parameters** | |
| Send 'Session in Progress' Every | Enter a time (in minutes) that defines how often a DHCT tells the DNCS that a VOD event is in progress. The Session in Progress (SIP) message prevents the system from tearing down sessions while a DHCT receives an event.<br>**Warning:** A reduction in VOD performance may occur when a large number of SIP messages are generated at the same time.<br>We recommend that you generate SIP messages at least every 120 minutes, but no more than 180 minutes. |
| Retry Requests Up To | How many times a DHCT should send a session request to the DNCS .<br>We recommend that you set this value to **1** for one, but no more than 2 retries.<br>Setting this value to two or more times results in subscribers having to wait longer for a response. In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For Network Response After | How long (in seconds) a DHCT should wait for confirmation that the DNCS is processing the session request<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| **Network Session Signal Parameters** | |
| Send 'Setup Proceeding' Every | How long (in seconds) a DHCT must wait to receive confirmation from the DNCS that it is processing the session request that the DHCT sent.<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| Retry Requests Up To | How many times the DNCS should request tuning information from the VOD server for a particular event.<br>We recommend that you set this value to be equal to or greater than the **Retry Requests Up To** parameter for DHCTs.<br>Setting this value to two or more times results in subscribers having to wait longer for a response.<br>In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For User Response After | How long (in seconds) the DNCS should wait for the VOD server to respond after the tuning information is requested.<br>We strongly recommend that you set this parameter to be greater than the **Stop Waiting For Network Response After** parameter for DHCTs. Doing so ensures that a DHCT initiates the teardown of a session before the DNCS does. |
| Highest Program Bandwidth | The maximum allowable bandwidth for VOD sessions. |
| Reuse Expired | How long (in seconds) the system must wait to reuse a session ID after the ID has |

| | |
|---|---|
| Session IDs After | expired<br><br>We recommend that you set this value to at least **3**, but no longer than **5** seconds. |

## Service Group Filter

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

From the Filter area on the Service Group Data window, you can quickly retrieve information about the service groups in your system. The Filter allows you to select service group attributes, such as a service group name, and find the service groups in your system that meet your search criteria.

## What do you want to do?

- Learn about service group filter settings
- Use the Filter to search and display the service groups in your system
- Learn about the data that the filter displays

### Service Group Filter Settings

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

This section describes service group Filter options and provides examples to show how the Filter searches for service groups based on your selections.

**Notes:**

- To learn more about service group data the Filter displays in the Service Group Data window, see Service Group Data.
- To learn how to use the Filter to search for and display certain service groups, see Use the Filter to Display Service Group Data.

### Service Group Filter Options

The following table describes the Filter options for searching service groups.

| By Field | By Value | Examples |
|---|---|---|
| **ID** | Enter the service group ID in the By Value field to have the filter display service group data for the ID you entered.<br><br>Important: The filter searches for the service group with an ID that exactly matches the number you enter in the By Value field. | If you enter **38** in the By Value field, the Filter finds and displays only the service group with an ID of 38. The Filter would not search for service groups whose IDs contain the number 38.<br><br>For example, service groups with IDs of 3855 or 138 would not be found. |
| **Name** | Enter any part of a service group name in the By Value field to have the filter display service groups whose names match any portion of the text entered in this field.<br><br>**Important:** This field is case-sensitive and accepts letters and numbers. | If you enter **Se** in the By Value field, the Filter finds and displays service groups with any of the following names:<br><br>▪All**Se**rvice<br>▪LaGrange **Se**rvice Group<br>▪**Se**rvice Group 10 |
| **Parent ID** | Enter the Parent ID of the service group whose data you want in the By Value field to have the filter display parent service groups with IDs that match any portion of the text entered in this field.<br><br>**Important:** The filter searches for the service group with a Parent ID that exactly matches the number you enter in the By Value field. | If you enter **38** in the By Value field, the Filter finds and displays only the service group with a Parent ID of 38. The Filter would not search for service groups whose Parent ID contain the number 38.<br><br>For example, service groups with Parent IDs of 3855 or 138 would not be found. |

### Use the Filter to Display Service Group Data

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

This section provides instructions for using the Filter to search and display the service groups in your system.

### Before You Begin

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following service group parameters:

- Service group ID
- Service group name
- Parent ID

### Display Service Group Data

1. Click the **By Field** arrow and select one of the following options:
   - ID
   - Name
   - Parent ID

   **Note:** For a description of these options, see Service Group Filter Settings.

2. Click in the **By Value** field and enter data in this field.

   **Note:** For examples of how By Value data affects searches, see Service Group Filter Settings.

3. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Service Group Data window.

   **Notes:**

   - For information about the data displayed in the Service Group Data window, see Service Group Data.
   - You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: ID, Parent ID, Name. Clicking the same heading again displays the column in descending order.

**Before You Begin**

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following service group parameters:

- Service group ID
- Service group name
- Parent ID

### Use the Filter to Display Service Group Data

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

This section provides instructions for using the Filter to search and display the service groups in your system.

### Before You Begin

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following service group parameters:

- Service group ID
- Service group name
- Parent ID

### Display Service Group Data

1. Click the **By Field** arrow and select one of the following options:
   - ID
   - Name
   - Parent ID

**Note:** For a description of these options, see Service Group Filter Settings.

1. Click in the **By Value** field and enter data in this field.

**Note:** For examples of how By Value data affects searches, see Service Group Filter Settings.

1. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Service Group Data window.

**Notes:**

- For information about the data displayed in the Service Group Data window, see Service Group Data.
- You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: ID, Parent ID, Name. Clicking the same heading again displays the column in descending order.

### Service Group Data

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

When you use the Filter to search for and display service groups, search results are shown in the Service Group Data window, which lists the following information:

| Field | Description |
|---|---|
| Service Group ID | Shows the unique numerical identifier for the service group. This field accepts up to 10 digits.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Service Group Name | Shows the name used to identify this service group.<br><br>You can use numbers and letters. We recommend that you establish a naming scheme that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example**: A name of VOD_SG_Hub1_MQ43 could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and that processes VOD data for Hub 1. |
| Groups: Available and Selected | Shows the groups that can be assigned to the parent service group. |
| Ports: Available and Selected | Shows the ports of the QAM, MQAM, or GQAM modulators that will provide VOD data for the service group. |

## Add a Service Group

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

These instructions describe how to add a service group to the DNCS.

**Note:** For more information about service groups, see Types of Service Groups.

**Important:** If you are using Overlay technology, remember that GoQAM modulators cannot be used to provide VOD services. GoQAM modulators produce partially encrypted sessions, which are not necessary for providing VOD.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also know which QAM, MQAM, or GQAM modulator will provide data for each VOD service.

### Adding a Service Group

After you add the content QAM, MQAM modulator, or GQAM modulator that will be providing data for a particular VOD service, complete these steps to add a service group for that modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Click **Add**. The Add Service Group window opens.
5. Complete the fields on the screen as described in Service Group Settings.

Use the Add Service Group window on the DNCS Administrative Console to add service groups to the DNCS.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and |

| | |
|---|---|
| | that processes VOD data for Hub 1. |
| Parent Group | Allows this service group to function as a parent service group.<br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Groups/Selected Groups | Determines the child groups associated with this parent group. Select groups from this list only when adding a parent service group to the DNCS.<br>To add a child to this parent service group, select a service group in the Available Group list and click **Add**.<br>The selected service group moves from the Available Groups list to the Selected Groups list.<br>**Notes:**<br>▪ If you make a mistake, you can remove ports from the Selected Groups list by clicking on the name of the group you want to remove in the Selected Groups list, and then clicking **Remove**. The selected group moves from the Selected Groups list into the Available Groups list.<br>▪ These lists display only when you select the **Parent Group** setting. For more information on parent service groups, see Types of Service Groups. |
| Available Ports/Selected Ports | Determines the ports associated with the service group.<br>Select the port of the QAM, MQAM, or GQAM modulator that will provide VOD data for this service group and click **Add**.<br>The selected port moves from the Available Ports list into the Selected Ports list.<br>Repeat for each QAM, MQAM, or GQAM modulator that will provide VOD data for this service group.<br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

### Related Topics

- Service Groups
- Edit Service Group Settings

6. Click **Save**. The system closes the Add Service Group window and displays the Service Group Data window, which now lists the service group that you just added. The message "Service Group Saved Successfully" appears in the status area of the window.

7. Click **File > Close** to return to the DNCS Administrative Console.

## Related Topics

- Modify a Service Group
- Remove a Service Group
- Types of Service Groups

## Add a Service Group

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

These instructions describe how to add a service group to the DNCS.

**Note:** For more information about service groups, see Types of Service Groups.

**Important:** If you are using Overlay technology, remember that GoQAM modulators cannot be used to provide VOD services. GoQAM modulators produce partially encrypted sessions, which are not necessary for providing VOD.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also know which QAM, MQAM, or GQAM modulator will provide data for each VOD service.

### Adding a Service Group

After you add the content QAM, MQAM modulator, or GQAM modulator that will be providing data for a particular VOD service, complete these steps to add a service group for that modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Click **Add**. The Add Service Group window opens.
5. Complete the fields on the screen as described in Service Group Settings.

Use the Add Service Group window on the DNCS Administrative Console to add service groups to the DNCS.

**Note:** To configure how the DNCS manages service group sessions, go to Session Signaling Parameter Settings.

| Field | Description |
|---|---|
| ID | A unique number to identify the service group.<br><br>**Important:** Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable. |
| Name | The name for the service group.<br><br>You can use alphanumeric characters.<br><br>Be sure to use a name that allows you to easily identify the VOD service, the QAM, MQAM, or GQAM modulators providing it, and which hub they serve.<br><br>**Example:** A name of **VOD_SG_Hub1_MQ43** could represent a VOD service group associated with an MQAM modulator, whose IP address ends in 43, and |

| | |
|---|---|
| | that processes VOD data for Hub 1. |
| Parent Group | Allows this service group to function as a parent service group.<br>A parent service group contains one or more child service groups. For more information, see Types of Service Groups. |
| Available Groups/Selected Groups | Determines the child groups associated with this parent group. Select groups from this list only when adding a parent service group to the DNCS.<br>To add a child to this parent service group, select a service group in the Available Group list and click **Add**.<br>The selected service group moves from the Available Groups list to the Selected Groups list.<br>**Notes:**<br>▪ If you make a mistake, you can remove ports from the Selected Groups list by clicking on the name of the group you want to remove in the Selected Groups list, and then clicking **Remove**. The selected group moves from the Selected Groups list into the Available Groups list.<br>▪ These lists display only when you select the **Parent Group** setting. For more information on parent service groups, see Types of Service Groups. |
| Available Ports/Selected Ports | Determines the ports associated with the service group.<br>Select the port of the QAM, MQAM, or GQAM modulator that will provide VOD data for this service group and click **Add**.<br>The selected port moves from the Available Ports list into the Selected Ports list.<br>Repeat for each QAM, MQAM, or GQAM modulator that will provide VOD data for this service group.<br>**Note:** If you make a mistake, you can remove ports from the Selected Ports list by clicking on the name of the port you want to remove in the Selected Ports list, and then clicking **Remove**. The selected port moves from the Selected Ports list into the Available Ports list. |

### Related Topics

- Service Groups
- Edit Service Group Settings

6. Click **Save**. The system closes the Add Service Group window and displays the Service Group Data window, which now lists the service group that you just added. The message "Service Group Saved Successfully" appears in the status area of the window.

7. Click **File > Close** to return to the DNCS Administrative Console.

## Related Topics

- Modify a Service Group
- Remove a Service Group
- Types of Service Groups

## Modify a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Select Service Group Name] > Open Selected Service Group**

This section describes how to modify service groups, which are used to provide VOD and other interactive services to subscribers.

After a service group has been saved in the DNCS, you can modify many of its parameters. For example, you can add a QAM modulator to the service group by selecting the modulator's RF output ports the VOD service will use. If your site uses generic QAM modulators, you can use the same method to add generic QAM modulators to service groups. However, to change the name or identifier (ID) of a service group, delete the service group and then add the service group again. When you add the service group back to the DNCS, use a new name or ID for the service group.

### Modifying a Service Group

Complete these steps to modify a service group in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Use the Filter to display the service group that you want to modify.

   **Note:** For assistance using the Filter, see Service Group Filter.

5. Select the box next to the Service Group that you want to modify.
6. Click **Edit**. The Edit Service Group window opens for the service group you selected.
7. Make any of the following changes. For assistance with any of the fields, see Edit Service Group Settings.
   - If this is a child service group, you can change the Parent ID and make this service group the child of another parent service group. Or, you can enter a Parent ID of 0 to make this a standalone service group instead of a child service group.

     Important: Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable.

   - For a parent, standalone, or child service group, you can change the RF ports that the service group uses by adding or removing RF ports:
     - To add RF ports to the service group, select a port in the Available Ports and click **Add** . The selected port moves from the Available Ports list to the Selected Ports list.
     - To remove RF ports from the service group, select a port in the **Selected Ports** list and click **Remove**. The selected port moves from the Selected Ports list to the Available Ports list.
8. When you finish making changes, click **Save** . The system saves the new service group information in the DNCS database. The Service Group Data window updates to include the new service group information.
9. Update your network map to reflect these changes.

## Modify a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Select Service Group Name] > Open Selected Service Group**

This section describes how to modify service groups, which are used to provide VOD and other interactive services to subscribers.

After a service group has been saved in the DNCS, you can modify many of its parameters. For example, you can add a QAM modulator to the service group by selecting the modulator's RF output ports the VOD service will use. If your site uses generic QAM modulators, you can use the same method to add generic QAM modulators to service groups. However, to change the name or identifier (ID) of a service group, delete the service group and then add the service group again. When you add the service group back to the DNCS, use a new name or ID for the service group.

### Modifying a Service Group

Complete these steps to modify a service group in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Service Group**. The Service Group Data window opens.
4. Use the Filter to display the service group that you want to modify.

   **Note:** For assistance using the Filter, see Service Group Filter.

5. Select the box next to the Service Group that you want to modify.
6. Click **Edit**. The Edit Service Group window opens for the service group you selected.
7. Make any of the following changes. For assistance with any of the fields, see Edit Service Group Settings.
   - If this is a child service group, you can change the Parent ID and make this service group the child of another parent service group. Or, you can enter a Parent ID of 0 to make this a standalone service group instead of a child service group.

     Important: Make certain that this field contains only numerical characters and that the field contains no leading or trailing spaces. Entering alphabetical characters or a leading or trailing space in this field can cause the service group and associated resources assigned to the service group to become non-editable or non-viewable.

   - For a parent, standalone, or child service group, you can change the RF ports that the service group uses by adding or removing RF ports:
     - To add RF ports to the service group, select a port in the Available Ports and click **Add** . The selected port moves from the Available Ports list to the Selected Ports list.
     - To remove RF ports from the service group, select a port in the **Selected Ports** list and click **Remove**. The selected port moves from the Selected Ports list to the Available Ports list.
8. When you finish making changes, click **Save** . The system saves the new service group information in the DNCS database. The Service Group Data window updates to include the new service group information.
9. Update your network map to reflect these changes.

# Delete a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Service Group Name] Delete Selected Service Group**

Use this procedure to delete a standalone, parent, or child service group from the DNCS.

**Important:** When you delete a parent service group, any child service groups that belong to the parent service group **are not** deleted. Child service groups remain until you delete each one individually, or change the child service group to a standalone service group by changing the Parent ID of the child service group to 0.

## You Need to Know

Before You Begin

Before you delete a service group, you must delete any associated QAM or MQAM modulators. In addition, you must have your network map available.

## Deleting a Service Group

1. Are there any QAM or MQAM modulators associated with this service group?
   - If **yes**, delete those modulators first. Go to Deleting a QAM, MQAM, GQAM, or GoQAM Modulator. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Service Group**. The Service Group Data window opens.
5. Use the Filter to display the service group that you want to delete.

   **Note:** For assistance using the Filter, see Service Group Filter Overview.
6. Select the box to the left of the service group that you want to delete.
7. Click **Delete**. A confirmation window opens and asks you to confirm the deletion.
8. Click **OK**. The system removes the service group from the Service Group Data window and a message appears in the Status area of the window to let you know that the deletion was successful.
9. Remove the service group from your network map.

# Delete a Service Group

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Service Group > [Service Group Name] Delete Selected Service Group**

Use this procedure to delete a standalone, parent, or child service group from the DNCS.

**Important:** When you delete a parent service group, any child service groups that belong to the parent service group **are not** deleted. Child service groups remain until you delete each one individually, or change the child service group to a standalone service group by changing the Parent ID of the child service group to 0.

## You Need to Know

Before You Begin

Before you delete a service group, you must delete any associated QAM or MQAM modulators. In addition, you must have your network map available.

## Deleting a Service Group

1. Are there any QAM or MQAM modulators associated with this service group?
   - If **yes**, delete those modulators first. Go to Deleting a QAM, MQAM, GQAM, or GoQAM Modulator. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Service Group**. The Service Group Data window opens.
5. Use the Filter to display the service group that you want to delete.

   **Note:** For assistance using the Filter, see Service Group Filter Overview.
6. Select the box to the left of the service group that you want to delete.
7. Click **Delete**. A confirmation window opens and asks you to confirm the deletion.
8. Click **OK**. The system removes the service group from the Service Group Data window and a message appears in the Status area of the window to let you know that the deletion was successful.
9. Remove the service group from your network map.

## Define Session Signaling Parameters

**Quick Path: DNCS Administrative Console > System Provisioning tab > DNCS System > DSM-CC tab**

When a subscriber requests an interactive service, such as VOD, the DHCT, DNCS, and VOD server communicate with each other. The DNCS allows you to manually define key parameters for these communications so that they suit the needs of your system. These parameters are defined when your system is upgraded or installed; however, you can change these values to keep up with any system modifications.

### Defining Session Signaling Parameters

**Quick Path: DNCS Administrative Console > System Provisioning tab > DNCS System > DSM-CC tab**

Follow these steps to modify existing settings for VOD session signaling.

1. If you have not already done so, follow the **Quick Path** shown above to display the **DSM- CC** (Digital Storage Media - Communication and Control) tab within the DNCS System Configuration window.
2. Enter a new setting in any of the following fields. See Session Signaling Parameter Settings for a description each field in the **DSM- CC** tab and the range of values that we recommend for those fields.

   The following table describes each field in the DSM-CC tab and provides the range of values that we recommend.

| Field | Description |
|---|---|
| **DHCT Session Signaling Parameters** | |
| Send 'Session in Progress' Every | Enter a time (in minutes) that defines how often a DHCT tells the DNCS that a VOD event is in progress. The Session in Progress (SIP) message prevents the system from tearing down sessions while a DHCT receives an event.<br>**Warning:** A reduction in VOD performance may occur when a large number of SIP messages are generated at the same time.<br>We recommend that you generate SIP messages at least every 120 minutes, but no more than 180 minutes. |
| Retry Requests Up To | How many times a DHCT should send a session request to the DNCS .<br>We recommend that you set this value to **1** for one, but no more than 2 retries.<br>Setting this value to two or more times results in subscribers having to wait longer for a response. In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For Network Response After | How long (in seconds) a DHCT should wait for confirmation that the DNCS is processing the session request<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| **Network Session Signal Parameters** | |
| Send 'Setup Proceeding' Every | How long (in seconds) a DHCT must wait to receive confirmation from the DNCS that it is processing the session request that the DHCT sent.<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| Retry Requests Up To | How many times the DNCS should request tuning information from the VOD server for a particular event.<br>We recommend that you set this value to be equal to or greater than the **Retry Requests Up To** parameter for DHCTs.<br>Setting this value to two or more times results in subscribers having to wait longer for a response.<br>In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |

| | |
|---|---|
| Stop Waiting For User Response After | How long (in seconds) the DNCS should wait for the VOD server to respond after the tuning information is requested.<br><br>We strongly recommend that you set this parameter to be greater than the **Stop Waiting For Network Response After** parameter for DHCTs. Doing so ensures that a DHCT initiates the teardown of a session before the DNCS does. |
| Highest Program Bandwidth | The maximum allowable bandwidth for VOD sessions. |
| Reuse Expired Session IDs After | How long (in seconds) the system must wait to reuse a session ID after the ID has expired<br><br>We recommend that you set this value to at least **3**, but no longer than **5** seconds. |

3. Click **Save**. The DNCS saves the information you entered and displays the message "Save complete" at the bottom of the DNCS System Configuration window.

4. Click **Close** to close the DNCS System Configuration window.

### Modifying Existing VOD Session Signaling Parameters

Follow these steps to modify existing settings for VOD session signaling.

1. From the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **DNCS System**. The DNCS System Configuration window opens.
3. Click the **DSM-CC** (Digital Storage Media - Communication and Control) tab.
4. Enter a new setting in any of the fields listed in the table in Session Signaling Parameter Settings.

The following table describes each field in the DSM-CC tab and provides the range of values that we recommend.

| Field | Description |
|---|---|
| **DHCT Session Signaling Parameters** | |
| Send 'Session in Progress' Every | Enter a time (in minutes) that defines how often a DHCT tells the DNCS that a VOD event is in progress. The Session in Progress (SIP) message prevents the system from tearing down sessions while a DHCT receives an event.<br>**Warning:** A reduction in VOD performance may occur when a large number of SIP messages are generated at the same time.<br>We recommend that you generate SIP messages at least every 120 minutes, but no more than 180 minutes. |
| Retry Requests Up To | How many times a DHCT should send a session request to the DNCS .<br>We recommend that you set this value to **1** for one, but no more than 2 retries.<br>Setting this value to two or more times results in subscribers having to wait longer for a response. In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For Network Response After | How long (in seconds) a DHCT should wait for confirmation that the DNCS is processing the session request<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| **Network Session Signal Parameters** | |
| Send 'Setup Proceeding' Every | How long (in seconds) a DHCT must wait to receive confirmation from the DNCS that it is processing the session request that the DHCT sent.<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| Retry Requests Up To | How many times the DNCS should request tuning information from the VOD server for a particular event.<br>We recommend that you set this value to be equal to or greater than the **Retry Requests Up To** parameter for DHCTs.<br>Setting this value to two or more times results in subscribers having to wait longer for a response.<br>In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For | How long (in seconds) the DNCS should wait for the VOD server to respond after |

| | |
|---|---|
| User Response After | the tuning information is requested.<br>We strongly recommend that you set this parameter to be greater than the **Stop Waiting For Network Response After** parameter for DHCTs. Doing so ensures that a DHCT initiates the teardown of a session before the DNCS does. |
| Highest Program Bandwidth | The maximum allowable bandwidth for VOD sessions. |
| Reuse Expired Session IDs After | How long (in seconds) the system must wait to reuse a session ID after the ID has expired<br>We recommend that you set this value to at least **3**, but no longer than **5** seconds. |

5. After you have updated the fields with new data, click **Save**. The DNCS saves the information you entered and displays the message "Save complete" at the bottom of the DNCS System Configuration window.

6. Click **Cancel** to close the DNCS System Configuration window.

## Session-Based Encryption for VOD

If you purchased and activated your license for the Session-Based Encryption (SBE) feature, your system can provide encrypted Video-on-demand (VOD) sessions to only the DHCTs that request them.

SBE uses a unique key to encrypt each session so that the session is accessible only to the DHCT that has requested it. Because these sessions are encrypted (secure) and because they are accessible only to the DHCT requesting the session, these sessions are referred to as secure exclusive sessions.

## Protect On-Demand Content From Unauthorized Copying

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules > BFS Client > [Expand the OSM File Cabinet] > File > Delete**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules > Please select a site > [Select Site] > BFS Client > [Expand the OSM File Cabinet] > File > Delete**

To protect the content of an encrypted on-demand source, assign CCI to each segment that provides a service from this source. This procedure describes how to configure the Set Up Segment window to assign a level of CCI to an existing segment. To determine the level of security required for each encrypted service you offer to subscribers, contact your corporate office or the content provider.

**Notes:**

- CCI settings are effective immediately.
- In a system where PowerKEY is not used, the provider of the primary conditional access (CA) system is responsible for delivering CCI data to the DHCT.
- A content-protection method is not enforced on OpenCable Host devices that are not running the PowerTV OS. For example, you may require the HDCP to be always on, but the OpenCable Host may disable HDCP for Copy Freely content.

**Important:** If more than one segment has been created from the same source, all segments must have the same levels of content-protection. Otherwise, content-protection may not work as expected for those segments.

**You Need to Know**

Additional Information

For details on these content-protection settings, including the content-protection methods used by output ports on our DHCTs, see Enabling Content Protection for Broadcast Programming Configuration Guide (part number 4005893). To obtain a copy of this publication, see Printed Resources.

Before You Begin

Before you begin, contact your corporate office or your content provider to determine the level of security required for each encrypted service you offer subscribers.

**Important:** CCI is delivered in the ECM for a program. As a result, it may be applied to any **encrypted** source. However, it cannot be applied to a **clear** source because clear sources do not require ECMs.

Time to Complete

Adding security to one segment takes about a minute.

### Removing the no_vod_cci File Flag

If the no_vod_cci file is present on the BFS, DHCTs automatically activate content protection on the 1394 output for any VOD or xOD sessions. For this reason, you should remove the no_vod_cci flag from the BFS if you want DHCTs to protect content based on the settings provided by the VOD or xOD application.

To remove the no_vod_cci file from the BFS, complete the following procedure.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **OS**. The DHCT OS List window opens.
4. Scroll through the OS list. Is the no_vod_cci file present in the list?
   - If **yes**, select the file and click **File > Delete**. The file is removed from the BFS. All VOD or xOD sessions built from this point forward use the content- protection settings specified in the session setup request.
   - If **no**, go to step 5.
5. Click **File > Close** to close the OS list.
6. Select the **Applications Interface Modules** tab.
7. Are you using our RCS Solution?
   - If **yes**, click **BFS Client**. The Please select a site window opens. Go to step 8.
   - If **no**, click **BFS Client**. The Broadcast File Server List window opens. Go to step 9.
8. Select **DNCS** from the list of sites. Then select **File > Select**. The Broadcast File Server List window opens for the site you selected.
9. Scroll down and double-click the **OSM** cabinet.
10. Is the no_vod_cci file present in the OSM cabinet?
    - If **yes**, select the file.
    - If **no**, go to step 12.
11. Click **File > Delete** to delete the file.
12. Click **File > Close** to close the Broadcast File Server List window.
13. Are you using our RCS Solution?
    - If **no**, you have successfully removed the no_vod_cci file flag.
    - If **yes**, go to step 14.
14. Do you want to remove the no_vod_cci file flag from other sites in your system?
    - If **yes**, from the Please select a site window, select the site whose no_vod_cci flag you want to remove. Then repeat this procedure from step 8 to remove the no_vod_cci flag file from this site.
    - If **no**, you have successfully removed the no_vod_cci file flag from all sites in your system. Select **File > Close** to close the Please select a site window.

### Creating the no_vod_cci File Flag

If your provider is not able to set up content protection for your server, complete the following instructions to set up a VOD file flag (no_vod_cci) to set all content to "copy never."

1. Open an xterm window.
2. At the dncs user prompt, type **pwd** and press **Enter**. The system displays the working directory.
3. Did the system display **/export/home/dncs** as the working directory?
   - If **yes**, go to step 4.
   - If **no**, type **cd /export/home/dncs** and press **Enter**. The system makes /export/home/dncs the working directory.
4. Type **touch no_vod_cci** and press **Enter**. The system creates an empty file in the directory /export/home/dncs and labels the file no_vod_cci.
5. Type **exit** and press **Enter**. The xterm window closes.
6. From the DNCS Administrative Console, select the **DNCS** tab.
7. Select the **Home Element Provisioning** tab.
8. Click **OS**. The DHCT OS List window opens.
9. Click **File > New**. The Set Up DHCT OS window opens.
10. Click **Browse**. The Select OS File window opens.
11. Click in the **Filter** field and type **/export/home/dncs/***. The files in the /export/home/dncs directory appear in the Files list.
12. Scroll down the Files list to find and select the file no_vod_cci that you created. The Selection field updates and displays the path to the no_vod_cci file.
13. Click **OK**. The Select OS File window closes and /export/home/dncs/no_vod_cci appears in the Source File field on the Set Up DHCT OS window.
14. In the **Destination File Name** field, type **bfs:///osm/no_vod_cci**.
15. In the **Description** field, type **File to Activate Content Protection on VOD**.
16. For **Format**, select **Out-of-Band File**.
17. Click **Save**. The system places the no_vod_cci file the BFS carousel and, as a result, DHCTs automatically activate content protection on 1394 outputs for any VOD or xOD sessions.

# Manage Regional Control System

## Introduction

This section provides instructions on provisioning and managing remote sites from a central DNCS and SARA Server.

Introduction

# Overview

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites**

If you are using our Regional Control System (RCS), you have the ability to provision and manage remote sites from a central DNCS and SARA Server. Because all system provisioning and management is done from a central DNCS, there is no need for system managers to be physically located at remote sites. In addition, if any sites (including the central, DNCS site) use our Overlay solution, these sites can deliver digital video services to set-tops boxes manufactured by us or by other vendors. (We refer to other vendors as **third-party vendors**.) All sites running RCS must use Direct ASI.

## What do you want to do?

- View the a diagram of the RCS elements that process data
- Set up RCS elements
- Learn how the Emergency Alert System functions in a central RCS site
- Learn how the Emergency Alert System functions in a remote RCS site
- Make changes to RCS elements
- Maintain an RCS
- Troubleshoot an RCS

# Topology of RCS Elements That Process System Data

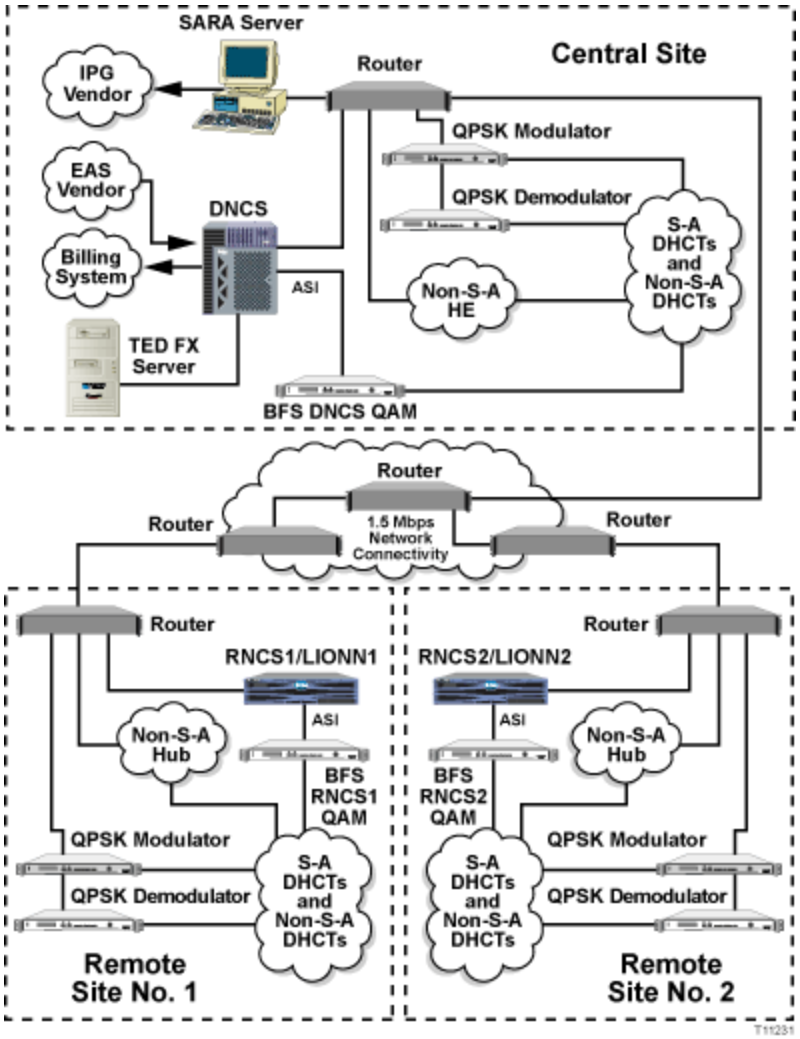
As shown in the following diagram, to communicate with remote sites, the DNCS and SARA Server use a 1.5 Mbps data link to route information to remote sites. From each remote router, information is passed on to a Remote Network Control Server or RNCS, which stores data received from the DNCS in persistent storage and cache. Each RNCS then connects to the elements of the remote digital broadband delivery system (DBDS) in much the same way that the elements of a DBDS connect to a DNCS. In fact, it may help to think of an RNCS as a remote DNCS with no user interface.

The Digital Broadband Delivery System (DBDS) is a network of hardware and software elements that connects content servers to DHCTs to deliver MPEG video, audio, digital data, and analog services to subscribers. The DNCS provides information about each element in a DBDS to other DBDS elements so that they can all communicate with each other.

**Notes:**

- You may also hear an RNCS referred to as a LIONN, or Lights Out Network Node because an RNCS has no operator lights and is a node on the RCS network.
- The following example shows how the elements that process **system data** interconnect to create a DBDS with an RCS. DBDS elements that process **content** are not shown here because these elements interconnect the same way in a typical DBDS as they do in a DBDS with an RCS.

The Digital Broadband Delivery System (DBDS) is a network of hardware and software elements that connects content servers to DHCTs to deliver MPEG video, audio, digital data, and analog services to subscribers. The DNCS provides information about each element in a DBDS to other DBDS elements so that they can all communicate with each other.


SARA Server
Central Site
IPG Vendor
Router
QPSK Modulator
EAS Vendor
DNCS
QPSK Demodulator
S-A DHCTs and Non-S-A DHCTs
Billing System
ASI
Non-S-A HE
TED FX Server
BFS DNCS QAM
Router
Router
1.5 Mbps Network Connectivity
Router
Router
Router
RNCS1/LIONN1
RNCS2/LIONN2
ASI
ASI
Non-S-A Hub
Non-S-A Hub
BFS RNCS1 QAM
BFS RNCS2 QAM
QPSK Modulator
QPSK Modulator
S-A DHCTs and Non-S-A DHCTs
S-A DHCTs and Non-S-A DHCTs
QPSK Demodulator
QPSK Demodulator
Remote Site No. 1
Remote Site No. 2
T11231

# Set Up RCS Elements

When setting up RCS elements, you will set up many of the DBDS elements that you are already familiar with. In addition to setting up those elements, you will also set up elements that are unique to an RCS configuration.

**Note:** For an overview of elements in a typical DBDS, see Setting Up Your Network.

## What do you want to do?

- Learn the process for setting up all RCS elements
- Add a remote site to an RCS
- Add a billing reference to an RCS site
- Add a headend to an RCS site
- Add a BFS QAM modulator to an RCS
- Verify the VASP configuration in an RCS

# Site Summary

If your DBDS uses an RCS, you can manage most of the logical elements (sites, headends, hubs) in your system from the Site Summary window.

You can perform any of the following tasks from the Site Summary window:

## Manage Sites

- Add a remote site to an RCS
- Modify an RCS site
- Delete an RCS site

## Manage Headends

- View the headends of a site
- Add a headend to an RCS site
- Modify an RCS headend
- Delete a headend from an RCS site

## Manage Hubs

- View the hubs of a site
- Add a hub to an RCS headend
- Modify an RCS hub
- Delete an RCS hub

## Manage Billing References

- Add a billing reference to an RCS site
- Modify a billing reference in your RCS
- Delete a billing reference from your RCS

# RCS Settings

Use the following topics to learn about the settings for various RCS components:

- RCS Remote Site Settings
- RCS Headend Settings
- RCS Hub Settings
- BFS QAM Settings
- RCS VASP Entry Settings

## RCS Remote Site Settings

Use the following fields when you manage a remote site in an RCS.

| Field | Description |
|---|---|
| Site Name | The name for the site.<br>You can use up to 15 alphanumeric characters.<br>Example: If your site is located in Denver, Colorado, you might enter Denver.<br>**Note:** Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Site ID | A unique number to identify this site.<br>Use any number 2 or greater.<br>**Important:** Make sure that each site ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to change this field later. |
| Site IP Address | The IP address of the RNCS/LIONN at the remote site.<br>Be careful to properly place the dots (.) between numbers.<br>@ |
| Site MAC Address | The MAC address of this RNCS/LIONN. |
| BFS MAC Address | A number that represents the BFS MAC address of the site you are adding, based on the following criteria:<br>▪Each address must be unique.<br>▪The central DNCS site always uses an address of 00:00:00:00:00:00.<br>▪If you are adding a remote site, use a similar, but unique address that incorporates the ID site ID.<br>Example: If you are adding the first remote site, you might use the number 00:00:00:00:00:02 to represent the BFS MAC address of the first remote site. |
| Online | Determines whether this site is active or inactive. |

## RCS Headend Settings

Use the following fields when you manage an RCS headend.

| Field | Description |
|---|---|
| Headend Name | The name you will use to identify this headend (for example, **HE1**).<br>You can use up to 15 alphanumeric characters.<br>**Example:** If this headend is in the Denver site, you might use **Dnvr_HE1**. |
| Headend ID | The number you will use to identify this headend.<br>You can use any number between 1 and 2147483647.<br>**Important:** Be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to modify this field later. |
| Site Name | The site this headend is associated with. |

## RCS Hub Settings

Use the following fields when you manage a hub in an RCS headend.

| Field | Description |
|---|---|
| Hub Name | The name you will use to identify this hub.<br>You can use up to 15 alphanumeric characters.<br>**Example:** If this hub is in Headend 1, which is in the Denver site, you might use **Dnvr_HE1_Hub1**. |
| Hub ID | The number you will use to identify this hub.<br>You can use up to eight digits.<br>**Important:** Be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to modify this field later. |
| Headend | The headend where this hub is located. |
| Time Zone | The time zone used where this hub resides. |
| DST Zone ID | If this hub resides in an area that uses daylight saving time, select the appropriate DST Zone ID.<br>**Notes:**<br>▪For more information on DST Zone ID, see the DST Zone ID field in Fields in the DST Rules window.<br>▪For more information on DST rules, see Set Daylight Saving Time Rules Window.<br>▪To manage time correctly on your network, you must install the Digital System Time Kit, if not installed previously. Refer to DBDS System Time Installation and Maintenance Guide (part number 4011510) for more information. To obtain a copy of this publication, see Printed Resources. |

## BFS QAM Settings

Use the Set Up QAM page to manage the BFS QAM modulators in your network. The following tabs in this window provide settings for the BFS QAM:

- Basic Parameters Settings
- Connection Settings
- Advanced Parameters settings - The system automatically sets up advanced parameters. As a result, you do not need to complete any fields on the Advanced Parameters tab.

**Important:** Do not change information in the Advanced Parameters tab without first consulting Cisco Services. Changing this data without direction from Cisco Services can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

### Basic Parameter Settings - BFS QAM Modulator

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪If the BFS QAM Modulator connects to a BFS BIG, click the **SWIF** option to select the type of card sending BFS data from the BFS BIG to this QAM modulator.<br>▪If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator<br>Select the type of modulation this QAM modulator uses. For example, if this modulator |

| | |
|---|---|
| uses | uses 256 QAM, you would select **256 QAM**. |
| **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

## Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

## Connections Settings - BFS QAM Modulator

Use the following fields when you manage the connections for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which the device that feeds or receives from the BFS QAM resides. |
| Device Type | Determines the device type that feeds this QAM:<br>▪If a BFS BIG feeds the BFS QAM, select **BIG**.<br>▪If an ASI card on the DNCS feeds this BFS QAM, select **ASI**. Select this option if you are using the QAM modulator with an RCS.<br>The option you select determines which parameters display for setup, as described below. |
| Device Name | The name of the device. Valid for either BFS BIG or ASI QAMs. |
| Card Type | The type of card in the BFS BIG.<br>Select **MSYNC SWIF**. |
| Slot Number | The slot number where the MSYNC control card is installed on the BFS BIG (usually, slot 3).<br>Valid for BFS BIG only. |
| Port Number | The port number for the various cards:<br>▪**For BFS BIG** - control card that is connected to this QAM modulator (usually port 1).<br>▪**For ASI** - Select the port number on the ASI card that is connected to this BFS QAM modulator. |

### Related Topics

- Add a BFS QAM
- Setting Up BFS QAM Modulator Connections in an RCS
- BFS QAM Modulator
- BFS QAM Settings

## RCS VASP Entry Settings

Use the following fields when you manage a VASP entry in an RCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you are adding.<br>Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry. |
| Name | The name of this VASP entry.<br>You can use up to 80 alphanumeric characters. Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br>**Example:** A name of VODhub1Q43 would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br>Be careful to properly place the dots (.) between numbers. If you are adding a VASP entry for the mmmRemote server, use the IP address for the RNCS/LIONN.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated.<br>Select **In Service** to activate this VASP. |
| Site ID | The site for which this VASP provides service. |

# Add a Remote Site to an RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Add Site**

**Important:** Follow this procedure only if you use an RCS.

If you are using a Regional Control System (RCS), the first step in setting up the elements in an RCS is to set up each site remote site that the RCS will manage. You can add up to 24 sites to your RCS. You need to set up one remote site for each RNCS/LIONN in your network. You do not need to set up a central site for your DNCS because the system automatically creates one for you.

## Adding a Remote Site to an RCS

Follow these steps to add a remote site to your RCS network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.

Click **Add Site**. A new row appears in the Site Summary window.

**Tip:** If you are adding several sites at once, you may find it easier to copy information from one field, paste it to another, and then modify the information you have pasted.

4. Complete the fields on the screen as described in RCS Remote Site Settings.

Use the following fields when you manage a remote site in an RCS.

| Field | Description |
|---|---|
| Site Name | The name for the site.<br>You can use up to 15 alphanumeric characters.<br>Example: If your site is located in Denver, Colorado, you might enter Denver.<br>**Note:** Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Site ID | A unique number to identify this site.<br>Use any number 2 or greater.<br>**Important:** Make sure that each site ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to change this field later. |
| Site IP Address | The IP address of the RNCS/LIONN at the remote site.<br>Be careful to properly place the dots (.) between numbers.<br>@ |
| Site MAC Address | The MAC address of this RNCS/LIONN. |
| BFS MAC Address | A number that represents the BFS MAC address of the site you are adding, based on the following criteria:<br>▪ Each address must be unique. |

| | |
|---|---|
| | ▪ The central DNCS site always uses an address of 00:00:00:00:00:00.<br>▪ If you are adding a remote site, use a similar, but unique address that incorporates the ID site ID.<br>Example: If you are adding the first remote site, you might use the number 00:00:00:00:00:02 to represent the BFS MAC address of the first remote site. |
| Online | Determines whether this site is active or inactive. |

5. Click **Save**. The system displays the message "Site data update completed."

**Tip:** If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already in use), click OK to close the message. Then click the **Go** menu and select **Back**. The system displays the information you entered earlier beginning with step 4. You can now modify this information and click **Save** again.

6. Click **OK**. The system saves information about this site.

7. Do you need to add another site?

- If **yes**, repeat this procedure from step 3.
- If **no**, go to step 8.

8. Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add a billing reference to each of your sites. Go to Add a Billing Reference to an RCS Site.
- If **no**, continue making any other changes that you need to make to your network. When finished, update your network map with the changes.

# Add a Remote Site to an RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Add Site**

**Important:** Follow this procedure only if you use an RCS.

If you are using a Regional Control System (RCS), the first step in setting up the elements in an RCS is to set up each site remote site that the RCS will manage. You can add up to 24 sites to your RCS. You need to set up one remote site for each RNCS/LIONN in your network. You do not need to set up a central site for your DNCS because the system automatically creates one for you.

## Adding a Remote Site to an RCS

Follow these steps to add a remote site to your RCS network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.

Click **Add Site**. A new row appears in the Site Summary window.

**Tip:** If you are adding several sites at once, you may find it easier to copy information from one field, paste it to another, and then modify the information you have pasted.

4. Complete the fields on the screen as described in RCS Remote Site Settings.

Use the following fields when you manage a remote site in an RCS.

| Field | Description |
|---|---|
| Site Name | The name for the site.<br>You can use up to 15 alphanumeric characters.<br>Example: If your site is located in Denver, Colorado, you might enter Denver.<br>**Note:** Be sure to use a name that is consistent with the naming scheme used on your network map. |
| Site ID | A unique number to identify this site.<br>Use any number 2 or greater.<br>**Important:** Make sure that each site ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to change this field later. |
| Site IP Address | The IP address of the RNCS/LIONN at the remote site.<br>Be careful to properly place the dots (.) between numbers.<br>@ |
| Site MAC Address | The MAC address of this RNCS/LIONN. |
| BFS MAC Address | A number that represents the BFS MAC address of the site you are adding, based on the following criteria:<br>▪ Each address must be unique. |

| | |
|---|---|
| | ▪ The central DNCS site always uses an address of 00:00:00:00:00:00.<br>▪ If you are adding a remote site, use a similar, but unique address that incorporates the ID site ID.<br>Example: If you are adding the first remote site, you might use the number 00:00:00:00:00:02 to represent the BFS MAC address of the first remote site. |
| Online | Determines whether this site is active or inactive. |

5. Click **Save**. The system displays the message "Site data update completed."

**Tip:** If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already in use), click OK to close the message. Then click the **Go** menu and select **Back**. The system displays the information you entered earlier beginning with step 4. You can now modify this information and click **Save** again.

6. Click **OK**. The system saves information about this site.

7. Do you need to add another site?

- If **yes**, repeat this procedure from step 3.
- If **no**, go to step 8.

8. Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add a billing reference to each of your sites. Go to Add a Billing Reference to an RCS Site.
- If **no**, continue making any other changes that you need to make to your network. When finished, update your network map with the changes.

# Add a Billing Reference to an RCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Billing References > Add Billing**

**Important:** Follow this procedure only if you use an RCS.

After adding remote sites to your RCS, next add billing references for each site (central and remote) in your RCS. A billing reference indicates the billing system to which each site is connected.

## Billing Reference Summary

If you are running an RCS system, you can manage the billing references in your system from the Billing References Summary window.

## What do you want to do?

From this window, you can perform the following tasks:

- Add a billing reference to an RCS site
- Delete a billing reference from an RCS site
- Modify a billing reference in your RCS

# Add a Billing Reference to an RCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Billing References > Add Billing**

**Important:** Follow this procedure only if you use an RCS.

After adding remote sites to your RCS, next add billing references for each site (central and remote) in your RCS. A billing reference indicates the billing system to which each site is connected.

## Billing Reference Summary

If you are running an RCS system, you can manage the billing references in your system from the Billing References Summary window.

## What do you want to do?

From this window, you can perform the following tasks:

- Add a billing reference to an RCS site
- Delete a billing reference from an RCS site
- Modify a billing reference in your RCS

## Adding a Billing Reference to an RCS Site

Follow these steps to add a billing reference to an RCS site.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Billing References**. The Billing Reference Summary opens and lists any billing IDs have been assigned to a site.
5. Click **Add Billing**. A new row appears in the Billing Reference Summary window.

**Note:** Be careful when entering information in these fields. After a billing reference is created, you cannot modify these fields unless you delete the billing reference and add it again using new information.

6. Click in the **Billing ID** field and type any number 2 or greater that you will use to identify the billing system for each site.

**Important:** Ensure that each billing ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map.

**Example:** You might have the billing ID match the Site ID.

7. Click the **Site Name** arrow and select the site you will associate with this billing ID.
8. Click **Save**. The system displays the message "Billing update completed."

**Tip:** If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already used), click **OK** to close the message. Then click the **Go** menu and select **Back**. The system displays the information you entered earlier in step 6. You can now modify this information and click **Save** again.

9. Do you need to add a billing reference to another site?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, go to step 10.
10. Are you setting up RCS elements for the first time?
    - If **yes**, you are ready to add headends to your sites. Click **Exit** to close the Billing Reference Summary list, then go to Add a Headend to an RNCS Site.
    - If **no**, continue making any other changes that you need to make to your network.

# Add a Headend to an RNCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Headends > Add Headend**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to add a headend to your system.

After setting up billing references for the sites to your RCS, next add headends in each of the sites by following the steps given below.

## Headend Summary

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Headends**

This window provides an at-a-glance status of the headends in your RCS. From this window, you can also modify the headends listed here.

## What do you want to do?

From this window, you can perform the following tasks:

- View the headends of a site
- Add a headend to an RCS site
- Modify an RCS headend
- Delete an RCS headend from a site

# Add a Headend to an RNCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Headends > Add Headend**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to add a headend to your system.

After setting up billing references for the sites to your RCS, next add headends in each of the sites by following the steps given below.

## Headend Summary

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Headends**

This window provides an at-a-glance status of the headends in your RCS. From this window, you can also modify the headends listed here.

## What do you want to do?

From this window, you can perform the following tasks:

- View the headends of a site
- Add a headend to an RCS site
- Modify an RCS headend
- Delete an RCS headend from a site

## Adding a Headend to an RNCS Site

Complete these steps to add a headend to a site.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens and lists all sites in the RCS network.
4. Click the **Select** button for the site where the headend is located.
5. Click **Headends**. The Headend Summary window for the site you selected in step 4 opens.
6. Click **Add Headend**. A new row containing empty fields appears in the Headend Summary window.

   **Tip:** If you are adding several headends at once, you may find it easier to copy information from one field, paste it to another, and then modify the information you have pasted.

7. Complete the fields on the screen as described in RCS Headend Settings.

   Use the following fields when you manage an RCS headend.

| Field | Description |
|---|---|
| Headend Name | The name you will use to identify this headend (for example, **HE1**).<br>You can use up to 15 alphanumeric characters.<br>**Example:** If this headend is in the Denver site, you might use **Dnvr_HE1**. |
| Headend ID | The number you will use to identify this headend.<br>You can use any number between 1 and 2147483647.<br>**Important:** Be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to modify this field later. |
| Site Name | The site this headend is associated with. |

8. Click **Save**. The system displays the message "Headend update completed."

   **Tip:** If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already in use), click the **Go** menu and select **Back**. The system displays the information you entered beginning with step 7. You can now modify this information and click **Save** again.

9. Click **OK**. The system saves information about this headend.
10. Do you need to add another headend?
    - If **yes**, repeat this procedure from step 6.
    - If **no**, go to step 11.
11. Are you setting up RCS elements for the first time?
    - If **yes**, you are ready to add hubs to your RCS network. Click **Exit** to close the Headend Summary list, then go to Add a Hub to an RCS Headend.
    - If **no**, continue making any other changes that you need to make to your RCS network.

# Add a Hub to an RCS Headend

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Hubs > Add Hub**

**Important:** Follow this procedure only if you use an RCS. If you do not use an RCS, follow a different method to add a hub to your system.

After you have added headends to your RCS, next add hubs. A hub represents the point at which out-of-band (QPSK-modulated) frequencies combine with inband (QAM) frequencies to be transmitted to subscribers through the radio frequency (RF) network.

## Adding a Hub to an RCS Headend

Complete these steps to add a hub to a headend.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens and lists all sites in the RCS network.
4. Click **Hubs**. The Hub Summary window opens.
5. Click **Add Hub**. A new row containing empty fields appears in the Hub Summary window.

   **Tip:** If you are adding several hubs at once, you may find it easier to copy information from one field, paste it to another, and then modify the information you have pasted.

6. Complete the fields on the screen as described in RCS Hub Settings.

   Use the following fields when you manage a hub in an RCS headend.

| Field | Description |
|---|---|
| Hub Name | The name you will use to identify this hub.<br>You can use up to 15 alphanumeric characters.<br>**Example:** If this hub is in Headend 1, which is in the Denver site, you might use **Dnvr_HE1_Hub1**. |
| Hub ID | The number you will use to identify this hub.<br>You can use up to eight digits.<br>**Important:** Be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to modify this field later. |
| Headend | The headend where this hub is located. |
| Time Zone | The time zone used where this hub resides. |
| DST Zone ID | If this hub resides in an area that uses daylight saving time, select the appropriate DST Zone ID.<br>**Notes:**<br>▪ For more information on DST Zone ID, see the DST Zone ID field in Fields in the DST Rules window.<br>▪ For more information on DST rules, see Set Daylight Saving Time Rules Window.<br>▪ To manage time correctly on your network, you must install the Digital System Time Kit, if not installed previously. Refer to DBDS System Time Installation and Maintenance Guide (part number 4011510) for more information. To obtain a copy of this publication, see Printed Resources. |

7. Click **Save**. The system displays the message "Hub save completed."
8. Click **OK**. The message closes and to show the Hub Summary window.
9. Do you need to add another hub?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, go to step 10.

10. Do any of the hubs in your RCS distribute services that require a QPSK demodulator in order to receive data from DHCTs and send this data to the DNCS? For example, services such as pay-per-view or video-on-demand require this configuration.

- If **yes**, add a node set to those hubs. Click **Exit** to close the Hub Summary window, then go to Adding a Node Set.
- If **no**, go to step 11.

11. Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add the elements that process system data to your RCS network. Click **Exit** to close the Hub Summary window, then go to Setting Up Elements that Process System Data.
- If **no**, continue making any other changes that you need to make to your RCS network.

# Add a BFS QAM Modulator to Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow another procedure to add a BFS QAM modulator to the DNCS.

Before adding a BFS QAM modulator to your RCS, make sure that you have first added an MPEG BFS source for the central DNCS site and for each remote site in your system.

A BFS QAM modulator receives BFS data, modulates the data onto an RF carrier, and then sends it downstream to all DHCTs on the headend. Each headend in your network must have a BFS QAM modulator associated with ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- The output transport stream ID of the ASI card on the DNCS or RNCS/LIONN

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the basic parameters of a BFS QAM modulator in an RCS.
2. Set up connections for a BFS QAM modulator in an RCS.
3. Activate a BFS QAM modulator in an RCS.

### Related Topics

- Recommendations for BFS QAM Modulators in an RCS
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

## Recommendations for BFS QAM Modulators in an RCS

We recommend the following regarding BFS QAM modulators:

- Make sure the BFS QAM modulator is **not** assigned to a specific hub, but that it sends BFS data to all hubs in the headend.
- When you activate the BFS QAM modulator, make sure that the **Allow SI** option is set to **No**. In an RCS, system information (SI) is carried on the out-of-band data path through a QPSK modulator.

## Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- The output transport stream ID of the ASI card on the DNCS or RNCS/LIONN

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

## Recommendations for BFS QAM Modulators in an RCS

We recommend the following regarding BFS QAM modulators:

- Make sure the BFS QAM modulator is **not** assigned to a specific hub, but that it sends BFS data to all hubs in the headend.
- When you activate the BFS QAM modulator, make sure that the **Allow SI** option is set to **No**. In an RCS, system information (SI) is carried on the out-of-band data path through a QPSK modulator.

# Add a BFS QAM Modulator to Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow another procedure to add a BFS QAM modulator to the DNCS.

Before adding a BFS QAM modulator to your RCS, make sure that you have first added an MPEG BFS source for the central DNCS site and for each remote site in your system.

A BFS QAM modulator receives BFS data, modulates the data onto an RF carrier, and then sends it downstream to all DHCTs on the headend. Each headend in your network must have a BFS QAM modulator associated with ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data for that headend.

### You Need to Know

Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- The output transport stream ID of the ASI card on the DNCS or RNCS/LIONN

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add a BFS QAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the basic parameters of a BFS QAM modulator in an RCS.
1. Set up connections for a BFS QAM modulator in an RCS.
1. Activate a BFS QAM modulator in an RCS.

### Related Topics

- Recommendations for BFS QAM Modulators in an RCS
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

## Recommendations for BFS QAM Modulators in an RCS

We recommend the following regarding BFS QAM modulators:

- Make sure the BFS QAM modulator is **not** assigned to a specific hub, but that it sends BFS data to all hubs in the headend.
- When you activate the BFS QAM modulator, make sure that the **Allow SI** option is set to **No**. In an RCS, system information (SI) is carried on the out-of-band data path through a QPSK modulator.

## Before You Begin

Before you begin, you must have your network map. You must also have the following information:

- IP address for the QAM modulator (from your system administrator)
- Subnet mask for the QAM modulator (from your system administrator)
- MAC address for the QAM modulator (click for information on locating the MAC address)
- The output transport stream ID of the ASI card on the DNCS or RNCS/LIONN

**Note:** All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

## Setting Up BFS QAM Modulator Basic Parameters in an RCS

Complete these steps to set up the basic parameters for a BFS QAM modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > QAM**. The Set Up QAM window opens with the Basic Parameters tab in the forefront.
5. Complete the fields on the screen as described in Basic Parameters - BFS QAM Modulator.

Use the following fields when you manage basic parameters for a BFS QAM modulator.

| Field | Description |
|---|---|
| Headend Name | The headend in which this BFS QAM modulator resides. |
| QAM Name | The name you will use to identify this BFS QAM modulator.<br>You can use up to 15 alphanumeric characters (for example, **HE1BFSQAM**).<br>Be sure to use a name that is consistent with the naming scheme used on your network map. |
| IP Address | The IP address for this QAM modulator.<br>Be careful to properly place the dots (.) between numbers.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Modulation Type | The type of modulation standard this modulator uses.<br>**Example:** If this is a 256 QAM modulator that uses ITU B modulation, select **ITU J.83 Annex B (6 MHz)**. |
| MAC Address | The MAC address for this QAM modulator. |
| Subnet Mask | The subnet mask where this QAM modulator resides.<br>If your system uses a standard network configuration, type **255.255.255.0,** otherwise type the subnet mask as assigned by your system administrator. |
| Default Gateway | If your system uses a default gateway, enter the IP address of the default gateway.<br>Using a default gateway speeds up the reconnection process that occurs after a BFS QAM modulator is rebooted. |
| Allow SI | Determines whether the QAM carries SI (system information), which defines it as a Distinguished QAM):<br>▪ Set to **yes** (selected) if this BFS QAM modulator will also function as a Distinguished QAM.<br>▪ Set to **no** (unselected) if this BFS QAM is being used in an RCS. SI information is carried by QPSK modulators in an RCS. |
| Input Port | Defines the interface that connects to this QAM modulator:<br>▪ If the BFS QAM Modulator connects to a BFS BIG, click the **SWIF** option to select the type of card sending BFS data from the BFS |

| | | |
|---|---|---|
| | BIG to this QAM modulator.<br>▪ If the BFS QAM Modulator connects directly to the DNCS, click the **ASI** option to indicate the type of card that sends BFS data from the DNCS to this QAM modulator. Select this option if you are using the QAM modulator with an RCS. | |
| INPUT Transport Stream | The system sets this value automatically when the corresponding transport stream ID is set up in the BFS BIG or ASI card and the connection is established on the Connectivity tab. | |
| RF OUT Fields | **Modulation -** The type of modulation this QAM modulator uses | Select the type of modulation this QAM modulator uses. For example, if this modulator uses 256 QAM, you would select **256 QAM**. |
| | **Transport Stream ID -** The number that identifies the transport stream the QAM sends to the DHCTs | Type a unique number to identify the transport stream going from this QAM modulator to the DHCTs on your system.<br>You can use up to 5 numeric characters. |
| | **Channel Center Frequency (MHz) -** The channel frequency you will use to send SI to DHCTs | Type the channel frequency that you will use to send SI to DHCTs on this headend.<br>We recommend that you enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies. |
| | **Continuous Wave Mode -** Determines whether the QAM produces an unmodulated RF carrier | Enable this option to produce an unmodulated RF carrier.<br>This is useful when performing testing. |
| | **Mute RF Output -** Determines whether the QAM's RF output port is muted | Enable this option to turn off the RF output for a port.<br>This is helpful when installing the modulator. |
| | **Disabled -** Determines whether you can set up additional sessions on an RF output port on the QAM | Enable this option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.)<br>This may be helpful when performing plant maintenance or in the rare event that a port fails. |
| | **Interleaver Depth -** Determines the depth of interleaving for the QAM | Select the depth of interleaving that the modulator uses.<br>Available only if you are using Overlay technology. |
| | **Port to Hubs -** Allows you to see the hubs available to this QAM | Click to view the hubs that are available to receive content data from this QAM. |

### Related Topics

- Connections Settings
- BFS QAM Settings
- Setting Up BFS QAM Modulator Basic Parameters in an RCS

6.Click **Save**. The system saves this data and closes the Output Port window.

**Important:** You should not need to use the Advanced Parameters tab because the system automatically

configures these settings for you. These settings tell a modulator which version of software to use. Do **not** change information in the Advanced Parameters tab without first consulting contact Cisco Services. Changing this data without direction from Cisco Services can degrade system performance.

7. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to set up the connections between the BFS QAM modulator and the ASI card. Go to Setting Up Connections for a BFS QAM Modulator in an RCS.

## Setting Up BFS QAM Modulator Connections in an RCS

After you set up the basic parameters for a BFS QAM modulator, complete these steps to set up the connections between the BFS QAM modulator and the ASI card on the DNCS or RNCS/LIONN.

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this QAM modulator.
2. If not already selected, click to select the **Input Port** option in the **QAM Name** area.
3. In the **Connect To** area, click the **Headend Name** arrow and select the headend in which the device that feeds the BFS QAM resides.
4. Click the **Device Type** arrow and select **ASI**.
5. Continue defining connections to the ASI card by entering the following information in any order.
   - Click the **Device Name** arrow and select the name you gave the ASI card when you defined it earlier as an MPEG source.
   - Click the **Port Number** arrow and select the port number on the ASI card that is connected to this BFS QAM modulator.
6. Click **Apply**. The system saves this information into the DNCS database.
7. Your next step is to activate the BFS QAM modulator. Go to Activating a BFS QAM Modulator in an RCS.

## Activating a BFS QAM Modulator in an RCS

After you set up the connections between the BFS QAM modulator and the device that feeds it, complete these steps to activate the BFS QAM modulator.

**Note:** You can activate a QAM modulator only after all parameters for the QAM modulator have been saved to the DNCS database, and only after the QAM modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1. On the Set Up QAM window, click the **Basic Parameters** tab. The Basic Parameters window opens.
2. At the **Administrative State** field, click the **Online** option.
3. If this BFS QAM modulator will also function as a Distinguished QAM modulator, verify that **Allow SI** is set to **No**. If it is not, click and select **No**.
4. Click **Save**. The system saves the QAM modulator information in the DNCS database and closes the Set Up QAM window. The QAM List window updates to include the new QAM modulator.
5. Add the new BFS QAM modulator to your network map.
6. Do you need to add another BFS QAM modulator to your RCS?
   - If **yes**, go back to Setting Up BFS QAM Modulator Basic Parameters in an RCS.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console. Go to Verify the VASP Configuration in an RCS.

# Verify the VASP Configuration in an RCS

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

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow another procedure to verify your VASP configuration.

After you add a BFS QAM modulator to the DNCS and to each RNCS/LIONN, verify that your Value Added Service Provider (VASP) entries are correct. VASP is a generic term for an entity that provides a service or functionality to elements of a Digital Broadband Delivery Service (DBDS).

For a DBDS to function properly, specific VASP entries for the central site and for each remote site must be defined on the DNCS. In addition, to these standard VASP entries, each site may have additional VASP entries to support any non-standard services that the site offers.

For example, if one of your remote sites offers interactive services, such as VOD, you must have one VASP entry for each VOD server installed in that site. Without these VASP entries, the RNCS/LIONN cannot process signals to and from the VOD servers installed at the site.

## VASP Entries Required for the Central Site

The following VASP entries are required for any central site in an RCS. These entries are created automatically by the system when your DBDS was initially installed:

- **Broadcast File System** Used by the BFS when starting its sessions
- **CPSession UI** Used by the user interface (UI) in the session setup request
- **GEARServer** Used for EAS activity
- **HCTM Server** Used for DHCT management
- **Message Server** Used by the system when sending pass-thru messages (this VASP never starts sessions)
- **MMM Server** Used for EAS activity
- **OSM Server** Used for DHCT operating system (OS) sessions

**Important:** Depending on the services your network offers, there may be more VASP entries listed in the DNCS. However, the entries listed above **must** be present **and** in service for the DBDS to function properly. In addition, if you are offering VOD, you must add one VASP entry for each VOD server installed in your central site. Without a VASP entry, the DNCS is unable to process signals to and from the VOD server.

## VASP Entry Required for Remote Sites

One **mmmRemote** VASP entry is required for each RNCS/LIONN in an RCS. This entry is used for EAS activity at a remote site and is created manually when an RNCS/LIONN site is first set up.

Occasionally, this entry may be missing or not in service. Therefore, it is a good idea to verify your VASP configuration whenever you make changes to your network.

**Important:** Depending on the services your network offers, there may be more VASP entries listed in an RNCS/LIONN. However, the mmmRemote entry **must** be present **and** in service for the DBDS to function properly. In addition, if a remote site offers VOD, you must add one VASP entry for each VOD server installed in the remote site. Without a VASP entry, an RNCS/LIONN is unable to process signals to and from the VOD server.

## VASP Entries Required for the Central Site

The following VASP entries are required for any central site in an RCS. These entries are created automatically by the system when your DBDS was initially installed:

- **Broadcast File System** Used by the BFS when starting its sessions
- **CFSession UI** Used by the user interface (UI) in the session setup request
- **GEARServer** Used for EAS activity
- **HCTM Server** Used for DHCT management
- **Message Server** Used by the system when sending pass-thru messages (this VASP never starts sessions)
- **MMM Server** Used for EAS activity
- **OSM Server** Used for DHCT operating system (OS) sessions

**Important:** Depending on the services your network offers, there may be more VASP entries listed in the DNCS. However, the entries listed above **must** be present **and** in service for the DBDS to function properly. In addition, if you are offering VOD, you must add one VASP entry for each VOD server installed in your central site. Without a VASP entry, the DNCS is unable to process signals to and from the VOD server.

# Verify the VASP Configuration in an RCS

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

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow another procedure to verify your VASP configuration.

After you add a BFS QAM modulator to the DNCS and to each RNCS/LIONN, verify that your Value Added Service Provider (VASP) entries are correct. VASP is a generic term for an entity that provides a service or functionality to elements of a Digital Broadband Delivery Service (DBDS).

For a DBDS to function properly, specific VASP entries for the central site and for each remote site must be defined on the DNCS. In addition, to these standard VASP entries, each site may have additional VASP entries to support any non-standard services that the site offers.

For example, if one of your remote sites offers interactive services, such as VOD, you must have one VASP entry for each VOD server installed in that site. Without these VASP entries, the RNCS/LIONN cannot process signals to and from the VOD servers installed at the site.

## VASP Entries Required for the Central Site

The following VASP entries are required for any central site in an RCS. These entries are created automatically by the system when your DBDS was initially installed:

- **Broadcast File System** — Used by the BFS when starting its sessions
- **CFSession UI** — Used by the user interface (UI) in the session setup request
- **GEARServer** — Used for EAS activity
- **HCTM Server** — Used for DHCT management
- **Message Server** — Used by the system when sending pass-thru messages (this VASP never starts sessions)
- **MMM Server** — Used for EAS activity
- **OSM Server** — Used for DHCT operating system (OS) sessions

**Important:** Depending on the services your network offers, there may be more VASP entries listed in the DNCS. However, the entries listed above **must** be present **and** in service for the DBDS to function properly. In addition, if you are offering VOD, you must add one VASP entry for each VOD server installed in your central site. Without a VASP entry, the DNCS is unable to process signals to and from the VOD server.

## VASP Entry Required for Remote Sites

One **mmmRemote** VASP entry is required for each RNCS/LIONN in an RCS. This entry is used for EAS activity at a remote site and is created manually when an RNCS/LIONN site is first set up.

Occasionally, this entry may be missing or not in service. Therefore, it is a good idea to verify your VASP configuration whenever you make changes to your network.

**Important:** Depending on the services your network offers, there may be more VASP entries listed in an RNCS/LIONN. However, the mmmRemote entry **must** be present **and** in service for the DBDS to function properly. In addition, if a remote site offers VOD, you must add one VASP entry for each VOD server installed in the remote site. Without a VASP entry, an RNCS/LIONN is unable to process signals to and from the VOD server.

## Verifying the VASP Configuration in an RCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Verify that the following VASP entries appear as shown in the appropriate VASP List window and that they show a status of **In Service**.

| VASP Entry Name | IP Address | Status | Site ID |
|---|---|---|---|
| Broadcast File System | 10.253.0.1 | In Service | 1 |
| CFSession UI | 10.253.0.1 | In Service | 1 |
| GEARServer | 10.253.0.1 | In Service | 1 |
| HCTM Server | 10.253.0.1 | In Service | 1 |
| Message Server | 10.253.0.1 | In Service | 1 |
| MMM Server | 10.253.0.1 | In Service | 1 |
| OSM Server | 10.253.0.1 | In Service | 1 |
| mmmRemote | 172.20.0.201 | In Service | 2 |

5. **Notes:**
   - The VASP entries shown in this table are the system default values. Your IP address entries might be different based on your system configuration. Check your network map to verify the IP addresses for your VASP entries.
   - Site ID 1 in this table represents the Site ID of the central site.
   - Site ID 2 in this table represents the Site ID of a remote site.
6. Do all of the VASP entries shown in step 4 appear in the VASP List window, does an mmmRemote entry show for each remote site in your RCS, and do all entries show a status of In Service?
   - If **yes**, go to step 6.
   - If **no**, go to step 7.
7. Do you need to add any VASP entries, such as for a VOD server?
   - If **yes**, go to Add a VASP Entry to Your RCS.
   - If **no**, go to step 8.
8. Take your next step based on the information in your VASP List window:
   - If entries are missing from your VASP List, add the missing entries. Go to Adding a VASP Entry to Your RCS.
   - If any entries do not show a status of In Service, activate these VASP entries. Go to Activating a VASP Entry in Your RCS.
9. Click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.
10. Are you setting up the elements of your system for the first time?

- If **yes**, go to Setting Up Two-Way Communication.
- If **no**, add the new VASP entry information to your network map.

# Add a VASP Entry to Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > File > New**

Complete these steps if you need to add a VASP entry to your RCS. For more descriptive information about VASP entries, refer to Verify the VASP Configuration in an RCS.

**Note:** Systems that do not use an RCS use a different method to add a VASP entry to a non-RCS system.

**Important:** If you are offering VOD services, you must add one VASP entry for each VOD server installed in your network. Without a VASP entry, a DNCS or RNCS/LIONN is unable to process signals to and from the server.

**You Need to Know**

Before You Begin

Before you begin, you must have the IP address of the server associated with the VASP entry you are adding (from your system administrator).

## Adding a VASP Entry to Your RCS

1. On the VASP List window, click **File > New**. The Set Up VASP window opens.
2. Complete the fields on the screen as described in RCS VASP Entry Settings.

Use the following fields when you manage a VASP entry in an RCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you are adding.<br>Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry. |
| Name | The name of this VASP entry.<br>You can use up to 80 alphanumeric characters. Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br>**Example:** A name of VODhub1Q43 would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br>Be careful to properly place the dots (.) between numbers. If you are adding a VASP entry for the mmmRemote server, use the IP address for the RNCS/LIONN.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated.<br>Select **In Service** to activate this VASP. |
| Site ID | The site for which this VASP provides service. |

3. Click **Save**. The system saves the VASP entry information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.
4. Do you need to add another VASP entry?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.
5. Are you setting up the elements of your system for the first time?
   - If **yes**, you are ready to set up the elements that provide two-way communication. Go to Setting Up Two-Way Communication.
   - If **no**, add the new VASP entry information to your network map.

## Activating a VASP Entry

Occasionally, a VASP entry is taken out of service, such as during maintenance or when you change VOD server brands (for example, replacing an nCube VOD server with a Concurrent VOD server). Use this procedure to place a VASP entry back into service that had been previously taken out of service.

1. On the VASP List window, click to select the VASP you need to place in service.
2. Click **File > Open**. The Set Up VASP window for that VASP opens.
3. Click the **In Service** option.
4. Click **Save**. The system places the VASP into service. The Set Up VASP window closes and the VASP List window updates to show the changed status for this VASP.
5. Do you need to activate another VASP?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.

# Make Changes to RCS Elements

After your network elements have been set up, you can make any of the following changes to your RCS, and update your network map to help you manage changes.

## Change RCS Elements

BFS QAM Modulator
CableCARD Module
DHCT
GoQAM IF Modulator
GoQAM RF Modulator
GQAM Modulator
MPEG BFS Source
MPEG Content Source
MQAM Modulator
Node Set
QAM Modulators
QPSK Demodulator
QPSK Modulator
RCS Headend
RCS Hub
RCS VASP Entries
Site
UpConverter

## Modify a Site in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary**

**Important:** Follow this procedure only if you use an RCS.

If you are using an RCS, you can modify any of the following parameters of an existing site:

- Site IP Address (If modifying the site IP address, update the mmmRemote VASP entry for this site.)
- Site MAC Address
- BFS MAC Address

To modify any other parameters of a site, first delete the site and then add the site again.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. To modify any of the following fields, click in each field and type the new information.
   - Site IP Address
   - Site MAC Address
   - BFS MAC Address

   **Note:** To modify the **Site Name** or **Site ID**, first delete the site and then add the site again.

   Tip: When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
5. Click **Save**. The system displays the message "Site Data update completed."
6. Click **OK**. The system saves your changes and displays the new settings in the Site Summary window.
7. Do you need to modify another site?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, go to step 8.
8. Have you made any changes to remote sites?
   - If **yes**, for each remote site you have made changes to, stop and restart the processes that run on the RNCS/LIONN of each remote site.
   - If **no**, go to step 9.
9. Did you change the site ID?
   - If **yes**, update the mmmRemote VASP entry for this site. To change a Site ID, first delete the VASP entry and then add the VASP entry to your RCS again using the new site ID.
   - If **no**, click **Exit** to close the Site Summary window.
10. Update your network map to reflect these changes.

## Modifying a Billing Reference in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Billing References**

**Important:** Follow this procedure only if you use an RCS.

To modify parameters of a billing reference, such as the billing ID and site name, first delete the billing reference and then add the billing reference again, using new information.

## Modify a Headend in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Headend Summary**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to modify a headend in your system.

After a headend has been saved in the DNCS, you can modify all parameters for that headend except for its ID. To change the Headend ID, delete the headend and then add the headend again.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Headends**. The Headends Summary window opens and lists the headends for all sites.
5. Modify any of the following parameters:
   - Headend Name
   - Site Name

   **Note:** To modify the **Headend ID**, first delete the headend and then add the headend again.
6. Click **Save**. The system displays the message "Headend save completed."
7. Click **OK**. The system saves your changes and displays the new settings in the Headend Summary window.
8. Do you need to modify another headend?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Exit** to close the Headend Summary window.

## Modify a Hub in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Site Summary window > [Make Changes] > Save > OK**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to modify a hub in your system.

After a hub has been saved in the DNCS, you can modify all parameters for that hub except for the Hub ID. To change the Hub ID, delete the hub and then add the hub again.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Hubs**. The Hubs Summary window opens and lists the hubs for all headends.
5. Modify any of the following parameters:
   - Hub Name
   - Timezone
   - DST Zone ID (For an explanation of these values, see Daylight Saving Time Rules Settings. For more information on DST rules, see Configure Daylight Saving Time Rules Window.)

   Use the following fields when you manage DST rule in the DNCS.

| Field | Description |
|---|---|
| **Note:** Settings in the first area of the window define how DST is observed in a particular DST Zone ID. | |
| Daylight Saving Time Zone ID | The IDs of the DST zones that the DNCS uses:<br>▪ **US** - United States of America.<br>▪ **UK** - United Kingdom of Great Britain and Northern Ireland.<br>▪ **Europe** - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland.<br>▪ **Australia** - All states and territories in the Commonwealth of Australia.<br>▪ **Local DST Zone** - Used for all other countries and territories, except as noted below. |
| **What if my country or territory isn't listed?**<br><br>If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK ), select that territory from the DST Zone ID list. For example, if you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province.<br><br>If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID. | |
| Daylight Saving Time Offset (minutes) | The time shift (in minutes) relative to standard time.<br><br>**Example:** If daylight saving time is one hour ahead, you would enter **60** in this |

| | |
|---|---|
| | field. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID.<br>This field accepts any positive number from 0 to 1439. |
| Effective Year | The year the DST rule becomes effective |
| Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied in that DST Zone ID.<br>**Important:** All DST rules except those created for the Australia Zone ID and Local Zone ID must be applied to the same year. | |
| Start: Month | The month the DST rule becomes effective |
| Start: Day | The day the DST rule becomes effective |
| Start: Day Rank in Month | The day of the month that the DST rule becomes effective.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Start: Hour | The hour the DST rule becomes effective. |
| Start: Minute | The number of minutes after the Start Hour that the DST rule becomes effective. |
| End: Month | The month the DST rule ends. |
| End: Day | The day the DST rule ends. |
| End: Day Rank in Month | The day of the month that the DST rule ends.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| End: Hour | The hour the DST rule ends. |
| End: Minute | The number of minutes after the End Hour that the DST rule ends. |
| Settings in the **Broadcast Start** area of the window define when the DNCS broadcasts this rule to DHCTs that reside in the DST Zone ID.<br>**Important:** Broadcast Start Time can begin no more than 30 days before the start of the DST rule. | |
| Year | The year that the DNCS begins broadcasting this rule to DHCTs. |
| Month | The month that the DNCS begins broadcasting this rule to DHCTs. |
| Day | The day that the DNCS begins broadcasting this rule to DHCTs. |
| Day Rank in Month | The day of the month that the DNCS begins broadcasting this rule to DHCTs.<br>**Example:** The first, second, third, fourth, or last Sunday of the month. |
| Hour | The hour that the DNCS begins broadcasting this rule to DHCTs |
| Minute | The number of minutes after the Start Hour that the DNCS begins broadcasting this rule to DHCTs |

6. When you finish making changes, click **Save**. A confirmation message opens.
7. Click **OK**. The Hub Summary window updates to include the new hub information. DHCTs receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a DHCT causes it to apply updates immediately.
8. Update your network map to reflect these changes.
9. Do you need to modify another hub by changing any of the parameters listed earlier in step 4?
   - If **yes**, repeat this procedure from step 5.

- If **no**, click **Exit** to close the Hub Summary window.

## Modify an RCS VASP Entry

**Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Open**

After a VASP entry has been saved in the DNCS, you can modify only the following parameters:

- The name of the VASP entry
- The status of the VASP entry (In Service or Out of Service)

**Important:** To change any other parameters, you must delete the VASP entry, and then re-add it to the DNCS, using the new information.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Click once on the row containing the VASP entry you want to modify.
5. Click **File > Open**. The Set Up VASP window opens for the VASP entry you selected.
6. To change the name of this VASP entry, click in the **Name** field and change the name as desired. You can use up to 80 alphanumeric characters.

   **Note:** We recommend that you establish a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.

   **Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43.

7. To change the status of this VASP entry from **In Service** to **Out of Service**, or vice versa, click the desired option so that is selected (**yellow**).
8. When you finish making changes, click **Save**. The system saves the new VASP information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP information.
9. Update your network map to reflect these changes.
10. Do you need to modify another VASP entry?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.

## Modify an MPEG BFS Source

**Important:** Do not attempt to modify or delete an MPEG BFS source without assistance from us. Certain BFS modifications may degrade system performance. For this reason, always consult us before making changes to an MPEG BFS source.

## Modify a BFS QAM Modulator

**Important:** Do not attempt to modify or delete a BFS QAM modulator without assistance from Cisco Services. Certain BFS modifications may degrade system performance. For this reason, always consult Cisco Services before making changes to a BFS QAM modulator.

# Delete RCS Elements

## Delete RCS Elements

| | | |
|---|---|---|
| BFS QAM Modulator | MPEG BFS Source | QPSK Modulator |
| CableCARD Module | MPEG Content Source | RCS Headend |
| DHCT | MQAM Modulator | RCS Hub |
| GoQAM IF Modulator | Node Set | RCS VASP Entries |
| GoQAM RF Modulator | QAM Modulators | Site |
| GQAM Modulator | QPSK Demodulator | UpConverter |

# Delete a Site in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Delete Selected Site**

**Important:** Follow this procedure only if you use an RCS.

You may want to delete a site because you are no longer using it, or because you need to modify its name or ID.

### Deleting a Site in Your RCS

1. Are there any headends associated with this site?
   - If **yes**, delete those headends first. Go to Delete a Headend in Your RCS. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **RNCS Sites**. The Site Summary window opens.
5. Click **Select** for the site that you want to delete.
6. Click **Delete Selected Site**. The system displays a question prompting you to confirm that you wish to delete this site.
7. Click **OK**. The system removes the site from the database and displays the updated Site Summary window, which no longer lists the site.
8. Do you need to delete another site?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Exit** to close the Site Summary window.

## Delete a Site in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Delete Selected Site**

**Important:** Follow this procedure only if you use an RCS.

You may want to delete a site because you are no longer using it, or because you need to modify its name or ID.

### Deleting a Site in Your RCS

1. Are there any headends associated with this site?
   - If **yes**, delete those headends first. Go to Delete a Headend in Your RCS. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **RNCS Sites**. The Site Summary window opens.
5. Click **Select** for the site that you want to delete.
6. Click **Delete Selected Site**. The system displays a question prompting you to confirm that you wish to delete this site.
7. Click **OK**. The system removes the site from the database and displays the updated Site Summary window, which no longer lists the site.
8. Do you need to delete another site?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Exit** to close the Site Summary window.

## Delete a Billing Reference From Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Billing References > Delete Selected Billing**

**Important:** Follow this procedure only if you use an RCS.

### Deleting a Billing Reference From Your RCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Billing References**. The Billing Reference Summary opens and lists any billing IDs have been assigned to a site.
5. Click **Select** for the billing reference that you want to delete.
6. Click **Delete Selected Billing**. The system displays a question prompting you to confirm that you wish to delete the billing reference for this site.
7. Click **OK**. The system removes the billing reference from the database and displays the updated Billing Reference Summary window, which no longer lists the billing reference.
8. Do you need to delete another billing reference?
    - If **yes**, repeat this procedure from step 5.
    - If **no**, click **Exit** to close the Site Summary window.

## Delete a Billing Reference From Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS > Site Summary > Billing References > Delete Selected Billing**

**Important:** Follow this procedure only if you use an RCS.

### Deleting a Billing Reference From Your RCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Billing References**. The Billing Reference Summary opens and lists any billing IDs have been assigned to a site.
5. Click **Select** for the billing reference that you want to delete.
6. Click **Delete Selected Billing**. The system displays a question prompting you to confirm that you wish to delete the billing reference for this site.
7. Click **OK**. The system removes the billing reference from the database and displays the updated Billing Reference Summary window, which no longer lists the billing reference.
8. Do you need to delete another billing reference?
    - If **yes**, repeat this procedure from step 5.
    - If **no**, click **Exit** to close the Site Summary window.

# Delete a Headend in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Headend Summary > Delete Selected Headend**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to delete a headend in your system.

You may want to delete a headend because you are no long using it, or because you need to modify its ID.

### You Need to Know

Before You Begin

Before you can delete a headend, you must delete all of the network elements that are associated with it. In addition, make sure you have your network map available.

### Deleting a Headend in Your RCS

1. Are there any hubs associated with this headend?
   - If **yes**, delete those hubs first. Go to Deleting a Hub in Your RCS. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **RNCS Sites**. The Site Summary window opens.
5. Click **Headends**. The Headends Summary window opens and lists the headends for all sites.
6. Click **Select** for the headend that you want to delete.
7. Click **Delete Selected Headend**. The system displays a question prompting you to confirm that you wish to delete this headend.
8. Click **OK**. The system removes the headend from the database and displays the updated Headend Summary window, which no longer lists the headend.
9. Delete the headend from your network map.
10. Do you need to delete another headend?
    - If **yes**, repeat this procedure from step 6.
    - If **no**, click **Exit** to close the Headend Summary window.

# Delete a Headend in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Headend Summary > Delete Selected Headend**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to delete a headend in your system.

You may want to delete a headend because you are no long using it, or because you need to modify its ID.

### You Need to Know

Before You Begin

Before you can delete a headend, you must delete all of the network elements that are associated with it. In addition, make sure you have your network map available.

### Deleting a Headend in Your RCS

1. Are there any hubs associated with this headend?
   - If **yes**, delete those hubs first. Go to Deleting a Hub in Your RCS. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **RNCS Sites**. The Site Summary window opens.
5. Click **Headends**. The Headends Summary window opens and lists the headends for all sites.
6. Click **Select** for the headend that you want to delete.
7. Click **Delete Selected Headend**. The system displays a question prompting you to confirm that you wish to delete this headend.
8. Click **OK**. The system removes the headend from the database and displays the updated Headend Summary window, which no longer lists the headend.
9. Delete the headend from your network map.
10. Do you need to delete another headend?
    - If **yes**, repeat this procedure from step 6.
    - If **no**, click **Exit** to close the Headend Summary window.

## Delete a Hub in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Hubs > Delete Selected Hub**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to delete a hub in your system.

You may want to delete a hub because you are no longer using it, or because you need to modify its ID or its headend.

### You Need to Know

Before You Begin

Before you can delete a hub, you must delete all of the network elements that are associated with it. In addition, make sure you have your network map available.

### Deleting a Hub in Your RCS

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to Deleting a Node Set. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **RNCS Sites**. The Site Summary window opens.
5. Click **Hubs**. The Hubs Summary window opens and lists the hubs for all headends.
6. Click **Select** for the hub that you want to delete.
7. Click **Delete Selected Hub**. The system displays a question prompting you to confirm that you wish to delete this hub.
8. Click **OK**. The system removes the hub from the database and displays the updated Hub Summary window, which no longer lists the hub.
9. Delete the hub from your network map.
10. Do you need to delete another hub?
    - If **yes**, repeat this procedure from step 6.
    - If **no**, click **Exit** to close the Hub Summary window.

## Delete an MPEG BFS Source

**Important:** Do not attempt to modify or delete an MPEG BFS source without assistance from us. Certain BFS modifications may degrade system performance. For this reason, always consult us before making changes to an MPEG BFS source.

### Deleting a Hub in Your RCS

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to Deleting a Node Set. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **RNCS Sites**. The Site Summary window opens.
5. Click **Hubs**. The Hubs Summary window opens and lists the hubs for all headends.
6. Click **Select** for the hub that you want to delete.
7. Click **Delete Selected Hub**. The system displays a question prompting you to confirm that you wish to delete this hub.
8. Click **OK**. The system removes the hub from the database and displays the updated Hub Summary window, which no longer lists the hub.
9. Delete the hub from your network map.
10. Do you need to delete another hub?
    - If **yes**, repeat this procedure from step 6.
    - If **no**, click **Exit** to close the Hub Summary window.

## Delete a Hub in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Site Summary > Hubs > Delete Selected Hub**

**Important:** This procedure can be used only for an RCS. If you do not use an RCS, follow a different procedure to delete a hub in your system.

You may want to delete a hub because you are no longer using it, or because you need to modify its ID or its headend.

### You Need to Know

Before You Begin

Before you can delete a hub, you must delete all of the network elements that are associated with it. In addition, make sure you have your network map available.

### Deleting a Hub in Your RCS

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to Deleting a Node Set. When finished, return to this procedure.
   - If **no**, go to step 2.
1. On the DNCS Administrative Console, click the **DNCS** tab.
1. Click the **System Provisioning** tab.
1. Click **RNCS Sites**. The Site Summary window opens.
1. Click **Hubs**. The Hubs Summary window opens and lists the hubs for all headends.
1. Click **Select** for the hub that you want to delete.
1. Click **Delete Selected Hub**. The system displays a question prompting you to confirm that you wish to delete this hub.
1. Click **OK**. The system removes the hub from the database and displays the updated Hub Summary window, which no longer lists the hub.
1. Delete the hub from your network map.
1. Do you need to delete another hub?
   - If **yes**, repeat this procedure from step 6.
   - If **no**, click **Exit** to close the Hub Summary window.

## Delete an MPEG BFS Source

**Important:** Do not attempt to modify or delete an MPEG BFS source without assistance from us. Certain BFS modifications may degrade system performance. For this reason, always consult us before making changes to an MPEG BFS source.

## Delete a BFS QAM Modulator

**Important:** Do not attempt to modify or delete a BFS QAM modulator without assistance from Cisco Services. Certain BFS modifications may degrade system performance. For this reason, always consult Cisco Services before making changes to a BFS QAM modulator.

# Manage a Digital Emergency Alert System

## Introduction

This section provides a brief overview of a digital EAS and how our DNCS helps operators comply with the FCC EAS mandate.

Overview of the Digital Emergency Alert System

# Overview of the Digital Emergency Alert System

**Warning: Only the FCC, National Weather Service, and local weather authorities are authorized to broadcast Emergency Alert Messages (EAMs). As a system operator, you can test the Emergency Alert System (EAS). However, you cannot generate an EAM yourself. In addition, do not modify any of the Emergency Alert System (EAS) settings in the DNCS unless you are specifically instructed to do so by the Federal Communications Commission (FCC), National Weather Service, local weather authority, or us. Otherwise, you could cause the EAS to perform improperly or not at all.**

The following topics provide a brief overview of a digital EAS and how our DNCS helps service providers comply with this FCC mandate:

- EAS in a Typical DBDS describes how the digital EAS functions in a DBDS that does not use a Regional Control System (RCS).
- EAS in the Central RCS Site describes how the digital EAS functions on the DNCS in the central site of an RCS.
- EAS in a Remote RCS Site describes how the digital EAS functions on the RNCS/LIONN in a remote site of an RCS.

# Manage a Digital Emergency Alert System

## Introduction

This section provides a brief overview of a digital EAS and how our DNCS helps operators comply with the FCC EAS mandate.

Overview of the Digital Emergency Alert System

# Overview of the Digital Emergency Alert System

**Warning: Only the FCC, National Weather Service, and local weather authorities are authorized to broadcast Emergency Alert Messages (EAMs). As a system operator, you can test the Emergency Alert System (EAS). However, you cannot generate an EAM yourself. In addition, do not modify any of the Emergency Alert System (EAS) settings in the DNCS unless you are specifically instructed to do so by the Federal Communications Commission (FCC), National Weather Service, local weather authority, or us. Otherwise, you could cause the EAS to perform improperly or not at all.**

The following topics provide a brief overview of a digital EAS and how our DNCS helps service providers comply with this FCC mandate:

- EAS in a Typical DBDS describes how the digital EAS functions in a DBDS that does not use a Regional Control System (RCS).
- EAS in the Central RCS Site describes how the digital EAS functions on the DNCS in the central site of an RCS.
- EAS in a Remote RCS Site describes how the digital EAS functions on the RNCS/LIONN in a remote site of an RCS.

# Digital Emergency Alert System in a Typical DBDS

For information on configuring, maintaining, or testing the EAS in a DBDS, refer to Configuring and Troubleshooting the Digital Emergency Alert System (part number 4004455). To obtain a copy of this publication, see Printed Resources.

Because many digital systems are very large, an Emergency Alert Message could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, contact the representative who handles your account.

# Digital EAS in a DBDS Using RCS

## Digital Emergency Alert System in the Central RCS Site

**Important:** This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic Digital EAS in a Typical DBDS, describes how the digital EAS functions in a DBDS with no RCS.

In an RCS, processes that manage EAMs reside both on the DNCS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in the **central** site, the EARS process on the DNCS sends the MMMServer process an Event EAM.

For more information on how an EAM is processed at the central site, see the following illustration. When reviewing this illustration, keep in mind that the equipment that receives the EAM the RF receiver and the Emergency Alert Controller (EAC) is provided by a vendor other than us.


**Notes:**

- To compare this with how an EAM is processed at the central RCS site, see EAS in a Remote RCS Site.
- For information on configuring, maintaining, or testing an EAS in an RCS, refer to the Distributed EAS

on the Regional Control System, Configuration and Troubleshooting Guide (part number 4002342).

- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, contact the representative who handles your account.

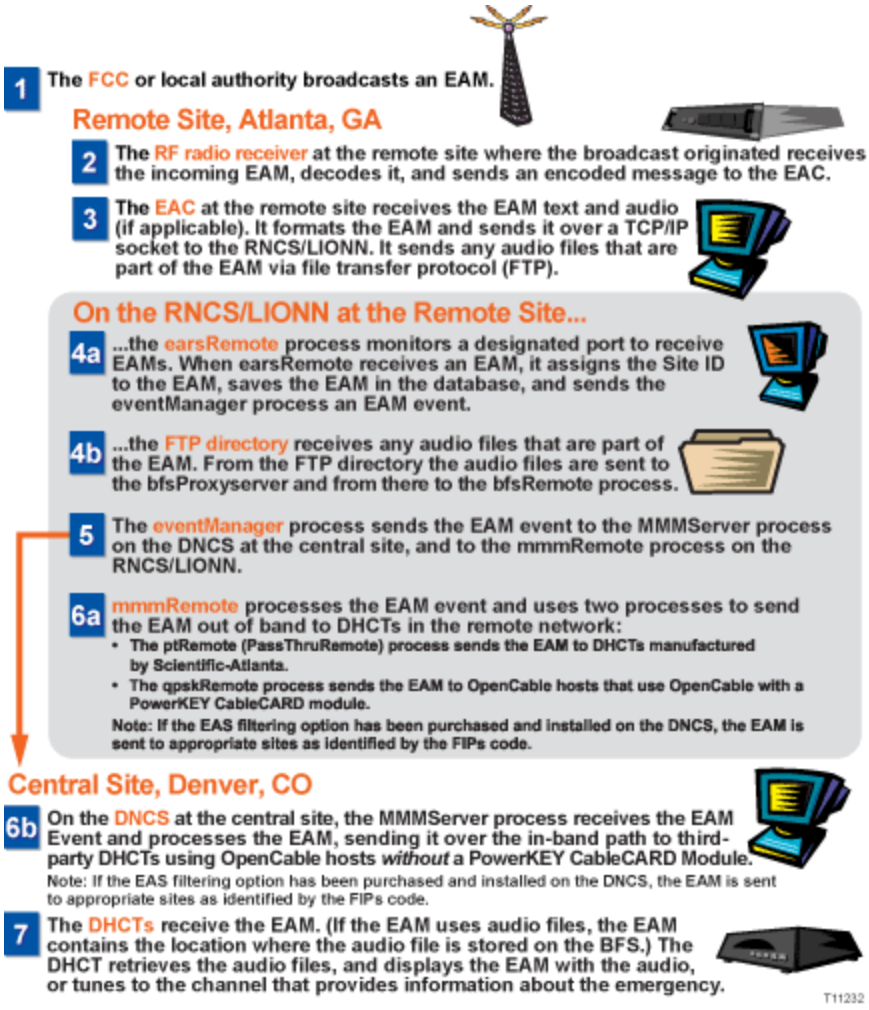
## Digital Emergency Alert System in a Remote RCS Site

**Important:** This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic Digital EAS in a Typical DBDS, describes how the digital EAS functions in a system without an RCS.

In an RCS, processes that manage Emergency Alert Messages (EAMs) reside both on the DNCS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in a **remote** site, it forwards the EAM on to a process on the RNCS/LIONN, which forwards the EAM on to the DNCS. Together, the DNCS and the RNCS/LIONN deliver the EAM to affected DHCTs in the RCS:

- EAMs processed by the DNCS are distributed to third-party DHCTs using OpenCable compliance without a PowerKEY CableCARD module.
- EAMs processed by an RNCS/LIONN are distributed to third-party DHCTs that use OpenCable compliance with a PowerKEY CableCARD module and to our DHCTs.

The following illustration explains in more detail the processes that are required to process an EAM. When reviewing this illustration, keep in mind that the equipment that receives the EAM the RF receiver and the Emergency Alert Controller (EAC) is provided by a vendor other than us.




**Notes:**

- To compare this with how an EAM is processed at the central RCS site, see EAS in the Central RCS Site .
- For information on configuring, maintaining, or testing an EAS in an RCS, refer to Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide (part number 4002342).
- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, contact the representative who handles your account.

## Digital Emergency Alert System in the Central RCS Site

**Important:** This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic Digital EAS in a Typical DBDS, describes how the digital EAS functions in a DBDS with no RCS.

In an RCS, processes that manage EAMs reside both on the DNCS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in the **central** site, the EARS process on the DNCS sends the MMMServer process an Event EAM.

For more information on how an EAM is processed at the central site, see the following illustration. When reviewing this illustration, keep in mind that the equipment that receives the EAM the RF receiver and the Emergency Alert Controller (EAC) is provided by a vendor other than us.


**Notes:**

- To compare this with how an EAM is processed at the central RCS site, see EAS in a Remote RCS Site.
- For information on configuring, maintaining, or testing an EAS in an RCS, refer to the Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide (part number 4002342).
- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, contact the representative who handles your account.

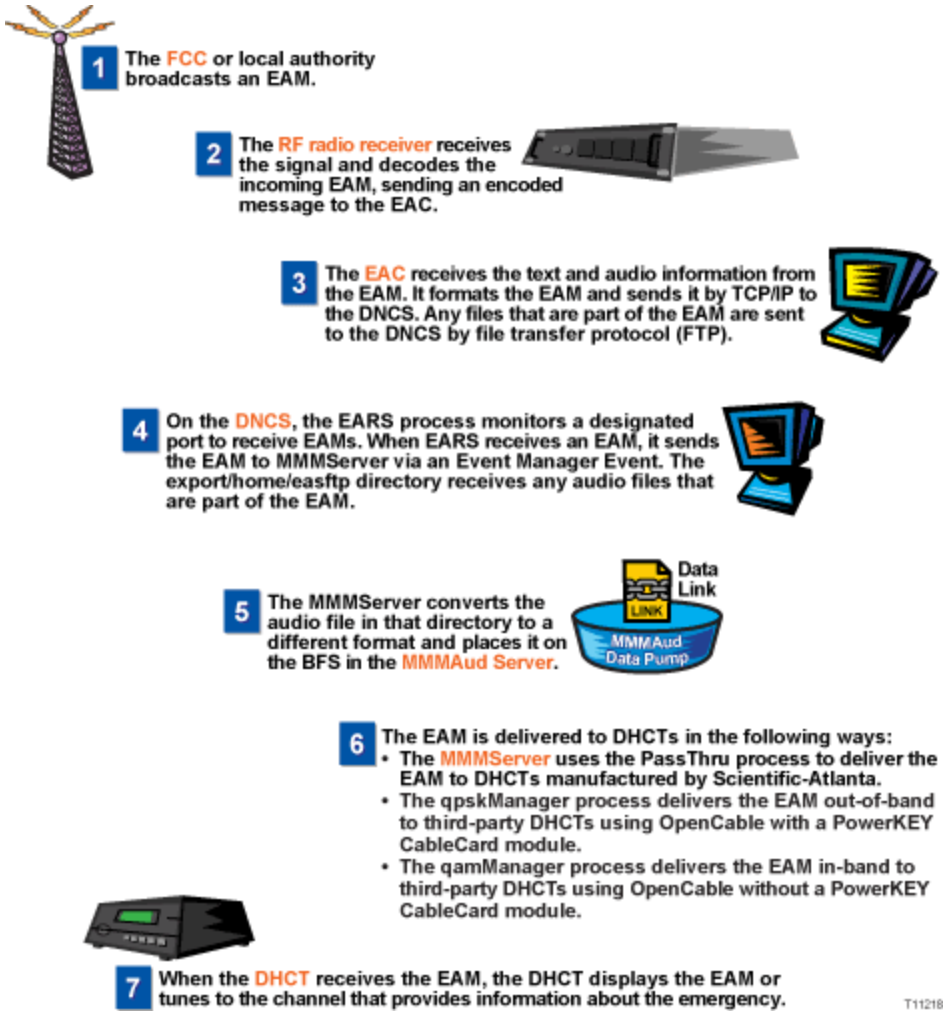
# Digital EAS in a DBDS Using RCS

## Digital Emergency Alert System in the Central RCS Site

**Important:** This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic Digital EAS in a Typical DBDS, describes how the digital EAS functions in a DBDS with no RCS.

In an RCS, processes that manage EAMs reside both on the DNCS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in the **central** site, the EARS process on the DNCS sends the MMMServer process an Event EAM.

For more information on how an EAM is processed at the central site, see the following illustration. When reviewing this illustration, keep in mind that the equipment that receives the EAM—the RF receiver and the Emergency Alert Controller (EAC)—is provided by a vendor other than us.




**Notes:**

- To compare this with how an EAM is processed at the central RCS site, see EAS in a Remote RCS Site.

- For information on configuring, maintaining, or testing an EAS in an RCS, refer to the Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide (part number 4002342).
- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, contact the representative who handles your account.

## Digital Emergency Alert System in a Remote RCS Site

**Important:** This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic Digital EAS in a Typical DBDS, describes how the digital EAS functions in a system without an RCS.

In an RCS, processes that manage Emergency Alert Messages (EAMs) reside both on the DNCS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in a **remote** site, it forwards the EAM on to a process on the RNCS/LIONN, which forwards the EAM on to the DNCS. Together, the DNCS and the RNCS/LIONN deliver the EAM to affected DHCTs in the RCS:

- EAMs processed by the DNCS are distributed to third-party DHCTs using OpenCable compliance without a PowerKEY CableCARD module.
- EAMs processed by an RNCS/LIONN are distributed to third-party DHCTs that use OpenCable compliance with a PowerKEY CableCARD module and to our DHCTs.

The following illustration explains in more detail the processes that are required to process an EAM. When reviewing this illustration, keep in mind that the equipment that receives the EAM—the RF receiver and the Emergency Alert Controller (EAC)—is provided by a vendor other than us.


**Notes:**

- To compare this with how an EAM is processed at the central RCS site, see EAS in the Central RCS Site.
- For information on configuring, maintaining, or testing an EAS in an RCS, refer to Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide (part number 4002342).
- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the DNCS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, contact the representative who handles your account.

# Suppress EAS Information on Digital Channels

**WARNING:**

**Use this feature at your own risk. It is imperative that service providers use this feature carefully so as not to suppress EAS messages on services that do not already provide EAS information. We do not take responsibility for the incorrect use of this feature.**

The EAS suppression feature allows service providers to suppress EAS information on digital channels that already provide EAS coverage to their viewers.

For example, the digital channel might carry a local over-the-air TV station that is rebroadcast through the service provider's system. The TV station provides EAS coverage through its own process.

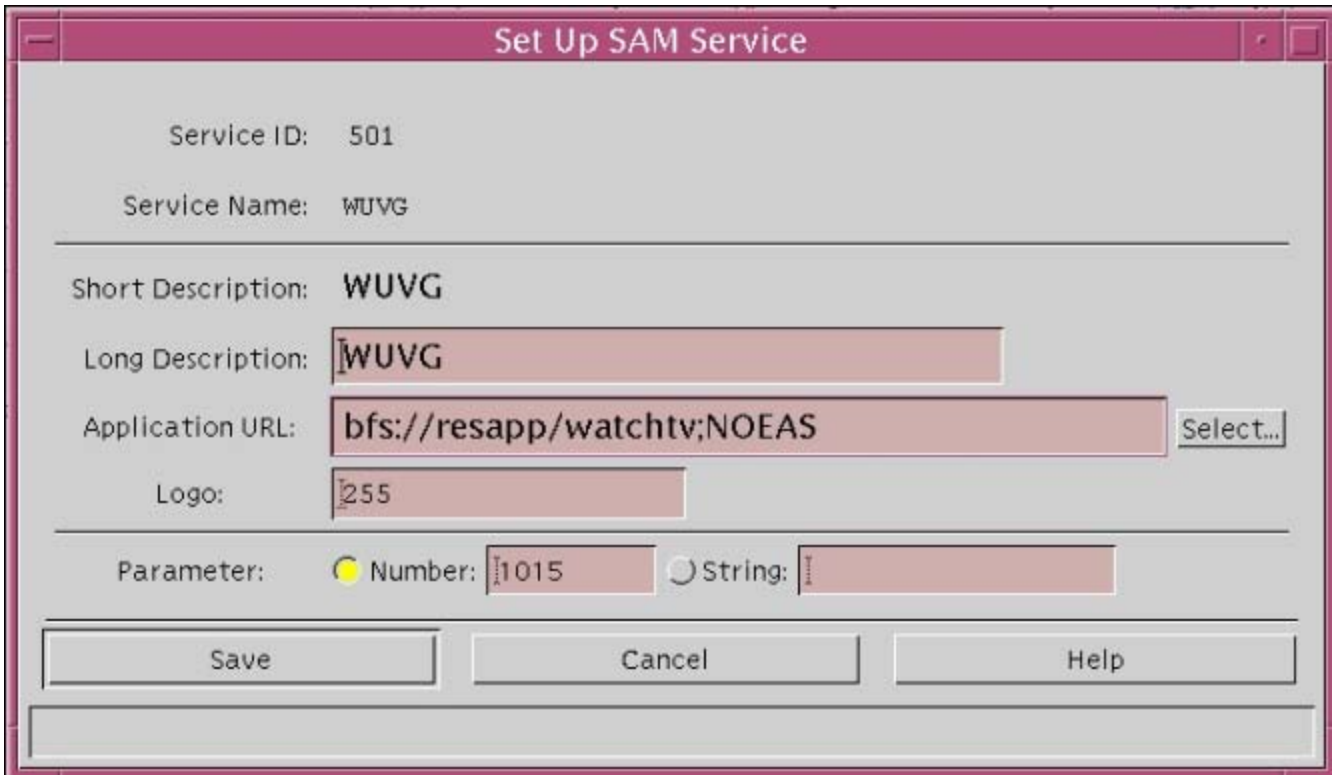
Beginning with SARA 1.60 and SARA 1.90 (DVR), a new URL modifier (**;NOEAS**) was added that allows service providers to suppress EAS on digital channels.

**Notes:**

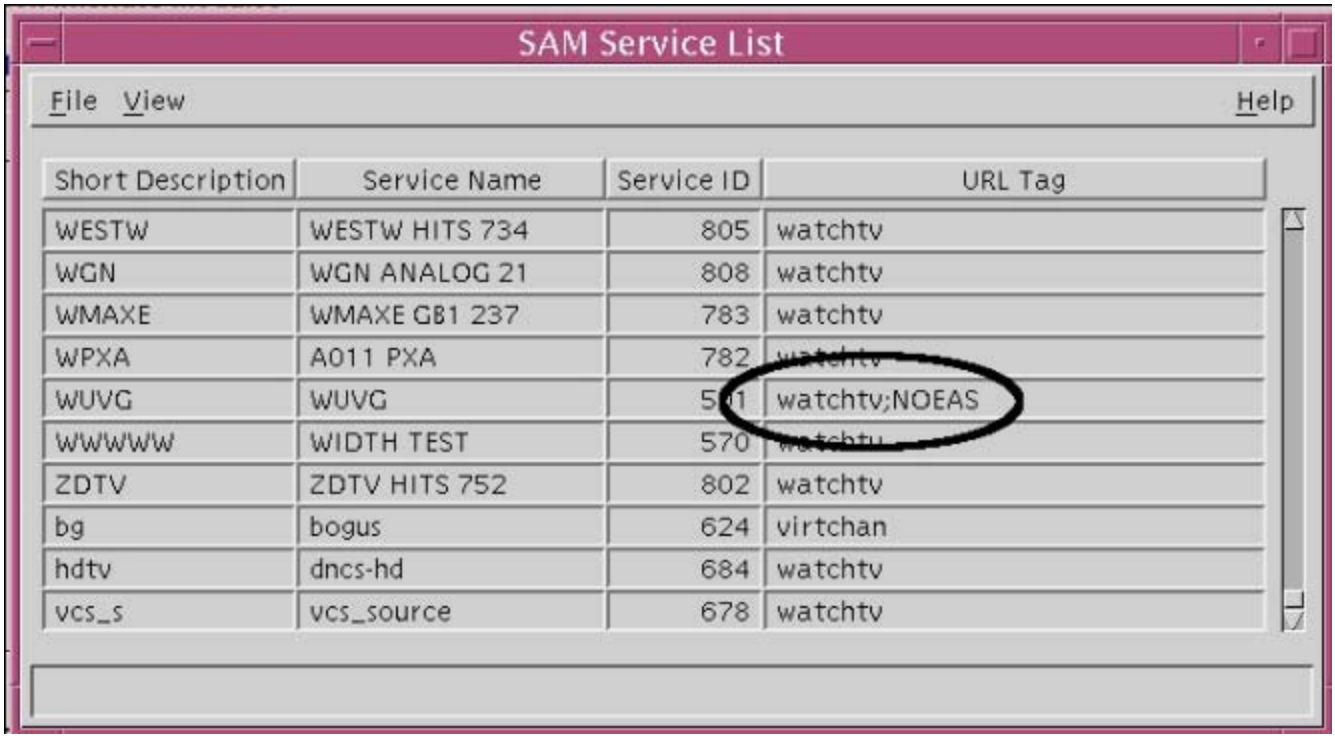
- EAS suppression is only available to systems that use SARA, our resident application.
- The URL modifier has no effect unless the set-top is tuned to a digital channel where the EAS message is received.

## Configuring a Channel to Suppress EAS Messages for System Releases Prior to SR 4.5

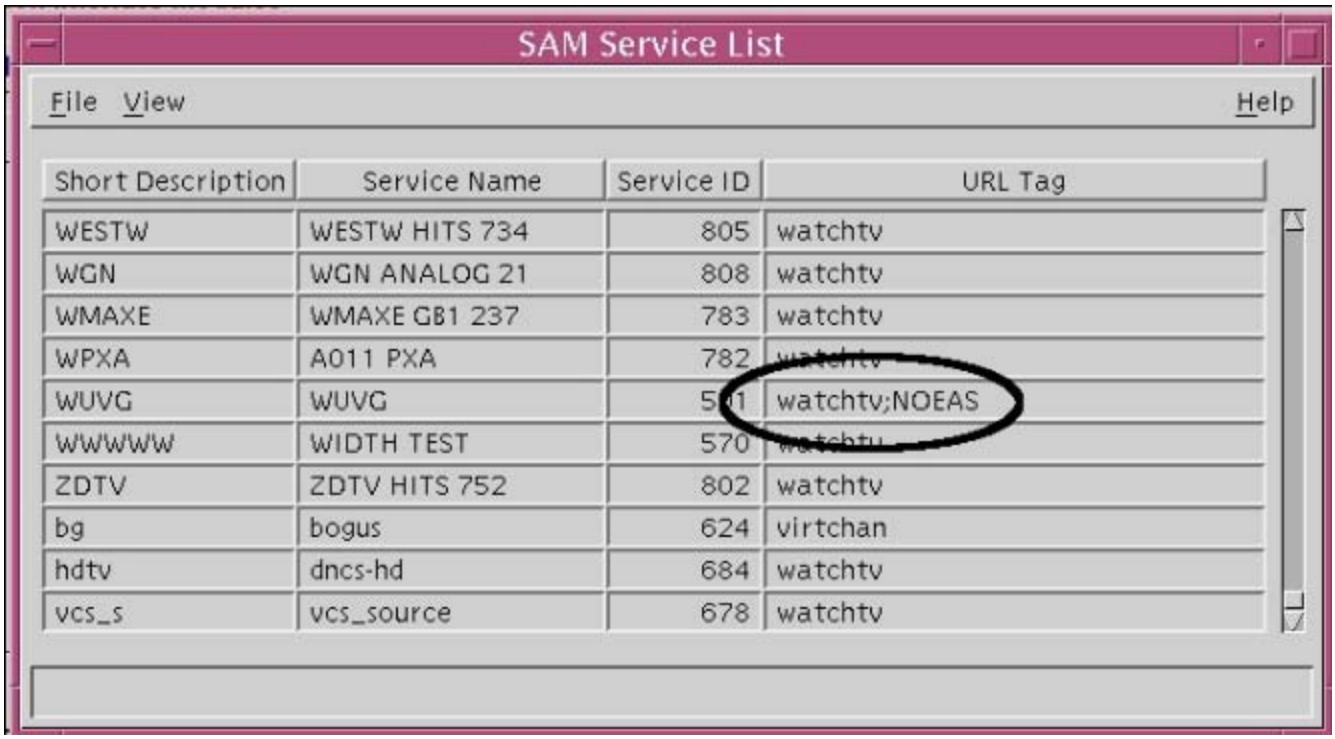
1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens.
3. Double-click the digital service you want to edit. The Set Up SAM Service window for that service opens.




4. Click in the Application URL line to place your cursor at the end of the URL statement.
5. Append the line to include **;NOEAS**.




6.Click **Save**. The Set Up SAM Service window closes. The SAM Service List shows the appended URL on the same line as the service you edited.




7.Click **File > Close** to close the SAM Service List.

# Manage a Third-Party Application

If you offer subscribers a service that is provided by a third-party application, such as video-on-demand (VOD), special tasks are required to prepare the DNCS to support the application.

If the application cannot use an existing data carousel, you will need to add an inband data carousel or an out-of-band (OOB) data carousel to the Broadcast File System (BFS). In some instances, you may need to add both an inband and OOB data carousel to the BFS. This section describes how to to add third-party applications to the DNCS and how to remove them.

Introduction

**Important:** The exact tasks that you need to complete vary according to the application itself. As a result, these procedures describe a generic process. Before attempting to follow these procedures, review them with the vendor of the application so that the vendor can assist you in tailoring these procedures to meet the needs of the application.

## What do you want to do?

- Prepare the DNCS to support the third-party application.
- Learn how to set up service the third-party application will provide to subscriber
- Remove a third-party application from the DNCS.

# Prepare the DNCS for Third-Party Applications

Before you can set up a service to provide subscribers with a third-party application, first prepare the DNCS to support the application. This section provides an overview of the tasks required to ensure that the DNCS can support a third-party application.

**You Need to Know**

Before You Begin

Make sure that you have completed the following before you begin this process:

- Install and configure any hardware required to support the application, such as servers that supply content for the third-party application.
- Load the engine for the third-party application onto the SARA Server.
- Consult with the vendor of the application to tailor these procedures to the unique needs of the application.
- Also make sure that you have the following information:
  - IP address of the server that provides this service (from the vendor of the equipment)
  - Super user (su) privileges and passwords (from your system administrator)
- Your network map

## Preparing the DNCS to Support a Third-Party Application

This section provides an overview of the process for preparing the DNCS to support a third-party application. Click any link to display step-by-step instructions for the procedures summarized here.

1. If necessary, **Add a VASP Entry to the DBDS**. If the application needs to negotiate resources with the DNCS, add a VASP entry to the DNCS so the DNCS can communicate with the device that provides third-party application data. If you determine that you need to add a VASP entry, the method you use to add the VASP depends on your system's configuration.
   - Add a VASP Entry to a Standard DBDS. If you are not using our RCS solution and you determine that the application needs to negotiate resources with the DNCS, add a VASP entry to the DNCS. A VASP entry ensures that the DNCS can communicate with the device that provides third-party application data.
   - Add a VASP Entry to Your RCS. If you are using our RCS solution, the application may also need to negotiate resources with each RNCS. If so, add a VASP entry for each RNCS so the RNCS can communicate with the device that provides the third-party application.

   **Important:** Some third-party applications use more than one device to provide data. When this is the case, you will need to add additional VASP entries so that you have one VASP entry for each device that provides data. Consult with your third-party application vendor to help you determine the number of VASP entries you need to add, if any.

2. Add Third-Party Devices to the DNCS Hosts Table (Optional) . Adding names to the DNCS hosts table allows you to type the device name, which is usually easier to remember, instead of the IP address every time you need to work with the device through the DNCS. Although this step is not required, you may find completing it is helpful when adding data carousels.

3. Consult our BFS Performance Recommendations. Our Broadcast File Server (BFS) performance recommendations can help the vendor of the third-party application decide whether a new data carousel is required for the application or if the application can use an existing data carousel. The vendor will

need to specify the number and type of carousels, names given to the carousels, the number of files placed on each carousel, and bandwidth requirements for the application.

4.Add Data Carousels to the BFS. Based on recommendations from the vendor of your third-party application, set up the BFS so that it can send third-party application data to DHCTs. Part of setting up the BFS may require that you add inband or out-of- band (OOB) data carousels (or sometimes both types of carousels) to the BFS. The BFS uses data carousels to send application data to all DHCTs in the system. Data carousels provide DHCTs with information about the third-party application:

- Add an Inband Data Carousel to the DNCS. Generally, if a fast data transfer rate is essential, using inband data carousel may be more beneficial.
- Add an Out-of-Band Carousel to the DNCS. If the third-party application requires access to data while simultaneously allowing the user to watch video, then use an OOB carousel for the application. Using an inband carousel in this situation results in the video being interrupted during data retrieval.

5.If necessary, Create a Package for the Third-Party Application (Optional). Creating a package is optional and is dependent upon how you plan to launch the third-party application (for example, via a channel). A package allows you to offer the service only to those subscribers who are authorized to receive it.

6.Register the Service With the SAM. A Service Application Manager (SAM) associates tuning information with other data that defines how the application operates. This association enables a DHCT to tune to the channel where the session belonging to the third-party application is streamed, extract necessary data, and use this information to run the application. (SAM service information is broadcast to DHCTs on data carousels that are dedicated to the SAM.)

7.Set the Method for Launching the Application. You can set up the third-party application to launch using a specific method depending on the needs of the application. For example, you may want the application to launch when a subscriber tunes to a particular channel. If so, you need to add the service for the application to appropriate channel maps.

8.If necessary, Add a Service to a Channel Map (Optional). Adding the service to the channel map is optional and is dependent upon how you plan to launch the third-party application. If you want the application to launch when a subscriber tunes to a particular channel, add the service to appropriate channel maps.

## Adding a VASP Entry

1.On the VASP List window, click **File > New**. The Set Up VASP window opens.

2.Complete the fields on the screen as described in ▸ VASP Entry Fields.

Use the following fields when you manage VASP entries in the DNCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.<br>**Example:** You might give a VASP entry associated with a VOD service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with a VOD service. |
| Name | The name of this VASP entry. You can use up to 80 alphanumeric characters. |

| | |
|---|---|
| | Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br><br>**Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br><br>Be careful to properly place the dots (.) between numbers.<br><br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated. Select **In Service** to activate this VASP. |

3. Click **Save**. The system saves the VASP entry information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.
4. Add the new VASP entry information to your network map.
5. Do you need to add another VASP entry?
   - If **yes**, repeat steps this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map. If your system uses Direct ASI, go to Setting Up Two-Way Communication.

## Preparing the DNCS to Support a Third-Party Application

This section provides an overview of the process for preparing the DNCS to support a third-party application. Click any link to display step-by-step instructions for the procedures summarized here.

1. If necessary, **Add a VASP Entry to the DBDS**. If the application needs to negotiate resources with the DNCS, add a VASP entry to the DNCS so the DNCS can communicate with the device that provides third-party application data. If you determine that you need to add a VASP entry, the method you use to add the VASP depends on your system's configuration.

    - Add a VASP Entry to a Standard DBDS. If you are not using our RCS solution and you determine that the application needs to negotiate resources with the DNCS, add a VASP entry to the DNCS. A VASP entry ensures that the DNCS can communicate with the device that provides third-party application data.
    - Add a VASP Entry to Your RCS. If you are using our RCS solution, the application may also need to negotiate resources with each RNCS. If so, add a VASP entry for each RNCS so the RNCS can communicate with the device that provides the third-party application.

**Important:** Some third-party applications use more than one device to provide data. When this is the case, you will need to add additional VASP entries so that you have one VASP entry for each device that provides data. Consult with your third-party application vendor to help you determine the number of VASP entries you need to add, if any.

2. Add Third-Party Devices to the DNCS Hosts Table (Optional) . Adding names to the DNCS hosts table allows you to type the device name, which is usually easier to remember, instead of the IP address every time you need to work with the device through the DNCS. Although this step is not required, you may find completing it is helpful when adding data carousels.

3. Consult our BFS Performance Recommendations. Our Broadcast File Server (BFS) performance recommendations can help the vendor of the third-party application decide whether a new data carousel is required for the application or if the application can use an existing data carousel. The vendor will need to specify the number and type of carousels, names given to the carousels, the number of files placed on each carousel, and bandwidth requirements for the application.

4. Add Data Carousels to the BFS. Based on recommendations from the vendor of your third-party application, set up the BFS so that it can send third-party application data to DHCTs. Part of setting up the BFS may require that you add inband or out-of- band (OOB) data carousels (or sometimes both types of carousels) to the BFS. The BFS uses data carousels to send application data to all DHCTs in the system. Data carousels provide DHCTs with information about the third-party application:

    - Add an Inband Data Carousel to the DNCS. Generally, if a fast data transfer rate is essential, using inband data carousel may be more beneficial.
    - Add an Out-of-Band Carousel to the DNCS. If the third-party application requires access to data while simultaneously allowing the user to watch video, then use an OOB carousel for the application. Using an inband carousel in this situation results in the video being interrupted during data retrieval.

5. If necessary, Create a Package for the Third-Party Application (Optional). Creating a package is optional and is dependent upon how you plan to launch the third-party application (for example, via a channel). A package allows you to offer the service only to those subscribers who are authorized to receive it.

6. Register the Service With the SAM. A Service Application Manager (SAM) associates tuning information with other data that defines how the application operates. This association enables a DHCT to tune to the channel where the session belonging to the third-party application is streamed, extract necessary data, and use this information to run the application. (SAM service information is broadcast to DHCTs on data carousels that are dedicated to the SAM.)

7. Set the Method for Launching the Application. You can set up the third-party application to launch using a specific method depending on the needs of the application. For example, you may want the application to launch when a subscriber tunes to a particular channel. If so, you need to add the service for the

application to appropriate channel maps.

8. If necessary, Add a Service to a Channel Map (Optional). Adding the service to the channel map is optional and is dependent upon how you plan to launch the third-party application. If you want the application to launch when a subscriber tunes to a particular channel, add the service to appropriate channel maps.

# Prepare the DNCS for Third-Party Applications

Before you can set up a service to provide subscribers with a third-party application, first prepare the DNCS to support the application. This section provides an overview of the tasks required to ensure that the DNCS can support a third-party application.

**You Need to Know**

Before You Begin

Make sure that you have completed the following before you begin this process:

- Install and configure any hardware required to support the application, such as servers that supply content for the third-party application.
- Load the engine for the third-party application onto the SARA Server.
- Consult with the vendor of the application to tailor these procedures to the unique needs of the application.
- Also make sure that you have the following information:
  - IP address of the server that provides this service (from the vendor of the equipment)
  - Super user (su) privileges and passwords (from your system administrator)
- Your network map

## Preparing the DNCS to Support a Third-Party Application

This section provides an overview of the process for preparing the DNCS to support a third-party application. Click any link to display step-by-step instructions for the procedures summarized here.

1. If necessary, **Add a VASP Entry to the DBDS**. If the application needs to negotiate resources with the DNCS, add a VASP entry to the DNCS so the DNCS can communicate with the device that provides third-party application data. If you determine that you need to add a VASP entry, the method you use to add the VASP depends on your system's configuration.
   - Add a VASP Entry to a Standard DBDS. If you are not using our RCS solution and you determine that the application needs to negotiate resources with the DNCS, add a VASP entry to the DNCS. A VASP entry ensures that the DNCS can communicate with the device that provides third-party application data.
   - Add a VASP Entry to Your RCS. If you are using our RCS solution, the application may also need to negotiate resources with each RNCS. If so, add a VASP entry for each RNCS so the RNCS can communicate with the device that provides the third-party application.

   **Important:** Some third-party applications use more than one device to provide data. When this is the case, you will need to add additional VASP entries so that you have one VASP entry for each device that provides data. Consult with your third-party application vendor to help you determine the number of VASP entries you need to add, if any.

1. Add Third-Party Devices to the DNCS Hosts Table (Optional) . Adding names to the DNCS hosts table allows you to type the device name, which is usually easier to remember, instead of the IP address every time you need to work with the device through the DNCS. Although this step is not required, you may find completing it is helpful when adding data carousels.

1. Consult our BFS Performance Recommendations. Our Broadcast File Server (BFS) performance recommendations can help the vendor of the third-party application decide whether a new data carousel is required for the application or if the application can use an existing data carousel. The vendor will need to specify the number and type of carousels, names given to the carousels, the

number of files placed on each carousel, and bandwidth requirements for the application.

1. Add Data Carousels to the BFS. Based on recommendations from the vendor of your third-party application, set up the BFS so that it can send third-party application data to DHCTs. Part of setting up the BFS may require that you add inband or out-of- band (OOB) data carousels (or sometimes both types of carousels) to the BFS. The BFS uses data carousels to send application data to all DHCTs in the system. Data carousels provide DHCTs with information about the third-party application:
   - Add an Inband Data Carousel to the DNCS. Generally, if a fast data transfer rate is essential, using inband data carousel may be more beneficial.
   - Add an Out-of-Band Carousel to the DNCS. If the third-party application requires access to data while simultaneously allowing the user to watch video, then use an OOB carousel for the application. Using an inband carousel in this situation results in the video being interrupted during data retrieval.

1. If necessary, Create a Package for the Third-Party Application (Optional). Creating a package is optional and is dependent upon how you plan to launch the third-party application (for example, via a channel). A package allows you to offer the service only to those subscribers who are authorized to receive it.

1. Register the Service With the SAM. A Service Application Manager (SAM) associates tuning information with other data that defines how the application operates. This association enables a DHCT to tune to the channel where the session belonging to the third-party application is streamed, extract necessary data, and use this information to run the application. (SAM service information is broadcast to DHCTs on data carousels that are dedicated to the SAM.)

1. Set the Method for Launching the Application. You can set up the third-party application to launch using a specific method depending on the needs of the application. For example, you may want the application to launch when a subscriber tunes to a particular channel. If so, you need to add the service for the application to appropriate channel maps.

1. If necessary, Add a Service to a Channel Map (Optional). Adding the service to the channel map is optional and is dependent upon how you plan to launch the third-party application. If you want the application to launch when a subscriber tunes to a particular channel, add the service to appropriate channel maps.

## Adding a VASP Entry

1. On the VASP List window, click **File > New**. The Set Up VASP window opens.

1. Complete the fields on the screen as described in ▸ VASP Entry Fields.

Use the following fields when you manage VASP entries in the DNCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.<br>**Example:** You might give a VASP entry associated with a VOD service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with a VOD service. |
| Name | The name of this VASP entry. You can use up to 80 alphanumeric characters.<br>Use a naming scheme that allows you to easily identify the type of server |

| | |
|---|---|
| | associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br><br>**Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br><br>Be careful to properly place the dots (.) between numbers.<br><br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated. Select **In Service** to activate this VASP. |

1. Click **Save**. The system saves the VASP entry information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.

1. Add the new VASP entry information to your network map.

1. Do you need to add another VASP entry?

   - If **yes**, repeat steps this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console. If your system does not use Direct ASI, go to Adding an ATM PVC Map . If your system uses Direct ASI, go to Setting Up Two-Way Communication.

## Adding a VASP Entry to Your RCS

1. On the VASP List window, click **File > New**. The Set Up VASP window opens.
2. Complete the fields on the screen as described in RCS VASP Entry Settings.

Use the following fields when you manage a VASP entry in an RCS.

| Field | Description |
|---|---|
| VASP Type | The type of VASP entry you are adding.<br>Select **General** for a VOD server or if you do not see the specific VASP type you need. |
| ID | A unique number that you will use to identify this VASP entry.<br>You can use up to 10 numeric characters. Use a numbering scheme that allows you to easily identify the type of service associated with each VASP entry. |
| Name | The name of this VASP entry.<br>You can use up to 80 alphanumeric characters. Use a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.<br>**Example:** A name of VODhub1Q43 would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43. |
| IP Address | The IP address for the server associated with this VASP entry based on your network map.<br>Be careful to properly place the dots (.) between numbers. If you are adding a VASP entry for the mmmRemote server, use the IP address for the RNCS/LIONN.<br>**Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. |
| Status | Determines whether this VASP is activated.<br>Select **In Service** to activate this VASP. |
| Site ID | The site for which this VASP provides service. |

3. Click **Save**. The system saves the VASP entry information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.
4. Do you need to add another VASP entry?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the VASP List window and return to the DNCS Administrative Console.
5. Are you setting up the elements of your system for the first time?
   - If **yes**, you are ready to set up the elements that provide two-way communication. Go to Setting Up Two-Way Communication.
   - If **no**, add the new VASP entry information to your network map.

## Add Third-Party Devices to the DNCS Hosts Table

After you add VASP entries to support devices that a third-party application uses, add the IP addresses and host names for these devices to the DNCS hosts table. Adding this information to the DNCS hosts table allows you to type the host's name, which is usually easier to remember, rather than the IP address every time you need to work with a component through the DNCS.

### You Need to Know

Before You Begin

Before you begin, make sure that you have the following items:

- IP address for the device as entered in the VASP table
- Super user (su) privileges and password (from your administrator)

### Adding Entries to the DNCS Hosts Table

Follow these steps to add entries for the devices that the third- party application uses to the DNCS hosts table.

1. Use the mouse to place the cursor on any open area on the DNCS desktop, and then click the middle mouse button. A menu appears with a list of options.
2. Click the left mouse button and select **xterm**. An xterm window appears.
3. Log in as **su**. A superuser prompt appears.
4. Type **vi /etc/hosts** and press **Enter**. The /etc/hosts file opens in a vi editor.
5. For each device, insert a blank line and add an entry for the device using the following format:

   **xxx.xxx.xxx.xxx devicename**

   **Note:** In the format shown above, **xxx.xxx.xxx.xxx** represents the IP address and **devicename** represents the name that you want to give the device. In the future, you can use this name instead of the IP address of the device when working with the device through the DNCS.

6. Type **:wq!** and press **Enter**. The system saves the changes to the /etc/hosts file and exits vi editor.
7. Type **exit** and press **Enter**. The system exits su mode and displays a root user prompt.
8. You are now ready to consult our BFS Performance Recommendations to determine the number and type of carousels that are needed to support the third-party application. Go to BFS Performance Recommendations.

## Add Third-Party Devices to the DNCS Hosts Table

After you add VASP entries to support devices that a third-party application uses, add the IP addresses and host names for these devices to the DNCS hosts table. Adding this information to the DNCS hosts table allows you to type the host's name, which is usually easier to remember, rather than the IP address every time you need to work with a component through the DNCS.

### You Need to Know

Before You Begin

Before you begin, make sure that you have the following items:

- IP address for the device as entered in the VASP table
- Super user (su) privileges and password (from your administrator)

### Adding Entries to the DNCS Hosts Table

Follow these steps to add entries for the devices that the third- party application uses to the DNCS hosts table.

1. Use the mouse to place the cursor on any open area on the DNCS desktop, and then click the middle mouse button. A menu appears with a list of options.
2. Click the left mouse button and select **xterm**. An xterm window appears.
3. Log in as **su**. A superuser prompt appears.
4. Type **vi /etc/hosts** and press **Enter**. The /etc/hosts file opens in a vi editor.
5. For each device, insert a blank line and add an entry for the device using the following format:

   **xxx.xxx.xxx.xxx devicename**

   **Note:** In the format shown above, **xxx.xxx.xxx.xxx** represents the IP address and **devicename** represents the name that you want to give the device. In the future, you can use this name instead of the IP address of the device when working with the device through the DNCS.

6. Type **:wq!** and press **Enter**. The system saves the changes to the /etc/hosts file and exits vi editor.
7. Type **exit** and press **Enter**. The system exits su mode and displays a root user prompt.
8. You are now ready to consult our BFS Performance Recommendations to determine the number and type of carousels that are needed to support the third-party application. Go to BFS Performance Recommendations.

# BFS Performance Recommendations

When determining the number and type of carousels to add to the BFS, consider the following important points:

You may assign multiple files to the same carousel as long as you consider the current and future performance requirements of the DBDS network. The more files you assign to a given data carousel, the longer it will take for the files to transfer to a DHCT.

You can redistribute existing application files among the data carousels as you add new application files to your system. consider current and future transfer speed requirements of the files when deciding whether to redistribute the application files.

Do not use any system default data carousels for third-party application files. We reserve default carousels for system files only.

### Related Topics

- Inband Versus Out-of-Band Considerations
- Inband Data Carousel Recommendations
- Out-of-Band Data Carousel Recommendations

## Inband Versus Out-of-Band Considerations

When deciding whether to assign files to an inband carousel or an out-of-band carousel, keep the following points in mind:

- Out-of-band data transfer rates are considerably slower than inband data transfer rates. Consider how fast a data transfer time you require. If a fast data transfer rate is essential, then assigning the file to an inband data carousel may be more beneficial than assigning that file to an out-of-band data carousel.
- If an application requires access to files while simultaneously allowing the user to watch video, then you should assign files for that application to an out-of-band carousel. If these application files are assigned to an inband carousel, video will be interrupted during the file retrieval.
- You can assign files for applications that do not allow the user to watch video while using the application to either the inband or out-of-band carousel, depending upon the size and the performance requirements of the application.

## Inband Data Carousel Recommendations

Consider these recommendations for managing inband data carousels on the DBDS:

- The data rate for the carousel should be either 1 or 2 Mbps (megabits per second).
- The block size should be 4000 bytes.
- The indication interval should be 100 ms (milliseconds).
- Depending upon your QAM modulation mode, the sum of your inband data carousel rates (including the OSM carousel), plus any additional audio-visual content that is combined on the modulator should not exceed the following totals:
  - If using 64-QAM modulation, 26 Mbps
  - If using 256-QAM modulation, 37 Mbps
- For assistance in adding an in-band carousel to a BFS host, see Add an Inband Data Carousel to the DNCS.

## Out-of-Band Data Carousel Recommendations

Keep the following points in mind when configuring out-of-band data carousels:

- When configuring out-of-band data carousel rates on the DBDS, you can add out-of-band carousels as long as the sum of your out-of-band data rates does not exceed 0.35 Mbps. We recommend that you strive to keep the aggregate out-of-band rate as low as possible.

  **Note:** Output from the Doctor Report will alert you when the sum of your out-of-band data carousel rates is greater than or equal to 0.30 Mbps. For more information about the Doctor Report, refer to the DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide (part number 740020). To obtain a copy of this guide, see Printed Resources.

- The indication interval should be 200 ms.
- For assistance in adding an out-of-band carousel to a BFS Host, see Add an Out-of-Band Carousel to the DNCS.

# Add a DNCS Source and Session for Inband Data Carousels

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

After you add inband data carousels to the PAT, create a DNCS source and session for the inband carousels. Adding a source and session identifies the resources (headend elements and transport streams) used to deliver application data from the headend to the access network.

## Adding a DNCS Source and Session for Inband Data Carousels

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application.

Follow these steps to add the new sources and sessions:

1. On the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront.
2. Click the **System Provisioning** tab if it is not already in the forefront.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field, and enter a name that describes one of the inband data carousels.
6. Click in the **Source ID** field and type the session number that you assigned to this carousel in the Inband Data PAT table.
7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window.
8. In the Source List window, click to highlight the source you just created.
9. Click **File > Source Definitions**. The Source Definition List window opens for this source.
10. Click **File > New Digital**. The Set Up Digital Source Definition window opens.
11. Click in the left **Session ID** field and type the session MAC address that you used when you created the inband data carousel for this source.
12. Click in the right **Session ID** field and type the source ID that you used when you added the source.

    **Note:** BFS sessions become effective as soon as they are saved. For this reason, do not specify an effective date and time for this session.

13. Click **Next.** The Define Session window opens.
14. Click the **BFS** option and click **Next**. The Save Source Definition window opens.
15. Click **Save**. The system saves the source definition in the DNCS database and creates the session you build for it. The Source Definition List now updates to include the new source information.
16. Does each PAT inband carousel that you created earlier have a DNCS source listed in the Source List?
    - If **yes**, go to step 17.
    - If **no**, repeat this procedure from step 4 to add a DNCS source and session for the PAT inband carousel.
17. Are you using our RCS Solution?
    - If **yes**, click **File > Close** to close the Source Definition List window.

- If **no**, click **File > Close** to close the Source Definition List window and return the Source List window. You are ready to add an inband BFS source to the DNCS. Go to Add an Inband BFS Source to the DNCS.

18. Repeat this procedure from step 5 to create a DNCS source and session for PAT inband carousels at each site.

19. If **no**, select **File > Close** to close the Source Definition List window and return the Source List window. Then select **File > Close** to close the Source List window. You are ready to add an inband BFS source to the DNCS. Go to Add an Inband BFS Source to the DNCS.

# Add a DNCS Source and Session for Inband Data Carousels

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

After you add inband data carousels to the PAT, create a DNCS source and session for the inband carousels. Adding a source and session identifies the resources (headend elements and transport streams) used to deliver application data from the headend to the access network.

## Adding a DNCS Source and Session for Inband Data Carousels

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application.

Follow these steps to add the new sources and sessions:

1. On the DNCS Administrative Console, click the **DNCS** tab if it is not already in the forefront.
2. Click the **System Provisioning** tab if it is not already in the forefront.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field, and enter a name that describes one of the inband data carousels.
6. Click in the **Source ID** field and type the session number that you assigned to this carousel in the Inband Data PAT table.
7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window.
8. In the Source List window, click to highlight the source you just created.
9. Click **File > Source Definitions**. The Source Definition List window opens for this source.
10. Click **File > New Digital**. The Set Up Digital Source Definition window opens.
11. Click in the left **Session ID** field and type the session MAC address that you used when you created the inband data carousel for this source.
12. Click in the right **Session ID** field and type the source ID that you used when you added the source.

    **Note:** BFS sessions become effective as soon as they are saved. For this reason, do not specify an effective date and time for this session.

13. Click **Next.** The Define Session window opens.
14. Click the **BFS** option and click **Next**. The Save Source Definition window opens.
15. Click **Save**. The system saves the source definition in the DNCS database and creates the session you build for it. The Source Definition List now updates to include the new source information.
16. Does each PAT inband carousel that you created earlier have a DNCS source listed in the Source List?
    - If **yes**, go to step 17.
    - If **no**, repeat this procedure from step 4 to add a DNCS source and session for the PAT inband carousel.
17. Are you using our RCS Solution?
    - If **yes**, click **File > Close** to close the Source Definition List window.

- If **no**, click **File > Close** to close the Source Definition List window and return the Source List window. You are ready to add an inband BFS source to the DNCS. Go to Add an Inband BFS Source to the DNCS.

18. Repeat this procedure from step 5 to create a DNCS source and session for PAT inband carousels at each site.

19. If **no**, select **File > Close** to close the Source Definition List window and return the Source List window. Then select **File > Close** to close the Source List window. You are ready to add an inband BFS source to the DNCS. Go to Add an Inband BFS Source to the DNCS.

# Add a BFS Server to the DNCS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > Servers > File > New**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > All Sites > Servers > File > New**

## Adding a BFS Server to the DNCS

After you add an inband source or add out-of-band source to the BFS, add a BFS server to receive data from the source you just added. BFS servers send this data to the BFS client on the DNCS.

1. On the DNCS Administrative Console, click the Application Interface Modules tab if it is not already in the forefront.
2. Click **BFS Admin**. Depending on your system configuration, the following window opens:
3. If you are using a typical DBDS with no RCS, the **BFS Administration window** opens. If this window opens, go to step 4.
4. If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 5.
5. Select **File > All Sites**.
6. Click the **Servers** tab.
7. Click **File > New**. The Authorize BFS Server window opens.
8. Click in the **Server Name** field and type a name for the server. Make sure that the name exactly matches the name of the application. Otherwise, the BFS may be unable to send third-party application data to DHCTs.
9. In the **Available Sources** field, click to select the sources that you have added to the BFS.
10. Click **Add**. The selection moves to the Selected Source field.
11. Add any other sources to the Selected Source field by repeating steps 9 and 10.
12. Click **Save**. The system saves the server information in the DNCS database and closes the Authorize BFS Server window.
13. Click **File > Close** to close the BFS Administration window.
14. Do you need to add other data carousels to this BFS?
    - If **yes**, repeat this procedure from step 5 to add an inband server for the other carousel to the BFS.
    - If **no**, you have successfully added a BFS server for the third-party application to the DNCS. You are ready to register this server with the BFS. Go to Register the Server With the BFS.

# Add a BFS Server to the DNCS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > Servers > File > New**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > All Sites > Servers > File > New**

## Adding a BFS Server to the DNCS

After you add an inband source or add out-of-band source to the BFS, add a BFS server to receive data from the source you just added. BFS servers send this data to the BFS client on the DNCS.

1. On the DNCS Administrative Console, click the Application Interface Modules tab if it is not already in the forefront.
2. Click **BFS Admin**. Depending on your system configuration, the following window opens:
3. If you are using a typical DBDS with no RCS, the **BFS Administration window** opens. If this window opens, go to step 4.
4. If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 5.
5. Select **File > All Sites**.
6. Click the **Servers** tab.
7. Click **File > New**. The Authorize BFS Server window opens.
8. Click in the **Server Name** field and type a name for the server. Make sure that the name exactly matches the name of the application. Otherwise, the BFS may be unable to send third-party application data to DHCTs.
9. In the **Available Sources** field, click to select the sources that you have added to the BFS.
10. Click **Add**. The selection moves to the Selected Source field.
11. Add any other sources to the Selected Source field by repeating steps 9 and 10.
12. Click **Save**. The system saves the server information in the DNCS database and closes the Authorize BFS Server window.
13. Click **File > Close** to close the BFS Administration window.
14. Do you need to add other data carousels to this BFS?
    - If **yes**, repeat this procedure from step 5 to add an inband server for the other carousel to the BFS.
    - If **no**, you have successfully added a BFS server for the third-party application to the DNCS. You are ready to register this server with the BFS. Go to Register the Server With the BFS.

# Register a Server With the BFS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > New Server**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > File > New Server**

After you have added a BFS server for the third-party application, register the BFS server with the BFS. When a server registers with the BFS, the BFS regularly broadcasts data held on the server to the access network. The BFS sends this data on data carousels to all DHCTs in the system. However, DHCTs retrieve information carried on data carousels for only the applications they are authorized to receive.

**Important:** If you are using our RCS solution, select All Sites to make the following changes to all existing sites and all future sites that will use this third-party application.

## Registering a Server with the BFS

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Client**. Depending on your system configuration, one of the following windows opens:
   - If you are using a typical DBDS with no RCS, the **Broadcast File Server List** window opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**. The Broadcast File Server List window opens.
4. Click **File > New Server**. The Set Up Server window opens.
5. Click in the **Server Name** arrow and select the BFS server that you authorized for the application. The system automatically selects the mode that the server uses and lists in the Available Sources list all of the sources (carousels) available to the server.
6. In the **Available Sources** field, click to select one of the sources that you have added to the BFS.
7. Click **Add**. The selection moves to the Selected Source field.
8. Add any other data sources that you created to the Selected Source field by repeating steps 6 and 7.
9. Click **Save**. The system saves the server information in the DNCS database. The Authorize BFS Server window closes and a cabinet icon, which represents the server, appears on the BFS List.
10. Do you need to register other servers with this BFS client?
    - If **yes**, repeat this procedure from step 4 to register another server with this BFS client.
    - If **no**, you have successfully registered the BFS server with the BFS Client. In some cases, you may also need to organize files and links for the third-party application. In most cases, however, you only need to add a file or link to the BFS server. To organize files and links, go to Organize the Files and Links Placed on a BFS Server. To add a file or link, go to Add Files and Links to the BFS List.

# Register a Server With the BFS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > New Server**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > File > New Server**

After you have added a BFS server for the third-party application, register the BFS server with the BFS. When a server registers with the BFS, the BFS regularly broadcasts data held on the server to the access network. The BFS sends this data on data carousels to all DHCTs in the system. However, DHCTs retrieve information carried on data carousels for only the applications they are authorized to receive.

**Important:** If you are using our RCS solution, select All Sites to make the following changes to all existing sites and all future sites that will use this third-party application.

## Registering a Server with the BFS

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Client**. Depending on your system configuration, one of the following windows opens:
   - If you are using a typical DBDS with no RCS, the **Broadcast File Server List** window opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**. The Broadcast File Server List window opens.
4. Click **File > New Server**. The Set Up Server window opens.
5. Click in the **Server Name** arrow and select the BFS server that you authorized for the application. The system automatically selects the mode that the server uses and lists in the Available Sources list all of the sources (carousels) available to the server.
6. In the **Available Sources** field, click to select one of the sources that you have added to the BFS.
7. Click **Add**. The selection moves to the Selected Source field.
8. Add any other data sources that you created to the Selected Source field by repeating steps 6 and 7.
9. Click **Save**. The system saves the server information in the DNCS database. The Authorize BFS Server window closes and a cabinet icon, which represents the server, appears on the BFS List.
10. Do you need to register other servers with this BFS client?
    - If **yes**, repeat this procedure from step 4 to register another server with this BFS client.
    - If **no**, you have successfully registered the BFS server with the BFS Client. In some cases, you may also need to organize files and links for the third-party application. In most cases, however, you only need to add a file or link to the BFS server. To organize files and links, go to Organize the Files and Links Placed on a BFS Server. To add a file or link, go to Add Files and Links to the BFS List.

# Organize Files and Links

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > [Select Server] > File > New Directory**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > [Select Server] > File > New Directory**

After you have registered a server with the BFS client, you may need to organize the data that the server provides by adding directories to the server. Directories are used if the third-party application requires that several files be placed on the server. To organize files by placing them in directories, create the directory first. After creating the directory, you can then add files or links to it.

**Important:** Unless instructed by us, do not edit existing servers. Editing existing servers without assistance from us may cause the system to become unstable.

## Adding Directories to the BFS List

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab if it is not already in the forefront.
2. Click **BFS Client**. Depending on your system configuration,one of the following windows opens:
   - If you are using a typical DBDS with no RCS, the **Broadcast File Server List** window opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**. The Broadcast File Server List window opens.
4. From the BFS List, click to highlight the server you just added. Then select **File > New Directory**. The Set Up Directory window appears.
5. Click in the **Directory Name** field and enter a name for the directory.
6. Click **Save**. The Set Up Directory window closes, and a folder icon appears beneath the server. The folder icon represents the directory and the name you assigned to the directory appears next to it.
7. Do you need to add another directory to this server?
   - If **yes**, repeat this procedure from step 4 to add another directory to the server.
   - If **no**, you have successfully added a directory to this server and are ready to add files or links to the directory. Go to Add Files or Links to a BFS.

# Organize Files and Links

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > [Select Server] > File > New Directory**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > [Select Server] > File > New Directory**

After you have registered a server with the BFS client, you may need to organize the data that the server provides by adding directories to the server. Directories are used if the third-party application requires that several files be placed on the server. To organize files by placing them in directories, create the directory first. After creating the directory, you can then add files or links to it.

**Important:** Unless instructed by us, do not edit existing servers. Editing existing servers without assistance from us may cause the system to become unstable.

## Adding Directories to the BFS List

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab if it is not already in the forefront.
2. Click **BFS Client**. Depending on your system configuration,one of the following windows opens:
   - If you are using a typical DBDS with no RCS, the **Broadcast File Server List** window opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**. The Broadcast File Server List window opens.
4. From the BFS List, click to highlight the server you just added. Then select **File > New Directory**. The Set Up Directory window appears.
5. Click in the **Directory Name** field and enter a name for the directory.
6. Click **Save**. The Set Up Directory window closes, and a folder icon appears beneath the server. The folder icon represents the directory and the name you assigned to the directory appears next to it.
7. Do you need to add another directory to this server?
   - If **yes**, repeat this procedure from step 4 to add another directory to the server.
   - If **no**, you have successfully added a directory to this server and are ready to add files or links to the directory. Go to Add Files or Links to a BFS.

# Add Files and Links to the BFS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > [Select Server] > File > New File or New Link**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > [Select Server] > File > New File or New Link**

After you have registered a server with the BFS client, you are ready to add files or links to the server or to its directory. When adding files or links, you have two options:

- You can place a physical file on the server. Typically, files are used when the amount of data is small. The vendor of your third-party application can help you determine whether you need to add a file or link.
- You can place a link to the file. Typically, links are used when many files must be placed on the server, or when a data file itself is large. The vendor of your third-party application can help you determine whether you need to add file a or link to the BFS list.

**Note:** If a server needs many files, a vendor may decide to organize the files by adding directories to the server and then adding the files or links to the directories. To organize files and links by placing them in directories, create the directory first. After a directory is created, you can then add files to the directory.

## Adding Files or Links to a BFS Server

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab if it is not already in the forefront.
2. Click **BFS Client**. Depending on your system configuration, one of the following windows opens:
   - If you are using a typical DBDS with no RCS, the **Broadcast File Server List** window opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**. The Broadcast File Server List window opens.
4. From the BFS List window, click to highlight the server or directory you just added. Then perform one of the following tasks:
   - If you want to add a file, select **File > New File**. The Set Up File window opens. Click in the **File Name** field and enter a name to help you remember what the file contains.
   - If you want to add a link, select **File > New Link**. The Set Up Link window opens. Click in the **Link Name** field and enter a name to help you remember the data to which the link points.
5. Click the **Source Name** arrow and select the sources (carousels) associated with this server or directory.
6. Click **Select**. The Path Selection Dialog window opens.
7. Scroll through the **Files** list on the right and click the file that contains the appropriate data. The **Selection** field displays the path to the file that you selected.
8. Click **OK**. The Path Selection Dialog window closes.
9. Click **Save**. The window closes and the new file or link appears beneath the server or directory you selected in step 4.

10. Do you need to add another file or link to the server or directory?

- If **yes**, repeat this procedure from step 4 to add another file or link to the server or directory.
- If **no**, you have successfully added an inband or OOB data carousel to the BFS. You are ready to add a package for the third-party application to the DNCS. A package allows you to offer the service to only those subscribers who are authorized to receive it. Go to Add a Service Package.

# Add Files and Links to the BFS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > [Select Server] > File > New File or New Link**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > All Sites > [Select Server] > File > New File or New Link**

After you have registered a server with the BFS client, you are ready to add files or links to the server or to its directory. When adding files or links, you have two options:

- You can place a physical file on the server. Typically, files are used when the amount of data is small. The vendor of your third-party application can help you determine whether you need to add a file or link.
- You can place a link to the file. Typically, links are used when many files must be placed on the server, or when a data file itself is large. The vendor of your third-party application can help you determine whether you need to add file a or link to the BFS list.

**Note:** If a server needs many files, a vendor may decide to organize the files by adding directories to the server and then adding the files or links to the directories. To organize files and links by placing them in directories, create the directory first. After a directory is created, you can then add files to the directory.

## Adding Files or Links to a BFS Server

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab if it is not already in the forefront.
2. Click **BFS Client**. Depending on your system configuration, one of the following windows opens:
   - If you are using a typical DBDS with no RCS, the **Broadcast File Server List** window opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**. The Broadcast File Server List window opens.
4. From the BFS List window, click to highlight the server or directory you just added. Then perform one of the following tasks:
   - If you want to add a file, select **File > New File**. The Set Up File window opens. Click in the **File Name** field and enter a name to help you remember what the file contains.
   - If you want to add a link, select **File > New Link**. The Set Up Link window opens. Click in the **Link Name** field and enter a name to help you remember the data to which the link points.
5. Click the **Source Name** arrow and select the sources (carousels) associated with this server or directory.
6. Click **Select**. The Path Selection Dialog window opens.
7. Scroll through the **Files** list on the right and click the file that contains the appropriate data. The **Selection** field displays the path to the file that you selected.
8. Click **OK**. The Path Selection Dialog window closes.
9. Click **Save**. The window closes and the new file or link appears beneath the server or directory you selected in step 4.

10. Do you need to add another file or link to the server or directory?

- If **yes**, repeat this procedure from step 4 to add another file or link to the server or directory.
- If **no**, you have successfully added an inband or OOB data carousel to the BFS. You are ready to add a package for the third-party application to the DNCS. A package allows you to offer the service to only those subscribers who are authorized to receive it. Go to Add a Service Package.

# Add an Inband Data Carousel

If, after consulting our BFS Performance Recommendations, the vendor of the application determines that you need to add an inband data carousel to support the application, follow these instructions. They give an overview of the process for adding an inband data carousel to the DNCS. Click any link to display step-by-step instructions for the procedures summarized here.

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application. Since most applications are not site-aware, you most likely need to make the following changes to every site in your system.

1. Add an Inband Carousel to the PAT. If the vendor of your application determines that an inband data carousel is required to support the application, you need to first add a data carousel to the Program Allocation Table (PAT). Data in the PAT enables a DHCT to correctly run a specific application. The PAT lists all of the programs in an MPEG stream and where to find the data for each program. In fact, it may help to think of a PAT as a table of contents for MPEG streams. When DHCTs tune to a channel, they extract the PAT and other information and use this data to display applications for subscribers. Because PAT data enables applications to run correctly, whenever you add an inband data carousel to the BFS to support a new application, you must first add an inband data carousel to the PAT.
2. Add a DNCS Source and Session to the DNCS. If the vendor of your application determines that an inband data carousel is required to support the application, you need to add a source and session for the application to the DNCS. Adding a source and session identifies the resources (headend elements and transport streams) used to deliver application data from the headend to the access network.
3. Add an Inband BFS Source to the DNCS. Adding a BFS source is the first step in setting up an inband data carousel. BFS sources provide data to BFS servers.
4. Add a BFS Server to the DNCS. Adding a BFS server is the second step in setting up an inband data carousel. BFS servers receive data from BFS sources and send the data to the BFS client on the DNCS.
5. Register the Server with the BFS. The third step in setting up an inband data carousel is to register the BFS server with the BFS client. When a server registers with the BFS client, the BFS regularly broadcasts data held on the server to the access network. The BFS sends this data on data carousels to all DHCTs in the system. However, DHCTs retrieve information carried on data carousels for only the applications they are authorized to receive.
6. Organize Files and Links (Optional). If needed, organize data that the third-party application provides by adding one or more directories to the BFS server. After you have added a directory, you can then add files or links to the directory.
7. Add a File or Link to the BFS Server. The last step in setting up the inband data carousel is to add a file or link from the server on the BFS client to the directory on the DNCS where you copied the third-party application. When this file or link is created, it provides the BFS server with data contained in the file.

## Add Inband Carousels to the PAT

**Quick Path - Without RCS: DNCS Administrative Console > DNCS tab > System Provisioning tab > BFS Admin > Hosts tab > [Select dncsatm] > File > Open > PAT Configuration**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Module tab > BFS Admin > [Select Site] > File > Select > Hosts tab > [Select dncsatm] > File > Open > PAT Configuration**

If, after reviewing the BFS Performance Recommendations, the vendor of your third-party application determines that you need to add one or more inband carousels to support the application, add inband carousels to the PAT (program allocation table).

The PAT lists all of the programs in an MPEG stream and where to find the data for each program. In fact, it may help to think of a PAT as a table of contents for MPEG streams. When DHCTs tune to a channel, they extract the PAT and other information and use this data to display applications for subscribers.

**Important:** If you are using our RCS solution, you need to complete this procedure for individually for each site.

**You Need to Know**

Before You Begin

If you are using our RCS solution, make sure that you know the BFS MAC address for each site that will use this third-party application. You can obtain this address from the Site Summary window.

### Adding Inband Carousels to the PAT

As part of this procedure, you will determine the session numbers to assign to the new inband carousels. When determining a session number to assign to the inband carousel, the number must meet the following requirements:

- The number must be an even number. (our numbering convention uses even numbers for inband carousels and odd numbers for out-of-band carousels.)
- The number must be higher than 200. (Numbers 1 to 200 are reserved for system-built sessions.)
- The number must be one that is not currently in use as a source ID (in the Source List) or as a session ID (in the Inband Data PAT table).
- If you are using our RCS solution and the third-party application will be used by more than one site, the number must be one that is not currently in use as a source ID (in the Source List) or as a session ID for any site that will use the application (Inband PAT table for each site that will use the application).

Follow these steps to determine the session numbers to assign to the new inband carousels and to then add the new inband carousels to the PAT.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click the **Source ID** column heading to sort the list of sources by source ID starting with the highest ID and ending with the lowest ID.

   **Note:** You might need to click the Source ID column more than once for the list to show in order from highest to the lowest.

5. Find the highest even-numbered Source ID. (If you ordered the Source ID list from highest to lowest, it should be the first number in the list.) Record this number so that you can refer to it later.
6. Does your system use Direct ASI?

   **Note:** If you are using our RCS Solution, your system uses Direct ASI. Direct ASI is required for RCS.

   - If **yes**, from the DNCS Administrative Console, select the **Application Interface Modules** tab and then click **BFS Admin**. The Please select a site window opens. Go to step 8.
   - If **no**, from the DNCS Administrative Console, select the **Network Element Provisioning** tab and then click **BIG**. The BIG List opens.

7. Click to select the BIG shown in the BIG List. Then select **File > Open**. The Set Up BIG window opens. Go to step 11.
8. Select DNCS from the list of sites. Then select **File > Select**. The Site DNCS BFS Administration window opens.
9. Click the **Hosts** tab.
10. Select **dncsatm** from the list of hosts. Then select File and click Open. The Set Up BFS Host window opens.
11. Click **PAT Configuration**. The window that opens depends on your system configuration:
    - For systems using Direct ASI, the Inband Data PAT list opens.
    - For systems that are not using Direct ASI, the BIG PAT list opens.
12. Use the scroll bar on the PAT list to view the highest session number in the table and write down this number so that you can refer to it later.

**Important:** If you are using RCS and other sites in your system will use the third-party application, repeat steps 8 to 12 as many times as is necessary to find the highest number in use at each site that will use the third-party application. (Be aware that you will need to modify step 8 by selecting a site other than the central DNCS site that will use the application.)

13. Compare the number (or numbers) you wrote down in step 12 to the number that you recorded in step 5, select the highest number, add two to it, and record this number. (For example, if the highest number is 4446, you would record 4448.)

**Important:** Be sure that the number you record is greater than 200. If it is not, use a number that is greater than 200. Also make sure that the number you record is an even number. If it is not, add 1 to the number so that it is an even number. You must use a number greater than 200 because session numbers 1 to 200 are reserved for system-built sessions. You must use an even number because our numbering convention uses even numbers for inband BFS carousels and odd numbers for out-of-band carousels.

**Note:** The number that you record in this step will be the session number for the third-party application.

14. Click **New Entry** on the PAT list. The BIG PAT Setup window opens and provides values in the Program Number and the PMT PID fields.

15. Click in the **Session MAC Address** field, and enter the following according to your system configuration:

- If you are using a typical DBDS with no RCS, enter 12 zeros (**00:00:00:00:00:00**) in this field.
- If you are using an RCS, enter the BFS MAC address of this site in this field. You can obtain this address from the Site Summary window. (To display the Site Summary window, click the **RNCS Sites** button on the System Provisioning tab.)

16. Click in the **Session Number** field and type the number that you wrote down in step 13.

**Important:** When entering numbers, make certain that you enter numbers in order from lowest to highest. Entering numbers in a random order will degrade system performance.

17. Click **Save**. An information message appears and reminds you that all BFS sessions must be torn down and rebuilt for deletions to take effect.

18. Click **OK**. The system saves your new inband data carousel.

19. Do you need to add other inband data carousels to the list?

- If **yes**, repeat steps 14 to 18 to add inband data carousels to the list.

  **Important:** When entering session numbers for additional carousels, add 2 to the number you previously entered so that each inband carousel has a unique session number that is an even number.

  **Example:** If you entered **4448** for the first carousel, enter **4450** for the second carousel, **4452** for the third carousel, and so on.

- If **no**, click **Close** to close the list.

20. Click **Save**. The system saves the changes you made, and the following occurs according to your system configuration:

- If your system is configured for Direct ASI, the Set Up BFS Host window closes.
- If your system is not configured for Direct ASI, the Set Up BIG window closes. You are ready to add a DNCS source and session for the inband carousel you created. Go to Add a DNCS Source and Session for Inband Data Carousels.

21. Are you using our RCS solution?

- If **yes**, select **File > Close** to close the Site DNCS BFS Administration window.
- If **no**, select **File > Close** to close the DNCS BFS Administration window. You are ready to add a DNCS source and session for the inband carousel you created. Go to Add a DNCS Source and Session for Inband Data Carousels.

22. Select the site where the application will be used. Then select **File > Select**. The Site-specific BFS Administration window opens.
23. Click the host listed in the Host tab. Then select **File > Open**. The Set Up BFS Host window opens.
24. Add one or more inband carousels to the PAT by repeating steps 11 to 20 for each inband carousel.
25. Now that you have added an inband carousel to the PAT for all sites that will use this application, go to Add a DNCS Source and Session for Inband Data Carousels.

# Add an OOB Data Carousel

## Adding an OOB Data Carousel

If, after consulting our BFS Performance Recommendations, the vendor of the application determines that you need to add an out-of-band (OOB) data carousel to support the application, follow these instructions. They give an overview of the process for adding an OOB data carousel to the DNCS. Click any link to display step-by-step instructions for the procedures summarized here.

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application. Most applications are not site-aware, so you most likely need to make the following changes to **every** site in your system.

1. Add an OOB BFS Source to the DNCS. Adding a BFS source is the first step in setting up an OOB data carousel. BFS sources provide data to BFS servers.
2. Add a BFS Server to the DNCS. Adding a BFS server is the second step in setting up an OOB data carousel. BFS servers receive data from BFS sources and send the data to the BFS client on the DNCS.
3. Register the Server with the BFS. The third step in setting up an OOB data carousel is to register the BFS server with the BFS client. When a server registers with the BFS client, the BFS regularly broadcasts data held on the server to the access network. The BFS sends this data on data carousels to all DHCTs in the system. However, DHCTs retrieve information carried on data carousels for only the applications they are authorized to receive.
4. Organize Files and Links (Optional). If needed, organize data that the third-party application provides by adding one or more directories to the BFS server.
5. Add a File or Link to the BFS Server. The last step in setting up the OOB data carousel is to add a file or link from the server on the BFS client to the directory on the DNCS where you copied the third-party application. When this file or link is created, it provides the server with data contained in the file.

**Note:** It is not necessary to add a DNCS source and session when adding an OOB carousel. Sources and sessions are needed only for applications whose data is carried on a QAM channel. Additionally, because PAT data acts as a table of contents for MPEG streams sent on QAM channels, only inband carousels require PAT data. As a result, it is not necessary to add a carousel to the PAT when adding an OOB carousel to the DNCS.

# Add an OOB Data Carousel

## Adding an OOB Data Carousel

If, after consulting our BFS Performance Recommendations, the vendor of the application determines that you need to add an out-of-band (OOB) data carousel to support the application, follow these instructions. They give an overview of the process for adding an OOB data carousel to the DNCS. Click any link to display step-by-step instructions for the procedures summarized here.

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application. Most applications are not site-aware, so you most likely need to make the following changes to **every** site in your system.

1. Add an OOB BFS Source to the DNCS. Adding a BFS source is the first step in setting up an OOB data carousel. BFS sources provide data to BFS servers.
2. Add a BFS Server to the DNCS. Adding a BFS server is the second step in setting up an OOB data carousel. BFS servers receive data from BFS sources and send the data to the BFS client on the DNCS.
3. Register the Server with the BFS. The third step in setting up an OOB data carousel is to register the BFS server with the BFS client. When a server registers with the BFS client, the BFS regularly broadcasts data held on the server to the access network. The BFS sends this data on data carousels to all DHCTs in the system. However, DHCTs retrieve information carried on data carousels for only the applications they are authorized to receive.
4. Organize Files and Links (Optional). If needed, organize data that the third-party application provides by adding one or more directories to the BFS server.
5. Add a File or Link to the BFS Server. The last step in setting up the OOB data carousel is to add a file or link from the server on the BFS client to the directory on the DNCS where you copied the third-party application. When this file or link is created, it provides the server with data contained in the file.

**Note:** It is not necessary to add a DNCS source and session when adding an OOB carousel. Sources and sessions are needed only for applications whose data is carried on a QAM channel. Additionally, because PAT data acts as a table of contents for MPEG streams sent on QAM channels, only inband carousels require PAT data. As a result, it is not necessary to add a carousel to the PAT when adding an OOB carousel to the DNCS.

## BFS OOB Source Settings

Use the following fields when you manage an out-of-band BFS source in the DNCS.

| Field | Description |
|---|---|
| Source Name | A name that describes this BFS source. |
| Source ID | A unique number that identifies this BFS source.<br>When selecting a number, make sure to select an odd number that is not in use and is higher than 200. (our numbering convention uses odd numbers for out-of-band- carousels and reserves numbers 1 to 200 for system-built sources.) |
| Source Type | Determines the type of source you are adding.<br>Select the **BFS** option. |
| Transport Type | Determines the transport type for the source.<br>Select the **Out-of-band** option. |
| Data Rate | The data rate for this source as specified by your third-party application vendor. |
| Block Size | The block size for this source as specified by your third-party application vendor. |
| Indication Interval | Determines how often the Download Indication messages are transmitted, as specified by your third-party application vendor. |
| Hosts | Determines the correct host for this source.<br>Select the correct host from the Available Hosts list and click **Add**. The host moves to the Selected Hosts list. |

# Add Out-of-Band BFS Source to the DNCS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > Sources > File > New**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > All Sites > Sources > File > New**

If, after reviewing the BFS Performance Recommendations, the vendor of your third-party application determines that you need to add out-of-band carousels to support the application, add these carousels to the BFS. The BFS uses out-of-band carousels to send data files to DHCTs telling the DHCTs how to run a specific application. BFS carousels make this information available to all DHCTs in your system. However, only those DHCTs specifically authorized and looking for the information will receive it. QPSK modulators send OOB data carousels to the access network.

**Important:** If you are using our RCS solution, select All Sites to make the changes to each site that will use this third-party application.

## You Need to Know

Before You Begin

Make sure that the vendor of your third-party application has provided you with recommendations for the following values.

- Data rate of each out-of-band data carousel
- Block size of each out-of-band data carousel
- Indication interval of each out-of-band data carousel

## Adding Out-of-Band Sources to the BFS

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. Depending on your system configuration,one the following windows opens:
   - If you are using a typical DBDS with no RCS, the **BFS Administration window** opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**.
4. Click the **Sources** tab if it is not already in the forefront.
5. Click **File > New**. The Set Up BFS Source window opens.
6. Complete the fields on the screen as described in BFS OOB Source Settings.

Use the following fields when you manage an out-of-band BFS source in the DNCS.

| Field | Description |
|---|---|
| Source Name | A name that describes this BFS source. |
| Source ID | A unique number that identifies this BFS source.<br>When selecting a number, make sure to select an odd number that is not in use and is higher than 200. (our numbering convention uses odd numbers for out-of-band- carousels and reserves numbers 1 to 200 for system-built sources.) |

| | |
|---|---|
| Source Type | Determines the type of source you are adding.<br>Select the **BFS** option. |
| Transport Type | Determines the transport type for the source.<br>Select the **Out-of-band** option. |
| Data Rate | The data rate for this source as specified by your third-party application vendor. |
| Block Size | The block size for this source as specified by your third-party application vendor. |
| Indication Interval | Determines how often the Download Indication messages are transmitted, as specified by your third-party application vendor. |
| Hosts | Determines the correct host for this source.<br>Select the correct host from the Available Hosts list and click **Add**. The host moves to the Selected Hosts list. |

**Important:** Do not change any other fields.

7. Click **Save**. The system saves the carousel in the DNCS database and closes the Set Up BFS Source window.

8. Do you need to add other data carousels to this BFS?
   - If **yes**, repeat this procedure from step 5 to add other out-of-band data carousels to the BFS.
   - If **no**, authorize BFS servers for these carousels.

# Add Out-of-Band BFS Source to the DNCS

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > Sources > File > New**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > All Sites > Sources > File > New**

If, after reviewing the BFS Performance Recommendations, the vendor of your third-party application determines that you need to add out-of-band carousels to support the application, add these carousels to the BFS. The BFS uses out-of-band carousels to send data files to DHCTs telling the DHCTs how to run a specific application. BFS carousels make this information available to all DHCTs in your system. However, only those DHCTs specifically authorized and looking for the information will receive it. QPSK modulators send OOB data carousels to the access network.

**Important:** If you are using our RCS solution, select All Sites to make the changes to each site that will use this third-party application.

## You Need to Know

Before You Begin

Make sure that the vendor of your third-party application has provided you with recommendations for the following values.

- Data rate of each out-of-band data carousel
- Block size of each out-of-band data carousel
- Indication interval of each out-of-band data carousel

## Adding Out-of-Band Sources to the BFS

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. Depending on your system configuration,one the following windows opens:
   - If you are using a typical DBDS with no RCS, the **BFS Administration window** opens. If this window opens, go to step 4.
   - If you are using an RCS, the **Please select a site window** opens. If this window opens, go to step 3.
3. Select **File > All Sites**.
4. Click the **Sources** tab if it is not already in the forefront.
5. Click **File > New**. The Set Up BFS Source window opens.
6. Complete the fields on the screen as described in BFS OOB Source Settings.

Use the following fields when you manage an out-of-band BFS source in the DNCS.

| Field | Description |
|---|---|
| Source Name | A name that describes this BFS source. |
| Source ID | A unique number that identifies this BFS source.<br>When selecting a number, make sure to select an odd number that is not in use and is higher than 200. (our numbering convention uses odd numbers for out-of-band- carousels and reserves numbers 1 to 200 for system-built sources.) |

| | |
|---|---|
| Source Type | Determines the type of source you are adding.<br>Select the **BFS** option. |
| Transport Type | Determines the transport type for the source.<br>Select the **Out-of-band** option. |
| Data Rate | The data rate for this source as specified by your third-party application vendor. |
| Block Size | The block size for this source as specified by your third-party application vendor. |
| Indication Interval | Determines how often the Download Indication messages are transmitted, as specified by your third-party application vendor. |
| Hosts | Determines the correct host for this source.<br>Select the correct host from the Available Hosts list and click **Add**. The host moves to the Selected Hosts list. |

**Important:** Do not change any other fields.

7. Click **Save**. The system saves the carousel in the DNCS database and closes the Set Up BFS Source window.

8. Do you need to add other data carousels to this BFS?
   - If **yes**, repeat this procedure from step 5 to add other out-of-band data carousels to the BFS.
   - If **no**, authorize BFS servers for these carousels.

# Set Up a Service

## Set Up Services Provided by a Third-Party Application

After you have added an inband data carousel or an OOB data carousel to support the third-party application, you are ready to setup services that the third-party application provides. Follow these steps to set up services for a third-party application.

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application. Since most applications are not site-aware, you most likely need to make the following changes to every site in your system.

1. Add a Service Package for the third-party application. A package allows you to offer the service only to those subscribers who are authorized to receive it.
2. Register the Service With the SAM. Registering a package with the Service Application Manager (SAM) associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT.
3. Set the Method for Launching the Application. You can set up the third-party application to launch using a specific method depending on the needs of the application. For example, you may want the application to launch when a subscriber tunes to a particular channel. If so, you need to add the service for the application to appropriate channel maps.
4. Add the Service to a Channel Map. Adding a service to the channel maps you have created enables subscribers to access the service by tuning to a particular channel.

# Set Up a Service

## Set Up Services Provided by a Third-Party Application

After you have added an inband data carousel or an OOB data carousel to support the third-party application, you are ready to setup services that the third-party application provides. Follow these steps to set up services for a third-party application.

**Important:** If you are using our RCS solution, make the following changes to each site that will use this third-party application. Since most applications are not site-aware, you most likely need to make the following changes to every site in your system.

1. Add a Service Package for the third-party application. A package allows you to offer the service only to those subscribers who are authorized to receive it.
2. Register the Service With the SAM. Registering a package with the Service Application Manager (SAM) associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT.
3. Set the Method for Launching the Application. You can set up the third-party application to launch using a specific method depending on the needs of the application. For example, you may want the application to launch when a subscriber tunes to a particular channel. If so, you need to add the service for the application to appropriate channel maps.
4. Add the Service to a Channel Map. Adding a service to the channel maps you have created enables subscribers to access the service by tuning to a particular channel.

## Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

**You Need to Know**

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

## Register a Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > File > New**

**Note:** This procedure does not apply to PPV services.

Registering a service with the SAM achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT
- Communicates the operation attributes to the DHCTs in your network
- Registers the service and its operation attributes with the BFS

For example, to access a standard audio/video program service, a DHCT must download the WatchTV application. The WatchTV application contains the operation attributes that tell the DHCT how to tune to and display a standard audio/video program service so that subscribers can hear and view the service. In the case of a VOD service, a DHCT must download a PTV (PowerTV) file to serve the same purpose.

In addition, if the service is to be included as part of a package, registering the service associates it with the specified package.

**Important:** Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot.

**Note:** If you want to adjust how often the SAM communicates service operation attributes to the DHCTs in your network, go to Scheduling Service Updates.

### You Need to Know

When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

## Set the Method for Launching the Third-Party Application

You can set up a third-party application to launch using one of the following methods:

- **Key.** Launch the third-party application when a subscriber presses a specific key on the remote control. For details, refer to Enhancing Your Subscribers' Experience: SARA Configurable Options (part number 4002178). To obtain a copy of this guide, see Printed Resources.
- **Services Portal.** Launch the third-party application from a Service Portal, which provides a menu of services and popular channels. For details, refer to Services Portal 3.0 Installation and Configuration Guide (part number 745238). To obtain a copy of this guide, see Printed Resources.
- **Channel.** Launch the third-party application when a subscriber tunes to a specific channel. To configure the application for this launch method, add the service for the application to a channel map. For assistance, see Add a Service to a Channel Map.

## Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

## Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.

7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.

8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?

   - If **yes**, go to Split a Channel.
   - If **no**, go to step 9.

9. Do you need to add another service to this channel map?

   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.

10. Do you need to add a service to another channel map?

    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

11. Do you need to include the service on your IPG?

    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.

12. Is this is a VOD service?

    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.

13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

## Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

## Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.

7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.

8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?

   - If **yes**, go to Split a Channel.
   - If **no**, go to step 9.

9. Do you need to add another service to this channel map?

   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.

10. Do you need to add a service to another channel map?

    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

11. Do you need to include the service on your IPG?

    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.

12. Is this is a VOD service?

    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.

13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

# Remove a Third-Party Application

If you decide to remove an application from the data carousel, you must delete the BFS sources from the data carousel. This section provides procedures for deleting a BFS carousel that is associated with the application you are removing from the DNCS.

**Important:** To delete the application from the DNCS, refer to the instructions that are unique to that application.

**CAUTION:** Because the procedures for deleting inband BFS sources from the data carousel requires you to teardown all BFS sessions, we recommend that you perform these procedures during a maintenance window.

1. Verify the Number of Sessions Before Deleting an Inband Source
2. Delete Client BFS Servers for Inband or Out-of-Band Carousels
3. Delete the BFS Server Authorized for the Inband or Out-of-Band Carousels
4. Delete BFS Sources from the Data Carousel for Inband or Out-of-Band Carousels
5. Remove an Application from the Source List
6. Remove the Inband BFS Carousel from the BIG PAT Table
7. Stop the BFS Server Processes
8. Tear Down and Rebuild BFS Sessions
9. Restart the BFS Server Processes
10. Verify the Number of Sessions After Deleting an Inband Source

## Verify the Number of Sessions Before Deleting an Inband Source

When a source is deleted from the system, the session count on the QAM carrying that inband source will decrease. By verifying the session count prior to deleting an inband source, you can determine whether the inband source was successfully deleted at the end of these procedures.

**Important:** If your system is running in an RCS environment, you will need to locate the respective QAM that is carrying the session you wish to delete.

1. Facing the front of the QAM modulator, press the OPTIONS button to cycle through the QAM menu screens until you see the Session Count screen.
2. Make a note of the number of sessions.

   **Note:** The session count will be referenced after you have completed the remaining procedures in this chapter. This value will allow you to verify that you have successfully deleted all sessions on the QAM after you have changed its configuration.

3. Go to Delete Client BFS Servers for Inband or Out-of-Band Carousels.

**Related Topics**

- Remove a Third-Party Application
- Manage a Third-Party Application

## Delete Client BFS Servers for Inband or Out-of-Band Carousels

This section describes the procedures for deleting the client BFS servers from the DNCS for either an inband or out-of-band carousel. Deleting the client BFS servers removes the registration of the data carousel from the BFS client.

1. From the DNCS Administrative Console, click the **Application Interface Modules** tab, and then click **BFS Client**. Depending on your system configuration, the following window opens:
   - If you are using a typical DBDS with no RCS, the Broadcast File Server List window opens. Go to step 3.
   - If you are using an RCS, the Please Select a Site window opens. Go to step 2.
2. Click **File > All Sites.** The Broadcast File Server List window opens.
3. From the **Broadcast File Server List** window, select the server that you want to delete.
4. Click **File > Delete**. A confirmation prompt appears.
5. Click **Yes** to confirm this deletion. The cabinet is deleted from the list.
6. Do you need to remove another client BFS server?
   - If **yes**, repeat steps 3 through 5.
   - If **no,** go to step 7.
7. Is your system running in an RCS environment?
   - If **yes**, go to step 8.
   - If **no**, click **File > Close** from the Broadcast File Server List window and then go to Delete the BFS Server Authorized for the Inband or Out-of-Band Carousels.
8. Are there other RCS sites that will use the application you are deleting?
   - If **yes**, repeat steps 2 through 6 until the application is deleted from all of the appropriate RCS sites.
   - If **no**, click **File > Close** from the Please Select a Site window.
9. Go to Delete the BFS Server Authorized for the Inband or Out-of-Band Carousels.

### Related Topics

- Remove a Third-Party Application
- Manage a Third-Party Application

## Delete the BFS Server Authorized for the Inband or Out-of-Band Carousels

This section describes the procedures for deleting the BFS server that is authorized for the data carousel from the DNCS.

1. From the DNCS Administrative Console, click the **Application Interface Modules** tab, and then click **BFS Admin**. Depending on your system configuration, the following window opens:
   - If you are using a typical DBDS with no RCS, the BFS Administration window opens. Go to step 3.
   - If you are using an RCS, the Please Select a Site window opens. Go to step 2.
2. Click **File > All Sites**. The Site AllSites BFS Administration window opens.
3. Click the **Servers** tab.
4. Select the server that is associated with the data carousel for the application you plan to delete.
5. Click **File > Delete**. A confirmation prompt appears.
6. Click **Yes** to confirm the deletion request.
7. Are you running an RCS system?
   - If **yes**, go to step 8.
   - If **no**, keep the BFS Administration window and go to Delete BFS Sources from the Data Carousel for Inband or Out-of-Band Carousels.
8. Does the application you deleted provide data to other sites?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, keep the BFS Administration window and go to Delete BFS Sources from the Data Carousel for Inband or Out-of-Band Carousels.

### Related Topics

- Remove a Third-Party Application
- Manage a Third-Party Application

## Delete BFS Sources from the Data Carousel for Inband or Out-of-Band Carousels

This section describes the procedures for deleting the BFS sources associated with the application you want to delete from an inband or out-of-band data carousel.

1. From the BFS Administration window, click the **Sources** tab.
2. Select the data carousel associated with the application you are deleting.
3. Are you deleting an inband or an out-of-band carousel?
   - If inband, go to step 4.
   - If out-of-band, go to step 5.
4. Make note of the source ID for the inband data carousel.

   **Note:** You will need to know the source when you remove the application from the BIG PAT table.
5. Click **File > Delete**. A confirmation window appears.
6. Click **Yes** to confirm this deletion.
7. Do you need to delete other data carousels from the BFS?
   - If **yes**, repeat steps 3 through 6.
   - If **no**, go to step 8.
8. Is your system running in an RCS environment?
   - If **yes**, go to step 9.
   - If **no**, click **File > Close** from the BFS Administration window. Then go to Remove an Application from the Source List.
9. Are there other RCS sites that were using the data carousels that you deleted?
   - If **yes**, select another site from the Please Select a Site window and go to step 1.
   - If **no**, click **File > Close** from the Site DNCS BFS Administration window. Then go to step 10.
10. Click **File > Select**. The Site DNCS BFS Administration window.
11. From the Site AllSites BFS Administration window, click **File > Close**.
12. From the Please Select a Site window, click **File > Close**.
13. Go to Remove an Application from the Source List.

**Related Topics**

- Remove a Third-Party Application
- Manage a Third-Party Application

## Remove an Application from the Source List

This section describes the procedures for removing the application from the source list on the DNCS.

1. From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.
2. Click **Source** to open the Source List window.
3. Select the source for this application.
4. Click **File > Source Definitions.** The Source Definitions List opens.
5. Are there any source definitions associated with this source?
   - If **yes**, go to step 6.
   - If **no**, go to step 11.
6. Select a session, click **File > Delete**. A confirmation window appears.
7. Click **Yes** to confirm the deletion.
8. Did you delete an SA digital source?
   - If **yes**, a message appears and asks you if you want to teardown the session associated with this source. Click **Yes** and go to step 9.
   - If **no** and are you are deleting a non-SA source, a message appears informing you that SI Manager must be restarted. Click **OK** and go to step 9.

**Note:** For help with restarting SI Manager, refer to the Digital Network Control System Online Help.

9. Do you need to delete another source definition?
   - If **yes**, repeat steps 6 through 8.
   - If **no**, go to step 10.
10. From the Source Definition List window, click **File > Close**.
11. From the Source List window, select the source you want to delete.
12. Click **File > Delete**. A confirmation window appears.
13. Click **Yes** to confirm the deletion. A warning message appears.
14. Read the warning message, and if you would like to continue with the deletion, click **Yes**.
15. From the Source List window, click **File > Close**.
16. Did you delete a non-SA source?
    - If **yes**, stop and restart SI Manager. Then go to step 17.

      **Note**: To stop and restart SI Manager, refer to the Digital Control System Online Help.

    - If **no**, go to step 17.
17. Is the data carousel associated with the application you are removing inband?
    - If **yes**, go to Remove the Inband BFS Carousel from the BIG PAT Table.
    - If **no**, you have completed all procedures for removing an out-of-band data carousel.

**Related Topics**

- Remove a Third-Party Application
- Manage a Third-Party Application

## Remove the Inband BFS Carousel from the BIG PAT Table

This section describes the procedures for removing an inband BFS carousel from the BIG PAT Table.

**Important:** Before you begin this procedure, make sure you know the source ID for the application source.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Does your system include a BIG (your system is not using an ASI card)?
   - If **yes**, click the Element Provisioning tab and then click BIG. The BIG List window opens.
   - If **no**, go to step 5.
3. From the BIG List window, double-click the **BFS BIG**. The Set Up BIG window opens.
4. Click **PAT Configuration** to open the BIG PAT window and go to step 8.
5. From the DNCS Administrative Console, click **Application Interface Modules**, and click **BFS Admin**. The BFS Administration window opens.
6. Select the appropriate host, click **File** and select **Open**. The Set Up BFS Host window opens.
7. Click **PAT Configuration**. The window that opens depends on your system configuration:
   - For systems using Direct ASI, the **Inband Data PAT** window opens.
   - For systems that are not using Direct ASI, the BIG PAT list opens.
8. Select the application session you want to delete and click **Delete Entry**. A message appears and prompts you to confirm the deletion request.
9. Click **Yes** to confirm the deletion. A confirmation message appears.
10. Click **OK**.
11. Do you need to delete an additional inband data carousel?
    - If **yes**, repeat steps 8 through 10.
    - If **no**, go to step 12.
12. On a sheet of paper, write down every entry in the BIG PAT or Inband Data PAT window with a session number greater than the session number for the data carousel you deleted.

    **Important:** Make sure to record the Session MAC address and the session number for each entry.
13. Follow these instructions to delete each entry with a session number great than the session number you deleted.
    - Highlight an out-of-order entry and click **Delete Entry**. A confirmation window opens.
    - Click **OK**. The system deletes the out-of-order entry.

    **Note:** Ignore any BFS restart messages that may appear. You will stop and restart the BFS processes later in this chapter.
14. Click **New Entry**. The BIG PAT Setup window opens.
15. On the **BIG PAT Setup** window, type the Session MAC Address and Session Number for the next out-of-order entry that you recorded on your sheet of paper from step 12.

    **Note:** The Program Number and PMT PID fields are already filled in. Use the default data for these entries.
16. Click **Save**. The system saves the just-added entry in proper ascending order.

17. Repeat steps 14 through 16 for each out-of-order entry that you recorded on the sheep of paper.

**Note:** When you have completed this procedure, all Program Numbers and PMT PIDs will be in ascending order.

18. Choose one of the following options:
    - Systems with a BIG: From the Set Up BIG window, click **Save** and click **Cancel**.
    - Systems with an ASI: From the **Set Up BIG** window, click **Save**.

19. Choose one of the following options:
    - Systems with a BIG: From the BIG List window, click **File** and select **Close**.
    - Systems with an ASI: From the BFS Administration window, click **File** and select **Close**.

20. Go to Stop the BFS Server Processes.

**Related Topics**

- Remove a Third-Party Application
- Manage a Third-Party Application

## Stop the BFS Server Processes

1. If the DNCS Control window is not already open, click the **Control** button in the DNCS area of the DNCS Administrative Console Status. The DNCS Control window opens.
2. Select **bfsServer**.
3. Click **Process > Stop Process.** A confirmation message opens.
4. Click **Yes** to stop the bfsServer process. The indicator next to bfsServer turns red.
5. Go to Tear Down and Rebuild BFS Sessions.

### Related Topics

- Remove a Third-Party Application
- Manage a Third-Party Application

## Tear Down and Rebuild BFS Sessions

This section provides procedures for tearing down and rebuilding BFS sessions. This procedure is required after you delete entries from the PAT table.

1. From the DNCS tab, click the **Utilities** tab, and then click **Session List**. The Session Filter window opens.
2. Select the **BFS QAM** and click **Display Sessions for Selected QAM**. The session data for the BFS QAM appears.
3. Click the **Select** box adjacent to the lowest numbered session. A checkmark appears in the Select box to the left of that session.
4. Click **Teardown Selected Sessions**. The system will tear down all sessions and will then rebuild each session.

   **Note:** It may take a few minutes for all of the sessions to rebuild.

5. When all sessions have been rebuilt (the session IDs are green in color), click **Exit all Session screens**.
6. Go to Restart the BFS Server Processes.

**Related Topics**

- Remove a Third-Party Application
- Manage a Third-Party Application

## Restart the BFS Server Processes

1. If the DNCS Control window is not already open, click the **Control** button in the DNCS area of the DNCS Administrative Console Status. The DNCS Control window opens.
2. From the list of processes, select **bfsServer**.
3. Click **Process > Start Process**.
4. Wait for the indicator next to bfsServer to turn green. A green indicator next to bfsServer means the process has restarted.

### Related Topics

- Remove a Third-Party Application
- Manage a Third-Party Application

## Verify the Number of Sessions After Deleting an Inband Source

This section describes how you can ensure that the inband source was successfully removed from your system.

**Important:** If your system is running in an RCS environment, you will need to locate the respective QAM in which the session was removed.

1. Facing the front of the QAM modulator, press the **OPTIONS** button to cycle through the QAM menu screens until you see the Session Count screen.
2. Make a note of the number of sessions.
3. Did the session count decrease appropriately from the value you recorded in step 2?
   - If **yes**, you have successfully completed these procedures.
   - If **no**, call Cisco Broadband Services.

**Related Topics**

- Remove a Third-Party Application
- Manage a Third-Party Application

# Set Up Services

## Introduction

After all of your network elements are installed and you have entered information about each into the DNCS database, you are ready to set up services for your subscribers.

Overview of Subscriber Services

# Overview

**Important:** If you have subscribers with the Explorer Home Entertainment Server, do not use these procedures to set up services. Instead, refer to Downloading New Client Application Platform Installation Instructions (part number 4003052). To obtain a copy of this document, see Printed Resources.

To see instructions for setting up a particular type of service, click on the service type:

- Clear Services Services that are delivered to subscribers unscrambled or unencrypted; for example, programming available through the three major networks (ABC, CBS, and NBC) is usually clear
- Secure Services Services that are encrypted or scrambled so that they are protected from being accessed (stolen) by people who have not paid for the service; usually offered at a price that is in addition to the price for clear services (for example, HBO, Showtime, and music channels)
- Pay-Per-View (PPV) Services Services that carry PPV events that subscribers can choose to purchase in addition to their normal cable programming; has some of the same characteristics as both clear and secure services
- Video-on-Demand (VOD) Services Services that allow a subscriber to use the remote control to select, purchase, and view a movie; once purchased, the viewer can then forward, reverse, pause, and play the movie just as he or she would with a VCR

**Note:** To learn how to protect encrypted content from unauthorized copying, see Content Protection.

# Clear Services

Clear services are delivered to subscribers "in the clear," meaning unscrambled or unencrypted. For example, programming available through the three major networks (ABC, CBS, and NBC) is usually clear.

Because these services are not encrypted, they are more susceptible to being accessed (stolen) by people who have not paid for the service. Therefore, you may also hear clear services referred to as "non-secure" services.

## Before You Begin

Before you set up clear services in your network, you must make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Setting Up Your Network.

You might also want to have your network map available.

## Time To Complete

Setting up a clear service takes approximately 45 minutes to an hour to complete.

## Performance Impact

Setting up a clear service does not impact network performance. You can complete this procedure at any time.

## Process Overview

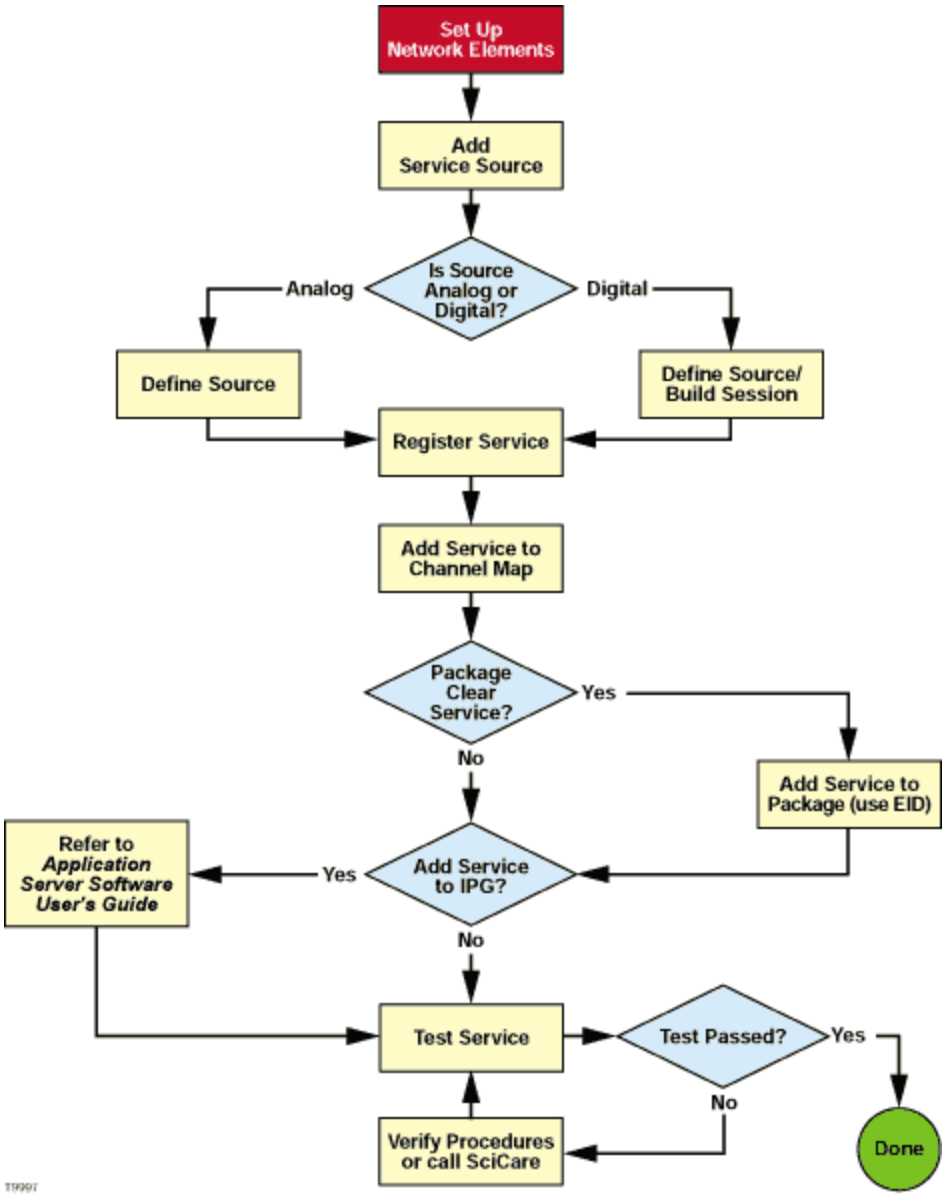
Complete these procedures to set up a clear service in your network. For step-by-step instructions for a particular procedure, click on that procedure.

1. Make sure you have completed all of the necessary steps specified in Setting Up Your Network.
2. Add the service source to the DNCS database.
3. Define parameters for the service source.
4. Do you want to offer the service to only specifically authorized subscribers?
   - If **yes**, go to step 5.
   - If **no**, go to step 6.
5. Add the clear service to a package.
   - If you are adding the clear service to a **new** package, add a service package, and then go to determine and convert the package EID from a hexadecimal to a decimal value. When finished, go to step 6.
   - If you are adding the clear service to an **existing** package, determine and convert the package EID from a hexadecimal to a decimal value.
6. Register the service.
7. Add the service to a channel map.
8. Do you want to include the service on your IPG?
   - If **yes**, refer to Application Server 3.1.2 User's Guide (part number 749606) or the SARA Application Server 3.1.5 User's Guide (part number 4009747) for instructions. When finished, go to step 9. (To obtain a copy of this user's guide, see Printed Resources.)
   - If **no**, go to step 9.

9. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

### Flow Diagram of Setting Up Clear Services

The following diagram illustrates the process of setting up a clear service.



## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

Time to Complete

Adding a content source takes approximately 5 minutes to complete.

Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Define a Content Source

**Note:** These procedures do not apply to VOD services.

After you add a content source to the DNCS database for a clear, secure, or PPV service, define parameters for the source so that the system knows how to process the service content.

**Important:** If you are sending the same source through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same content source through six QAM modulators, you must define the source six times once for each modulator.

## Define an Analog Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Analog**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source in the DNCS. You do not need to define a source for a VOD service.

**Note:** You do not need to build a session for an analog source.

**Important:** If you are sending the same source content through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator.

### You Need to Know

Before You Begin

Before you define an **analog** service source, you must have the following information:

- Name of the source as you defined it when you added the content source
- If the service source is going to only one hub, name of that hub as defined in your network (refer to your network map)
- Number of the channel where the service will be displayed

**Important:** Before you set up a **secure analog service** in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

Time To Complete

Defining an analog source takes approximately 10 minutes to complete.

Performance Impact

Defining an analog source does not impact network performance. You can complete this procedure at any time.

### Analog Source Settings

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪**Default** - Distributes the source to all hubs.<br>▪**Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪**Now** - The service is available for viewing immediately.<br>▪**Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |

### Defining an Analog Source

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define.
5. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
6. Click **File > New Analog**. The Set Up Source Definition window opens.
7. Complete the fields on the screen as described in Analog Source Settings.

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪ **Default** - Distributes the source to all hubs.<br>▪ **Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪ **Now** - The service is available for viewing immediately.<br>▪ **Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source. |

You must type two digits for each value.

**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.

**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

This option is only activated if you select the **Custom** option in the Date/Time field.

8. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source Definition window. The Source Definition List window updates to include the new source information.

9. Do you need to define another analog source for this service?

- If **yes**, repeat this procedure from step 6.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

10. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

11. Click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 13.
- If **no**, your next step is to register the clear service. Go to Register a Service.

13. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

**Define a Digital Source and Session**

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Digital**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source. Then build a session from the source definition. You do not need to define a source and session for a VOD service.

**Important:**

- If you are sending the same source through more than one QAM, MQAM, GQAM, or GoQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator. This also applies to GQAM stat mux dejitter groups (SMDGs).
- If you are setting up a CF session as a **stat mux dejitter group (SMDG)** session, the session must use the same input port and output port that the SMDG uses. Otherwise, the session may fail. You can set up a maximum of 60 sessions on an SMDG. For assistance setting up an SMDG, see Setting Up Stat Mux Dejitter Groups.

**You Need to Know**

Before You Begin

Before you define a digital service source, you must have the following information:

- Name of the service source as you defined it when you added the content source
- Number of the channel where the service will be displayed
- Service source ID as you defined it when you added the content source
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)
- As part of defining a digital session, you will identify the bandwidth that the session requires and the QAM carrier that the session uses. When assigning sessions to a QAM carrier, use the following guidelines to ensure that the throughput is sized appropriately for the carrier.
  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

**Example:** Placing 10 video streams at 3.75 Mbps on a single QAM carrier would require 37.5 Mbps, plus an additional 0.375 Mbps (for overhead), resulting in a total of 37.875 Mbps bandwidth used. In this example, a 256-QAM modulator would have 0.936 Mbps of unused bandwidth on the QAM carrier, and no additional services could be placed on this carrier without resulting in a loss of quality.

Time To Complete

Defining a digital content source and building a session from the source definition takes approximately 20 minutes to complete.

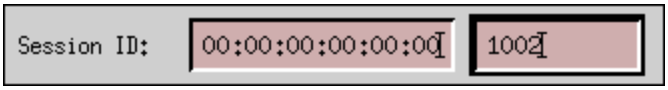
Performance Impact

Defining a digital content source and building a session from the source definition does not impact network

performance. You can complete this procedure at any time.

### Digital Source and Session Settings

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br><br>**Right Session ID field** - The source ID you used when you added the content source.<br><br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br><br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br><br>You must type two digits for the month and day, and four digits for the year.<br><br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br><br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br><br>You must type two digits for each value.<br><br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br><br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br><br>Select the **Broadcast programming** option because this source will provide broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br><br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.

- Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
- For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

| | | |
|---|---|---|
| Wrap-up | See below for more information pertinent to the specific output device you selected. | |
| | ASI ports on a QAM, MQAM, or GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| | GbE ports on a GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 |

| | |
|---|---|
| | Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪**Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪**GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪**MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps |

for each QAM carrier.

○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

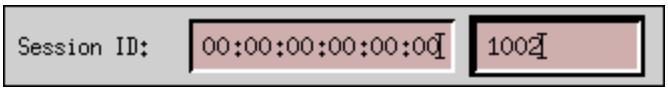
▪**Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.

▪**Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

### Defining a Digital Source and Session

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define and click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
5. Click **File > New Digital**. The Digital Source Set Up window opens.
6. Complete the fields on the screen as described in Digital Source and Session Settings.

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br>**Right Session ID field** - The source ID you used when you added the content source.<br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br>Select the **Broadcast programming** option because this source will provide |

| | |
|---|---|
| | broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
- Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
- For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

| | | |
|---|---|---|
| Wrap-up | See below for more information pertinent to the specific output device you selected. | |
| | ASI ports on a QAM, MQAM, or GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| | GbE ports on a GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program |

| | |
|---|---|
| | number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪ **Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪ **GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪ **MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪ **Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the |

UpConverter (if used).

- **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.

**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:

  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

- **Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.
- **Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

7. On the Save Source Definition window, click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

8. Do you need to define another digital source for this service?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

**Note:** You would define more than one digital service source if you have more than one MPEG source feeding the same content into different portions of your network.

9. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

10. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 11.
- If **no**, your next step is to register the clear service. Go to Register a Service.

11. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

## Register a Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > File > New**

**Note:** This procedure does not apply to PPV services.

Registering a service with the SAM achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT
- Communicates the operation attributes to the DHCTs in your network
- Registers the service and its operation attributes with the BFS

For example, to access a standard audio/video program service, a DHCT must download the WatchTV application. The WatchTV application contains the operation attributes that tell the DHCT how to tune to and display a standard audio/video program service so that subscribers can hear and view the service. In the case of a VOD service, a DHCT must download a PTV (PowerTV) file to serve the same purpose.

In addition, if the service is to be included as part of a package, registering the service associates it with the specified package.

**Important:** Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot.

**Note:** If you want to adjust how often the SAM communicates service operation attributes to the DHCTs in your network, go to Scheduling Service Updates.

### You Need to Know

When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

### Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

## Register a Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > File > New**

**Note:** This procedure does not apply to PPV services.

Registering a service with the SAM achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT
- Communicates the operation attributes to the DHCTs in your network
- Registers the service and its operation attributes with the BFS

For example, to access a standard audio/video program service, a DHCT must download the WatchTV application. The WatchTV application contains the operation attributes that tell the DHCT how to tune to and display a standard audio/video program service so that subscribers can hear and view the service. In the case of a VOD service, a DHCT must download a PTV (PowerTV) file to serve the same purpose.

In addition, if the service is to be included as part of a package, registering the service associates it with the specified package.

**Important:** Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot.

**Note:** If you want to adjust how often the SAM communicates service operation attributes to the DHCTs in your network, go to Scheduling Service Updates.

### You Need to Know

When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

### Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### Service Registration Settings

Use the following fields when you register a service in the DNCS.

| Field | Description |
|---|---|
| Service Name | The name you want to use to identify this service (for example, Discovery Kids).<br>You can use up to 20 alphanumeric characters. |
| Short Description | A brief description of this service.<br>You can use up to 5 alphanumeric characters.<br>**Example:** For the Discovery Kids service, you might type **DSCK**.<br>This description will appear on the IPG and on the channel banner on the subscriber's television screen. |
| Long Description | A detailed description of this service.<br>You can use up to 32 alphanumeric characters.<br>This information is for your benefit only. Subscribers will not see this information. |
| Application URL | Path on the BFS where the software file resides.<br>Type the following information:<br>▪Path on the BFS where the software file resides (for example, **bfs://resapp/watchtv**)<br>▪**Note:** You can also click **Select** to select the path from the list that appears.<br>▪If the service is a VOD service, type a semicolon (**;**) and then **EID=<decimal equivalent of EID>** (if necessary, refer to Determine and Convert a Package EID)<br>▪If the service is a VOD service, type a semicolon (**;**) and then **level2-TRUE**<br>Your final entry should look similar to the following example: **bfs://resapp/watchtv;EID=83;level2-TRUE** for VOD services or **bfs://resapp/watchtv** for non-VOD services.<br>**Note:** You can also click **Select** to select the path from the list that appears. |
| Logo | The number for the logo associated with this service, if required. |
| Parameter | Define the type of service:<br>▪For a VOD service, type **0**.<br>▪For a clear or secure service, type the **service source ID** that you assigned when you added the service source. |

### Registering a Service

Complete these steps to register a service.

**Note:** This procedure does not apply to PPV services.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens.
3. Click **File > New**. The Set Up SAM Service window opens.
4. Complete the fields on the screen as described in Service Registration Settings.

Use the following fields when you register a service in the DNCS.

| Field | Description |
|---|---|
| Service Name | The name you want to use to identify this service (for example, Discovery Kids).<br>You can use up to 20 alphanumeric characters. |
| Short Description | A brief description of this service.<br>You can use up to 5 alphanumeric characters.<br>**Example:** For the Discovery Kids service, you might type **DSCK**.<br>This description will appear on the IPG and on the channel banner on the subscriber's television screen. |
| Long Description | A detailed description of this service.<br>You can use up to 32 alphanumeric characters.<br>This information is for your benefit only. Subscribers will not see this information. |
| Application URL | Path on the BFS where the software file resides.<br>Type the following information:<br>▪ Path on the BFS where the software file resides (for example, **bfs://resapp/watchtv**)<br>▪ **Note:** You can also click **Select** to select the path from the list that appears.<br>▪ If the service is a VOD service, type a semicolon (**;**) and then **EID=<decimal equivalent of EID>** (if necessary, refer to Determine and Convert a Package EID)<br>▪ If the service is a VOD service, type a semicolon (**;**) and then **level2-TRUE**<br>Your final entry should look similar to the following example: **bfs://resapp/watchtv;EID=83;level2-TRUE** for VOD services or **bfs://resapp/watchtv** for non-VOD services.<br>**Note:** You can also click **Select** to select the path from the list that appears. |
| Logo | The number for the logo associated with this service, if required. |
| Parameter | Define the type of service:<br>▪ For a VOD service, type **0**.<br>▪ For a clear or secure service, type the **service source ID** that |

you assigned when you added the service source.

5.Click **Save**. The system saves the service information in the DNCS database, registers the service with the BFS, and closes the Set Up SAM Service window. The SAM Service List window updates to include the new service with its Service ID.

6.Record the Service ID that the system assigns to the service. You will need it when you add the service to the IPG. In the following example, the Service ID is 196.

| Short Description | Service Name | Service ID | URL Tag |
|---|---|---|---|
| HPPV | PPV HBO | 196 | ippv |

7.Do you need to register another service with the SAM?

- If yes, repeat this procedure from step 3.
- If no, click **File > Close** to close the SAM Service List window and return to the DNCS Administrative Console.

8.Your next step is to add the service to a channel map. Does a channel map already exist to which you want to add this service?

- If **yes**, go to Add a Service to a Channel Map.
- If **no**, go to Add a Channel Map.

## Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

### You Need to Know

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

### Guidelines for Adding Services

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.
- You must add a service package for each VOD service. Otherwise, your authorized subscribers will not be able to access the VOD service.
- Because clear services are not encrypted, packaging a clear service does not protect it from being

accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

**Related Topics**

- Service Package Settings
- Adding a Service Package

## Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

### You Need to Know

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

### Guidelines for Adding Services

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.
- You must add a service package for each VOD service. Otherwise, your authorized subscribers will not be able to access the VOD service.
- Because clear services are not encrypted, packaging a clear service does not protect it from being

accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

**Related Topics**

- Service Package Settings
- Adding a Service Package

## Service Package Settings

Use the following fields when you manage a service package in the DNCS.

| Field | Description |
|---|---|
| Package Name | The name that identifies this package.<br><br>You can use up to 20 alphanumeric characters.<br><br>**Important:** The package name that you enter must be compatible with the package name rules that your billing system uses. Default packages (those used for InstaStaging) are the only exception.<br><br>**Notes:**<br><br>▪The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br><br>▪Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Default Staging Package | Allows you to define a package as a default staging package.<br><br>This option appears only if you have enabled InstaStaging on the DNCS.<br><br>**Notes:**<br><br>▪The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br><br>▪Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Duration | Allows subscribers to have unlimited access to the package.<br><br>The **Unlimited** option in the Duration field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services. |
| Pay Per View | Not supported at this time. |
| Impulse Pay Per View | Not supported at this time. |
| Allow Event Extension | Not supported at this time. |

## Related Topics

- Adding a Service Package
- Guidelines for Adding Services

### Adding a Service Package

Complete these steps to add a new service package to the DNCS.

**Note:** This procedure applies to secure, VOD, and packaged clear services and default staging packages when using InstaStaging. It does not apply to PPV or unpackaged clear services.

**Packages for InstaStaging:** If you are adding default packages for use with InstaStaging, be aware that you can specify multiple default packages. In addition, if your site is a SARA site and uses a Service Disconnect package (sometimes referred to as a "brick mode" package), be sure that the default staging option is selected for the Service Disconnect package.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.

   **Note:** By default, the Package List window shows only non-PPV packages (Subscription Only). To view the list of all packages, click the **Show** button and select **All Packages**.

4. Click **File > New**. The Set Up Package window opens.
5. Complete the fields on the screen as described in Service Package Settings.

Use the following fields when you manage a service package in the DNCS.

| Field | Description |
|---|---|
| Package Name | The name that identifies this package.<br><br>You can use up to 20 alphanumeric characters.<br><br>**Important:** The package name that you enter must be compatible with the package name rules that your billing system uses. Default packages (those used for InstaStaging) are the only exception.<br><br>**Notes:**<br>▪ The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br>▪ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Default Staging Package | Allows you to define a package as a default staging package.<br><br>This option appears only if you have enabled InstaStaging on the DNCS.<br><br>**Notes:**<br>▪ The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br>▪ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Duration | Allows subscribers to have unlimited access to the package.<br><br>The **Unlimited** option in the Duration field is selected by default. This option |

| | |
|---|---|
| | allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services. |
| Pay Per View | Not supported at this time. |
| Impulse Pay Per View | Not supported at this time. |
| Allow Event Extension | Not supported at this time. |

**Related Topics**

- Adding a Service Package
- Guidelines for Adding Services

6.Click **Save**. The system saves the package information in the DNCS database and closes the Set Up Package window. The Package List window updates to include the new package.

**Note:** If you are using InstaStaging and have created a default staging package, an asterisk (*) appears next to this package to indicate it is a default staging package.

7.Are you using our RCS solution?

- If **yes**, go to step 8.
- If **no**, go to step 9.

8.Are there other RCS sites that will use the third-party application that this package provides?

- If **yes**, repeat this procedure from step 4 to add a package to another site.
- If **no**, go to step 9.

9.Do you need to add a secure service to this package?

- If **yes**, go to Adding a Secure Service to a Package.
- If no, go to step 10.

10.Do you need to add a VOD or clear service to this package?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to step 11.

11.Are you setting up Instastaging?

- If **yes**, you need to Identify Existing Packages as Default Packages.
- If **no**, go to step 12.

12.Click **File > Close** to close the Package List window.

13.Go to Registering a Service.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

**Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?
   - If **yes**, go to Split a Channel.
   - If **no**, go to step 9.
9. Do you need to add another service to this channel map?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
10. Do you need to add a service to another channel map?
    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.
11. Do you need to include the service on your IPG?
    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.
12. Is this is a VOD service?
    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.
13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
1. Click **Channel Maps**. The Display Channel Map List window opens.
1. Click once on the row containing the channel map to which you want to add this service.

**Note:** If you select the Default channel map, this service will be available to all hubs.

1. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
1. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

1. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
1. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
1. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?
    - If **yes**, go to Split a Channel.
    - If **no**, go to step 9.
1. Do you need to add another service to this channel map?
    - If **yes**, repeat this procedure from step 5.
    - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
1. Do you need to add a service to another channel map?
    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.
1. Do you need to include the service on your IPG?
    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.
1. Is this is a VOD service?
    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.
1. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

## Test a Service

**Note:** Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops for services with your billing system vendor.

After you have completed all the steps in setting up a particular type of service, verify that you set up the service successfully by using a test set-top and a television.

Is the new service packaged?

- If **yes**, first authorize the set-top to receive the package.
- If **no**, verify a successful service setup by trying to access the service.

**Related Topics**

- Authorize a Set-Top for a Service
- Verify a Successful Service Setup
- Locating a Set-Top MAC Address

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

▸ Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

▸ Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

▸ Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

▸ Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

▸ Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

▸ Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Locating a Set-Top MAC Address

To locate the MAC address of a set-top, do one of the following:

- Display the set-top diagnostic screens.
- Look on the back of the set-top for a label with the MAC address recorded on it.

# Secure Services

## Set Up Secure Services

In contrast to a clear service, a secure service is encrypted or scrambled so that it is protected from being accessed (stolen) by people who have not paid for the service. Encrypted services are considered to be more "secure" from theft than clear services. We use the PowerKEY Conditional Access (CA) system to secure services.

Secure services are usually offered to subscribers at a price that is in addition to the price they pay for clear services. Following are some examples of secure services:

- HBO
- Showtime
- Music channels

## Before You Begin

Before you set up secure services in your network, you must make sure all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Setting Up Your Network.

You may also want to have your network map available.

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370). (To obtain a copy of this guide, see Printed Resources .)

## Time To Complete

Setting up a secure service takes approximately 45 minutes to an hour to complete.

## Performance Impact

Setting up a secure service does not impact network performance. You can complete this procedure at any time.

# Secure Services

## Set Up Secure Services

In contrast to a clear service, a secure service is encrypted or scrambled so that it is protected from being accessed (stolen) by people who have not paid for the service. Encrypted services are considered to be more "secure" from theft than clear services. We use the PowerKEY Conditional Access (CA) system to secure services.

Secure services are usually offered to subscribers at a price that is in addition to the price they pay for clear services. Following are some examples of secure services:

- HBO
- Showtime
- Music channels

## Before You Begin

Before you set up secure services in your network, you must make sure all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Setting Up Your Network.

You may also want to have your network map available.

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370). (To obtain a copy of this guide, see Printed Resources .)

## Time To Complete

Setting up a secure service takes approximately 45 minutes to an hour to complete.

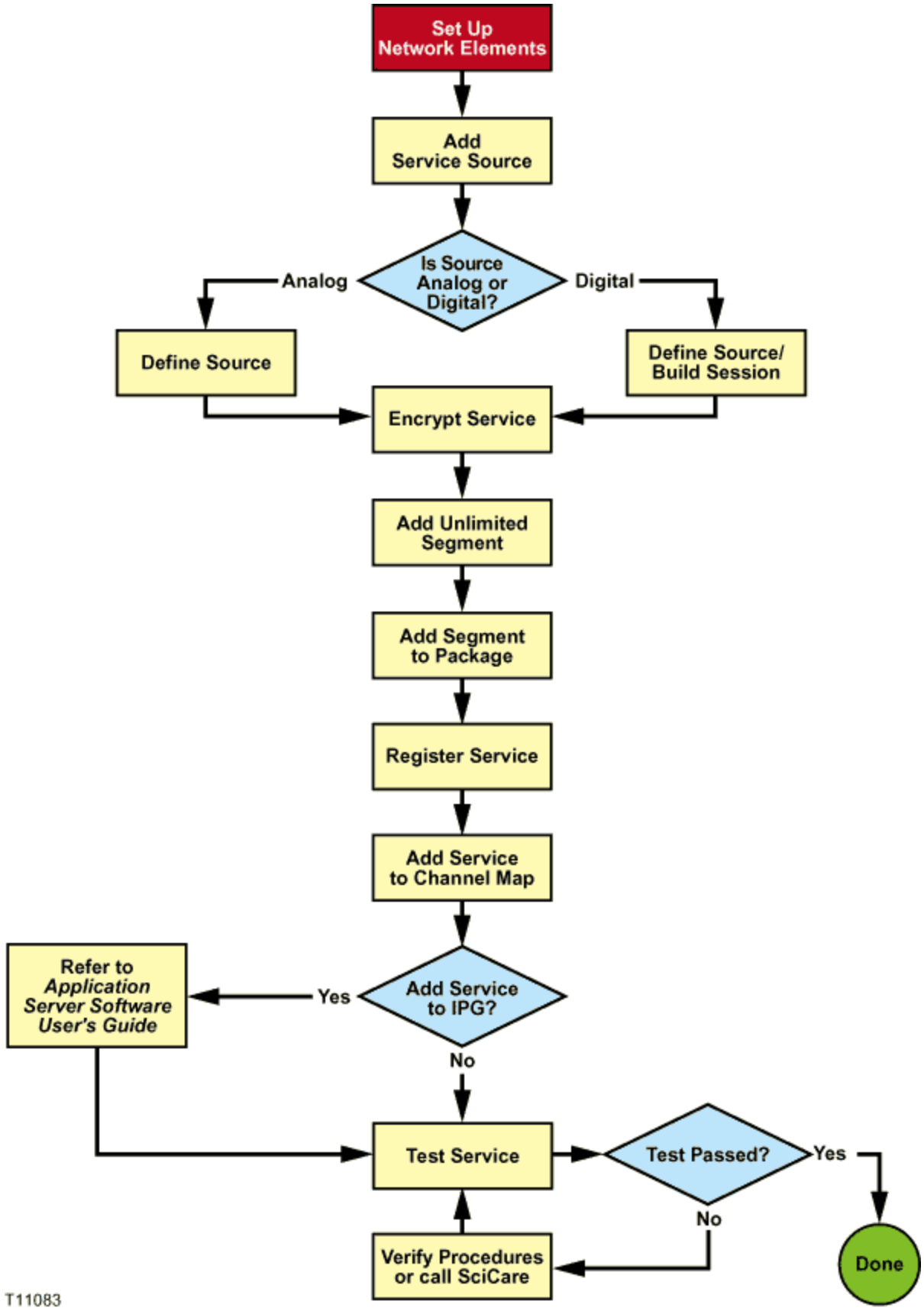
## Performance Impact

Setting up a secure service does not impact network performance. You can complete this procedure at any time.

### Flow Diagram for Setting Up Secure Services

The following diagram illustrates the process of setting up a secure service.

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370). (To obtain a copy of this guide, see Printed Resources .)


Set Up Network Elements
Add Service Source
Is Source Analog or Digital?
Analog
Digital
Define Source
Define Source/ Build Session
Encrypt Service
Add Unlimited Segment
Add Segment to Package
Register Service
Add Service to Channel Map
Add Service to IPG?
Yes
Refer to Application Server Software User's Guide
No
Test Service
Test Passed?
Yes
No
Verify Procedures or call SciCare
Done
T11083

### Setting Up Secure Services

Complete these procedures to set up a secure service in your network. For step-by-step instructions for a particular procedure, click on that procedure.

1. Make sure you have completed all of the necessary steps specified in Setting Up Your Network.
2. Add the service source to the DNCS database.
3. Define parameters for the service source.
4. Encrypt the content coming from the service source so that it is available only to authorized subscribers.
5. Add an unlimited segment for the service.
6. Add the service segment to a package.
7. Register the service.
8. Add the service to a channel map.
9. Do you want to include the service on your IPG?
    - If **yes**, refer to SARA Application Server 3.4.1 User's Guide (part number 4012159) for instructions. (To obtain a copy of this guide, see Printed Resources.)
    - If **no**, go to step 10.
10. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Define a Content Source

**Note:** These procedures do not apply to VOD services.

After you add a content source to the DNCS database for a clear, secure, or PPV service, define parameters for the source so that the system knows how to process the service content.

**Important:** If you are sending the same source through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same content source through six QAM modulators, you must define the source six times once for each modulator.

## Define an Analog Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Analog**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source in the DNCS. You do not need to define a source for a VOD service.

**Note:** You do not need to build a session for an analog source.

**Important:** If you are sending the same source content through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator.

### You Need to Know

Before You Begin

Before you define an **analog** service source, you must have the following information:

- Name of the source as you defined it when you added the content source
- If the service source is going to only one hub, name of that hub as defined in your network (refer to your network map)
- Number of the channel where the service will be displayed

**Important:** Before you set up a **secure analog service** in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

Time To Complete

Defining an analog source takes approximately 10 minutes to complete.

Performance Impact

Defining an analog source does not impact network performance. You can complete this procedure at any time.

### Analog Source Settings

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪**Default** - Distributes the source to all hubs.<br>▪**Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪**Now** - The service is available for viewing immediately.<br>▪**Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |

### Defining an Analog Source

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define.
5. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
6. Click **File > New Analog**. The Set Up Source Definition window opens.
7. Complete the fields on the screen as described in Analog Source Settings.

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪ **Default** - Distributes the source to all hubs.<br>▪ **Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪ **Now** - The service is available for viewing immediately.<br>▪ **Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source. |

You must type two digits for each value.

**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.

**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

This option is only activated if you select the **Custom** option in the Date/Time field.

8. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source Definition window. The Source Definition List window updates to include the new source information.

9. Do you need to define another analog source for this service?

- If **yes**, repeat this procedure from step 6.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

10. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

11. Click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 13.
- If **no**, your next step is to register the clear service. Go to Register a Service.

13. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

### Define a Digital Source and Session

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Digital**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source. Then build a session from the source definition. You do not need to define a source and session for a VOD service.

**Important:**

- If you are sending the same source through more than one QAM, MQAM, GQAM, or GoQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator. This also applies to GQAM stat mux dejitter groups (SMDGs).
- If you are setting up a CF session as a **stat mux dejitter group (SMDG)** session, the session must use the same input port and output port that the SMDG uses. Otherwise, the session may fail. You can set up a maximum of 60 sessions on an SMDG. For assistance setting up an SMDG, see Setting Up Stat Mux Dejitter Groups.

**You Need to Know**

Before You Begin

Before you define a digital service source, you must have the following information:

- Name of the service source as you defined it when you added the content source
- Number of the channel where the service will be displayed
- Service source ID as you defined it when you added the content source
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)
- As part of defining a digital session, you will identify the bandwidth that the session requires and the QAM carrier that the session uses. When assigning sessions to a QAM carrier, use the following guidelines to ensure that the throughput is sized appropriately for the carrier.
  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

**Example:** Placing 10 video streams at 3.75 Mbps on a single QAM carrier would require 37.5 Mbps, plus an additional 0.375 Mbps (for overhead), resulting in a total of 37.875 Mbps bandwidth used. In this example, a 256-QAM modulator would have 0.936 Mbps of unused bandwidth on the QAM carrier, and no additional services could be placed on this carrier without resulting in a loss of quality.

Time To Complete

Defining a digital content source and building a session from the source definition takes approximately 20 minutes to complete.

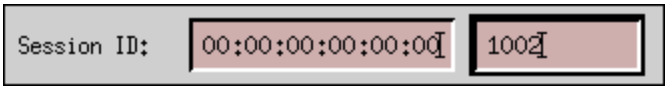
Performance Impact

Defining a digital content source and building a session from the source definition does not impact network

performance. You can complete this procedure at any time.

### Digital Source and Session Settings

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br><br>**Right Session ID field** - The source ID you used when you added the content source.<br><br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br><br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br><br>You must type two digits for the month and day, and four digits for the year.<br><br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br><br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br><br>You must type two digits for each value.<br><br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br><br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br><br>Select the **Broadcast programming** option because this source will provide broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br><br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.

| | |
|---|---|
| | ▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| Wrap-up | See below for more information pertinent to the specific output device you selected. |
| ASI ports on a QAM, MQAM, or GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| GbE ports on a GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 |

| | |
|---|---|
| | Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪**Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪**GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪**MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps |

for each QAM carrier.

○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

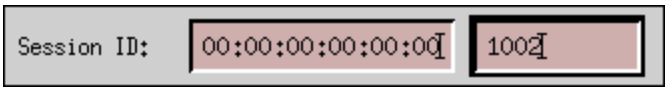
▪**Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.

▪**Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

### Defining a Digital Source and Session

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define and click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
5. Click **File > New Digital**. The Digital Source Set Up window opens.
6. Complete the fields on the screen as described in Digital Source and Session Settings.

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br>**Right Session ID field** - The source ID you used when you added the content source.<br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br>Select the **Broadcast programming** option because this source will provide |

| | |
|---|---|
| | broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
- Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
- For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

| | | |
|---|---|---|
| Wrap-up | See below for more information pertinent to the specific output device you selected. | |
| | ASI ports on a QAM, MQAM, or GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| | GbE ports on a GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program |

| | |
|---|---|
| | number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪ **Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪ **GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪ **MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪ **Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the |

UpConverter (if used).

- **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.

**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:

  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

- **Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.
- **Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

7. On the Save Source Definition window, click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

8. Do you need to define another digital source for this service?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

**Note:** You would define more than one digital service source if you have more than one MPEG source feeding the same content into different portions of your network.

9. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

10. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 11.
- If **no**, your next step is to register the clear service. Go to Register a Service.

11. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

## Encrypt a Service

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Security Modes > File > New**

**Note:** This procedure applies to secure and PPV services. It does not apply to clear or VOD services.

After you define a secure or PPV service source, you must set the system to encrypt all of the content coming from that source. Encryption ensures that this content is available only to authorized subscribers.

### You Need to Know

Time to Complete

Encrypting a service takes approximately 10 minutes to complete.

Performance Impact

Encrypting a service does not impact network performance. You can complete this procedure at any time.

### Service Encryption Settings

Use the following fields when you encrypt a service in the DNCS.

| Field | Description |
|---|---|
| Security Mode | Determines whether the service is encrypted. |
| Security Mode | The security mode of the service:<br>▪Select the **Clear** option to distribute the service in the clear (unencrypted)<br>▪Select the **Encrypted** option to distribute the service as an encrypted service |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪**Now** - The service is available for viewing immediately<br>▪**Custom** - Set a specific date and time for service availability in the **Effective Date a**nd **Effective Time** fields |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** Type July 4, 2008, as **07042008**. The system inputs the slashes for you and displays 07/04/2003.<br>This option is only activated if you select the **Custom** option in Date/Time. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** Type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>**Notes:**<br>▪Make sure the time you enter is at least 15 minutes into the future.<br>▪You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in Date/Time. |
| AM/PM | Establishes which portion of the day you want the system to begin encrypting this service.<br>Select either **AM** or **PM** from the list. |

### Encrypting a Service

Complete these steps to encrypt service content.

**Note:** This procedure applies to secure and PPV services. It does not apply to clear or VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you want to encrypt.
5. Click **File > Security Modes**. The Security Mode List window opens for the service source you selected.
6. Click **File > New**. The Set Up Security Mode window opens.
7. Complete the fields on the screen as described in Service Encryption Settings.

Use the following fields when you encrypt a service in the DNCS.

| Field | Description |
|---|---|
| Security Mode | Determines whether the service is encrypted. |
| Security Mode | The security mode of the service:<br>▪ Select the **Clear** option to distribute the service in the clear (unencrypted)<br>▪ Select the **Encrypted** option to distribute the service as an encrypted service |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪ **Now** - The service is available for viewing immediately<br>▪ **Custom** - Set a specific date and time for service availability in the **Effective Date a**nd **Effective Time** fields |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** Type July 4, 2008, as **07042008**. The system inputs the slashes for you and displays 07/04/2003.<br>This option is only activated if you select the **Custom** option in Date/Time. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** Type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>**Notes:**<br>▪ Make sure the time you enter is at least 15 minutes into the future.<br>▪ You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in |

| | |
|---|---|
| | Date/Time. |
| AM/PM | Establishes which portion of the day you want the system to begin encrypting this service.<br><br>Select either **AM** or **PM** from the list. |

8. Click **Save**. The system saves the encryption information in the DNCS database and closes the Set Up Security Mode window. The Security Mode List window updates to include the new encryption information.

9. Do you need to set up another security mode for this service source? For example, you may want to allow all of your subscribers to have access to a normally encrypted service (such as HBO) for a limited time (such as a weekend) in an attempt to entice more people to purchase the service.

- If **yes**, repeat this procedure from step 6.
- If **no**, go to step 10.

10. Click **File > Close** to close the Security Mode List window and return to the Source List window.

11. Is this a secure service?

- If **yes**, your next step is to add an unlimited segment for the service source. Go to Add an Unlimited Segment.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Your next step is to create the PPV service and add it to the IPG as described in the SARA Application Server 3.4.1 User's Guide (part number 4012159). To obtain this guide, refer to Printed Resources. When finished, go to Add a Service to a Channel Map.

## Add an Unlimited Segment

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Segments > File > New**

**Important:** Follow this procedure to set up secure services only. Do not use this procedure to set up clear, PPV, or VOD services.

After you encrypt a secure service, you must set up an unlimited segment for that service source. Setting up an unlimited segment for a source instructs the system to continuously send content from that source. This allows authorized subscribers to access the service content at any time.

**Note:** Currently, there are no services that you set up in the DNCS that use limited segments.

### Time To Complete

Adding an unlimited segment takes approximately 10 minutes to complete.

### Performance Impact

Adding an unlimited segment does not impact network performance. You can complete this procedure at any time.

### Unlimited Segment Settings

Use the following fields when you manage unlimited segments in the DNCS.

| Field | Description |
|---|---|
| Name | The name that identifies this segment.<br>You can use up to 20 alphanumeric characters. |
| Duration | The duration of this segment.<br>Since this is an unlimited segment, select **Unlimited**. |
| Do not complete the **Start Date** and **Start Time** fields. The DNCS automatically selects the current date as the start date, with the start time several minutes in the future. | |
| Blackout/Spotlight Control | Not currently supported.<br>Select **None**. |
| Fingerprint | Not currently supported.<br>Select **None**. |
| Digital Copy Rights | The content protection for 1394 ports that receive this segment, appropriate for your system:<br>▪**Copy Never** - Prevents subscribers from making a copy of any program or event associated with this segment.<br>The FCC does not permit a segment to be marked "Copy Never" unless that segment is being used for pay-per-view (PPV).<br>▪**Copy One Generation** - Allows subscribers to make a single copy of any program or event associated with this segment.<br>▪**Copy Freely** - Allows subscribers to make as many copies as they like of any program or event associated with this segment. |
| Macrovision | Sets the content protection of PPV or VOD on analog composite output ports that receive this segment, appropriate for your system:<br>▪**Enabled** - Use the Macrovision content protection process to prevent subscribers from copying all events that this segment processes.<br>**Note:** If you select Enabled, an informational window should open that describes the licensing restrictions of the Macrovision protection process.<br>Did the informational window open?<br>○If **yes**, click **OK**.<br>○If **no**, contact Cisco Services.<br>▪**Disabled** - Do not use Macrovision content protection.<br>▪**Follow Package Definition** - Not currently supported |
| CIT (constrained image trigger) flag | Sets content protection on YPbPr (component) high-definition analog output ports that receive this segment, appropriate for your system:<br>▪**Clear** - Allows high-definition analog outputs to display video at full HD resolution.<br>▪**Set** - Cause high-definition analog outputs to reduce the effective image resolution to less than 520,000 pixels. |

**Note:** Setting the CIT flag may not change the actual resolution displayed on a high-definition analog output. Instead, some DHCT vendors may choose to apply bandwidth filtering to reduce the image resolution.

### Adding an Unlimited Segment

**Important:** If you are using Macrovision content protection and you are setting up two unlimited segments from the same content, make sure that all of the segments use the same level of Macrovision. Otherwise, content protection may not work as expected for these segments.

**Note:** This procedure applies only to secure services. It does not apply to clear, PPV, or VOD services.

1. Is the Source List window open?
   - If **yes**, go to step 5.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **System Provisioning** tab.
4. Click **Source**. The Source List window opens.
5. Click once on the row containing the service source for which you are setting up an unlimited segment.
6. Click **File > Segments**. The Segment List (by Source) window opens for the source you selected.
7. Click **File > New**. The Set Up Segment window opens.
8. Complete the fields on the screen as described in Unlimited Segment Settings.

Use the following fields when you manage unlimited segments in the DNCS.

| Field | Description |
|---|---|
| Name | The name that identifies this segment.<br>You can use up to 20 alphanumeric characters. |
| Duration | The duration of this segment.<br>Since this is an unlimited segment, select **Unlimited**. |
| Do not complete the **Start Date** and **Start Time** fields. The DNCS automatically selects the current date as the start date, with the start time several minutes in the future. | |
| Blackout/Spotlight Control | Not currently supported.<br>Select **None**. |
| Fingerprint | Not currently supported.<br>Select **None**. |
| Digital Copy Rights | The content protection for 1394 ports that receive this segment, appropriate for your system:<br>▪**Copy Never** - Prevents subscribers from making a copy of any program or event associated with this segment. The FCC does not permit a segment to be marked "Copy Never" unless that segment is being used for pay-per-view (PPV).<br>▪**Copy One Generation** - Allows subscribers to make a single copy of any program or event associated with this segment.<br>▪**Copy Freely** - Allows subscribers to make as many copies as they like of any program or event associated with this segment. |
| Macrovision | Sets the content protection of PPV or VOD on analog composite output ports that receive this segment, appropriate for your system: |

| | |
|---|---|
| | ▪**Enabled** - Use the Macrovision content protection process to prevent subscribers from copying all events that this segment processes.<br>**Note:** If you select Enabled, an informational window should open that describes the licensing restrictions of the Macrovision protection process.<br>Did the informational window open?<br>○ If **yes**, click **OK**.<br>○ If **no**, contact Cisco Services.<br>▪**Disabled** - Do not use Macrovision content protection.<br>▪**Follow Package Definition** - Not currently supported |
| CIT (constrained image trigger) flag | Sets content protection on YPbPr (component) high-definition analog output ports that receive this segment, appropriate for your system:<br>▪**Clear** - Allows high-definition analog outputs to display video at full HD resolution.<br>▪**Set** - Cause high-definition analog outputs to reduce the effective image resolution to less than 520,000 pixels.<br>**Note:** Setting the CIT flag may not change the actual resolution displayed on a high-definition analog output. Instead, some DHCT vendors may choose to apply bandwidth filtering to reduce the image resolution. |

9. Click **Save**. The system saves the segment information in the DNCS database and closes the Set Up Segment window. The Segment List (by Source) window updates to include the new segment information. If you scroll through the list horizontally, you will see a yellow band that indicates when the segment is scheduled to start and its duration.

10. Do you need to set up another unlimited segment for this service source?

▪If **yes**, repeat this procedure from step 7.

**Important:** When creating other segments from the same source, make certain that all segments have the same levels of Macrovision CCI (if used); otherwise, the content protection may not work as expected for these segments.

▪If **no**, click **File > Close** to close the Segment List (by Source) window and return to the Source List window. Go to step 11.

11. Click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Your next step is to add the secure service segment to a package. Does a package already exist to which you want to add this service segment?

▪If **yes**, go to Add a Secure Service to a Package.

▪If **no**, go to Add a Service Package.

## Add a Secure Service to a Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > [Package Name] > File > Provision**

**Note:** This procedure applies only to secure services. It does not apply to clear, PPV, or VOD services.

After you set up an unlimited segment for a secure service, you must add the service segment to a package. A package consists of one or more service segments that are available only to specifically authorized subscribers.

For example, you can offer subscribers different levels of service, such as Basic and Premium. Your Basic service could include nothing but clear services. Because these services are sent to all subscribers in the clear (unencrypted), you do not need to add them to packages.

On the other hand, your Premium service could offer additional services to subscribers who are willing to pay extra for them. You encrypt those additional services to keep them secure from being accessed by anyone who has not paid the extra price for them.

The only way for a subscriber to access secure services is for you to place the secure services in a package, and then authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable that DHCT to decrypt the secure services.

**Important:** The DNCS does not support packages within packages or packages for virtual channels. This ability will be available in a future release of the DNCS.

### Before You Begin

If you need to add a secure service to a new package, you must first add the package to the DNCS. If necessary, go to Add Service Package before you begin this procedure.

### Time To Complete

Adding a secure service to a package takes approximately 10 minutes to complete.

### Performance Impact

Adding a secure service to a package does not impact network performance. You can complete this procedure at any time.

### Adding a Secure Service to a Package

**Note:** This procedure applies only to secure services. It does not apply to clear, PPV, or VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.

   **Note:** By the default, the Package List window shows only non-PPV packages (**Subscription Only**). To view the list of all packages, click the **Show** button and select **All Packages**.

4. Click once on the row containing the package to which you want to add a service segment.
5. Click **File > Provision**. The Package Provisioning window opens for the package you selected.
6. Click **File > Add Segment**. The Segment Selection window opens showing all of the service segments

that have been defined on your system.

**Important:** Although there is an option to add packages to a package, do **not** select this option. This version of the DNCS does not support packages within packages.

7. Click to select the service segment you want to add to this package. You can select more than one segment by holding down the **Ctrl** key as you click on each segment.
8. Click **OK** to close the Segment Selection window. The Package Provisioning window updates to include the service segment(s) you selected for the package.
9. Click **File > Close** to close the Package Provisioning window and return to the Package List window.
10. Do you need to add a service segment to another package?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Package List window and return to the DNCS Administrative Console.
11. Your next step is to register the secure service. Go to Register a Service.

## Add a Secure Service to a Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > [Package Name] > File > Provision**

**Note:** This procedure applies only to secure services. It does not apply to clear, PPV, or VOD services.

After you set up an unlimited segment for a secure service, you must add the service segment to a package. A package consists of one or more service segments that are available only to specifically authorized subscribers.

For example, you can offer subscribers different levels of service, such as Basic and Premium. Your Basic service could include nothing but clear services. Because these services are sent to all subscribers in the clear (unencrypted), you do not need to add them to packages.

On the other hand, your Premium service could offer additional services to subscribers who are willing to pay extra for them. You encrypt those additional services to keep them secure from being accessed by anyone who has not paid the extra price for them.

The only way for a subscriber to access secure services is for you to place the secure services in a package, and then authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable that DHCT to decrypt the secure services.

**Important:** The DNCS does not support packages within packages or packages for virtual channels. This ability will be available in a future release of the DNCS.

### Before You Begin

If you need to add a secure service to a new package, you must first add the package to the DNCS. If necessary, go to Add Service Package before you begin this procedure.

### Time To Complete

Adding a secure service to a package takes approximately 10 minutes to complete.

### Performance Impact

Adding a secure service to a package does not impact network performance. You can complete this procedure at any time.

### Adding a Secure Service to a Package

**Note:** This procedure applies only to secure services. It does not apply to clear, PPV, or VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.

   **Note:** By the default, the Package List window shows only non-PPV packages (**Subscription Only**). To view the list of all packages, click the **Show** button and select **All Packages**.

4. Click once on the row containing the package to which you want to add a service segment.
5. Click **File > Provision**. The Package Provisioning window opens for the package you selected.
6. Click **File > Add Segment**. The Segment Selection window opens showing all of the service segments

that have been defined on your system.

**Important:** Although there is an option to add packages to a package, do **not** select this option. This version of the DNCS does not support packages within packages.

7. Click to select the service segment you want to add to this package. You can select more than one segment by holding down the **Ctrl** key as you click on each segment.
8. Click **OK** to close the Segment Selection window. The Package Provisioning window updates to include the service segment(s) you selected for the package.
9. Click **File > Close** to close the Package Provisioning window and return to the Package List window.
10. Do you need to add a service segment to another package?
    - If **yes**, repeat this procedure from step 4.
    - If **no**, click **File > Close** to close the Package List window and return to the DNCS Administrative Console.
11. Your next step is to register the secure service. Go to Register a Service.

## Register a Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > File > New**

**Note:** This procedure does not apply to PPV services.

Registering a service with the SAM achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT
- Communicates the operation attributes to the DHCTs in your network
- Registers the service and its operation attributes with the BFS

For example, to access a standard audio/video program service, a DHCT must download the WatchTV application. The WatchTV application contains the operation attributes that tell the DHCT how to tune to and display a standard audio/video program service so that subscribers can hear and view the service. In the case of a VOD service, a DHCT must download a PTV (PowerTV) file to serve the same purpose.

In addition, if the service is to be included as part of a package, registering the service associates it with the specified package.

**Important:** Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot.

**Note:** If you want to adjust how often the SAM communicates service operation attributes to the DHCTs in your network, go to Scheduling Service Updates.

### You Need to Know

When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

### Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

## Register a Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > File > New**

**Note:** This procedure does not apply to PPV services.

Registering a service with the SAM achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT
- Communicates the operation attributes to the DHCTs in your network
- Registers the service and its operation attributes with the BFS

For example, to access a standard audio/video program service, a DHCT must download the WatchTV application. The WatchTV application contains the operation attributes that tell the DHCT how to tune to and display a standard audio/video program service so that subscribers can hear and view the service. In the case of a VOD service, a DHCT must download a PTV (PowerTV) file to serve the same purpose.

In addition, if the service is to be included as part of a package, registering the service associates it with the specified package.

**Important:** Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot.

**Note:** If you want to adjust how often the SAM communicates service operation attributes to the DHCTs in your network, go to Scheduling Service Updates.

### You Need to Know

When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

### Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### Service Registration Settings

Use the following fields when you register a service in the DNCS.

| Field | Description |
|---|---|
| Service Name | The name you want to use to identify this service (for example, Discovery Kids).<br>You can use up to 20 alphanumeric characters. |
| Short Description | A brief description of this service.<br>You can use up to 5 alphanumeric characters.<br>**Example:** For the Discovery Kids service, you might type **DSCK**.<br>This description will appear on the IPG and on the channel banner on the subscriber's television screen. |
| Long Description | A detailed description of this service.<br>You can use up to 32 alphanumeric characters.<br>This information is for your benefit only. Subscribers will not see this information. |
| Application URL | Path on the BFS where the software file resides.<br>Type the following information:<br>▪Path on the BFS where the software file resides (for example, **bfs://resapp/watchtv**)<br>▪**Note:** You can also click **Select** to select the path from the list that appears.<br>▪If the service is a VOD service, type a semicolon (**;**) and then **EID=<decimal equivalent of EID>** (if necessary, refer to Determine and Convert a Package EID)<br>▪If the service is a VOD service, type a semicolon (**;**) and then **level2-TRUE**<br>Your final entry should look similar to the following example: **bfs://resapp/watchtv;EID=83;level2-TRUE** for VOD services or **bfs://resapp/watchtv** for non-VOD services.<br>**Note:** You can also click **Select** to select the path from the list that appears. |
| Logo | The number for the logo associated with this service, if required. |
| Parameter | Define the type of service:<br>▪For a VOD service, type **0**.<br>▪For a clear or secure service, type the **service source ID** that you assigned when you added the service source. |

### Registering a Service

Complete these steps to register a service.

**Note:** This procedure does not apply to PPV services.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens.
3. Click **File > New**. The Set Up SAM Service window opens.
4. Complete the fields on the screen as described in Service Registration Settings.

Use the following fields when you register a service in the DNCS.

| Field | Description |
|---|---|
| Service Name | The name you want to use to identify this service (for example, Discovery Kids).<br>You can use up to 20 alphanumeric characters. |
| Short Description | A brief description of this service.<br>You can use up to 5 alphanumeric characters.<br>**Example:** For the Discovery Kids service, you might type **DSCK**.<br>This description will appear on the IPG and on the channel banner on the subscriber's television screen. |
| Long Description | A detailed description of this service.<br>You can use up to 32 alphanumeric characters.<br>This information is for your benefit only. Subscribers will not see this information. |
| Application URL | Path on the BFS where the software file resides.<br>Type the following information:<br>▪ Path on the BFS where the software file resides (for example, **bfs://resapp/watchtv**)<br>▪ **Note:** You can also click **Select** to select the path from the list that appears.<br>▪ If the service is a VOD service, type a semicolon (**;**) and then **EID=<decimal equivalent of EID>** (if necessary, refer to Determine and Convert a Package EID)<br>▪ If the service is a VOD service, type a semicolon (**;**) and then **level2-TRUE**<br>Your final entry should look similar to the following example: **bfs://resapp/watchtv;EID=83;level2-TRUE** for VOD services or **bfs://resapp/watchtv** for non-VOD services.<br>**Note:** You can also click **Select** to select the path from the list that appears. |
| Logo | The number for the logo associated with this service, if required. |
| Parameter | Define the type of service:<br>▪ For a VOD service, type **0**.<br>▪ For a clear or secure service, type the **service source ID** that |

you assigned when you added the service source.

5.Click **Save**. The system saves the service information in the DNCS database, registers the service with the BFS, and closes the Set Up SAM Service window. The SAM Service List window updates to include the new service with its Service ID.

6.Record the Service ID that the system assigns to the service. You will need it when you add the service to the IPG. In the following example, the Service ID is 196.

| Short Description | Service Name | Service ID | URL Tag |
|---|---|---|---|
| HPPV | PPV HBO | 196 | ippv |

7.Do you need to register another service with the SAM?

- If yes, repeat this procedure from step 3.
- If no, click **File > Close** to close the SAM Service List window and return to the DNCS Administrative Console.

8.Your next step is to add the service to a channel map. Does a channel map already exist to which you want to add this service?

- If **yes**, go to Add a Service to a Channel Map.
- If **no**, go to Add a Channel Map.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

**Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?
   - If **yes**, go to Split a Channel.
   - If **no**, go to step 9.
9. Do you need to add another service to this channel map?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
10. Do you need to add a service to another channel map?
    - If **yes**, repeat this procedure from step 3.
    - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.
11. Do you need to include the service on your IPG?
    - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
    - If **no**, go to step 12.
12. Is this is a VOD service?
    - If **yes**, complete any additional procedures required by the vendor of your VOD server.
    - If **no**, go to step 13.
13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

### Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

### Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
1. Click **Channel Maps**. The Display Channel Map List window opens.
1. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

1. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
1. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

1. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
1. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
1. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?
   - If **yes**, go to Split a Channel.
   - If **no**, go to step 9.
1. Do you need to add another service to this channel map?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
1. Do you need to add a service to another channel map?
   - If **yes**, repeat this procedure from step 3.
   - If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.
1. Do you need to include the service on your IPG?
   - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
   - If **no**, go to step 12.
1. Is this is a VOD service?
   - If **yes**, complete any additional procedures required by the vendor of your VOD server.
   - If **no**, go to step 13.
1. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

## Test a Service

**Note:** Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops for services with your billing system vendor.

After you have completed all the steps in setting up a particular type of service, verify that you set up the service successfully by using a test set-top and a television.

Is the new service packaged?

- If **yes**, first authorize the set-top to receive the package.
- If **no**, verify a successful service setup by trying to access the service.

**Related Topics**

- Authorize a Set-Top for a Service
- Verify a Successful Service Setup
- Locating a Set-Top MAC Address

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

▸ Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

▸ Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

▸ Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

▸ Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

▸ Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

▸ Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Locating a Set-Top MAC Address

To locate the MAC address of a set-top, do one of the following:

- Display the set-top diagnostic screens.
- Look on the back of the set-top for a label with the MAC address recorded on it.

# PPV Services

A PPV service carries PPV events that subscribers can choose to purchase in addition to their normal cable programming. A PPV service has some of the same characteristics as both a clear and a secure service.

Like a clear service, subscribers can always access a PPV service by tuning to a channel that carries the service. The channel displays a banner that advertises the PPV events that subscribers can purchase through that PPV service.

However, like a secure service, the content for a PPV service is encrypted so that only subscribers who have paid for the content can access the content. In this case, the content is a PPV event.

## Before You Begin

Before you set up PPV services in your network, you must make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to Setting Up Your Network.

You also want to have your network map readily available.

## Time to Complete

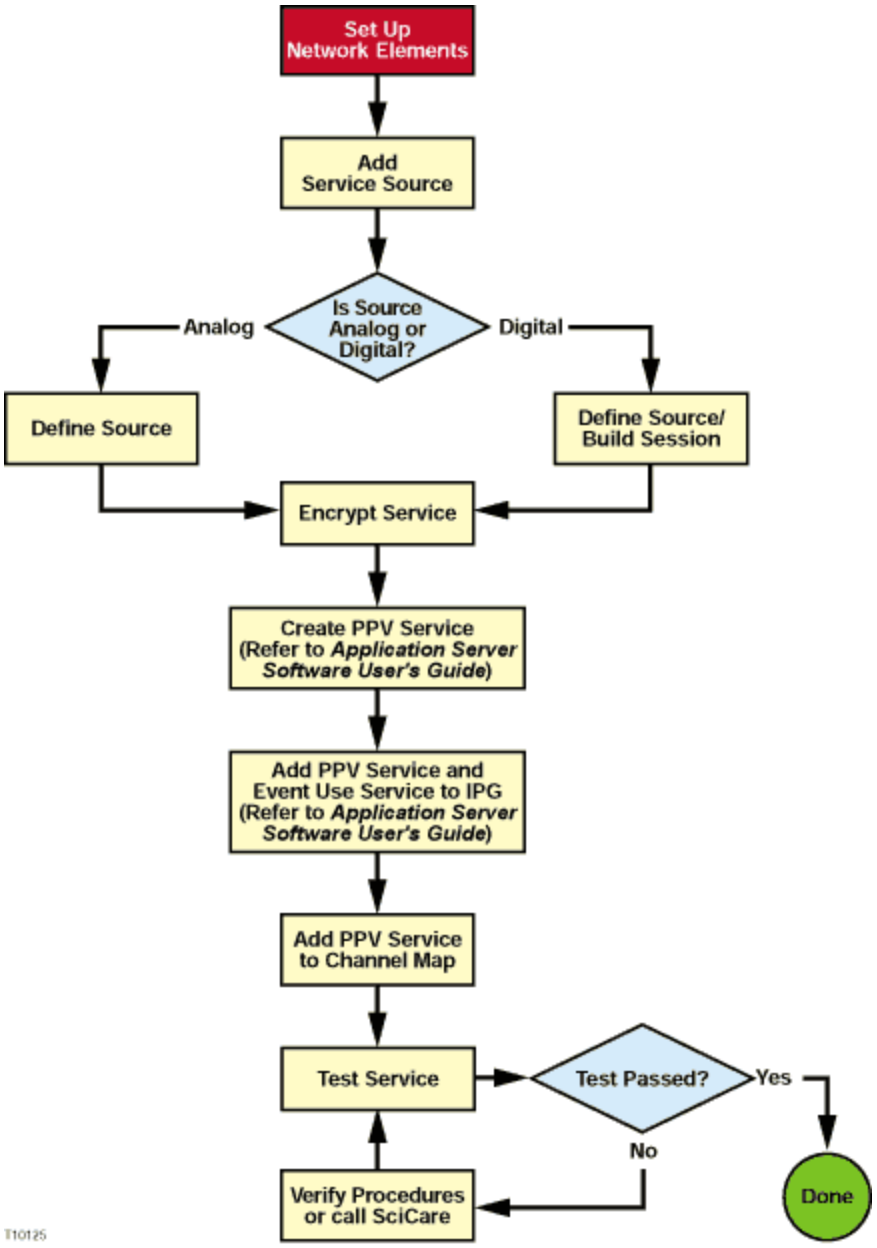
Setting up a PPV service takes approximately 45 minutes to an hour to complete.

## Performance Impact

Setting up a PPV service does not impact network performance. You can complete this procedure at any time.

### Setting Up PPV Services Flow Diagram

The following diagram illustrates the process of setting up a secure service.



### Setting Up PPV Services

Complete these procedures to set up a PPV service in your network. For step-by-step instructions for a particular procedure, click on that procedure.

1. Make sure you have completed all of the necessary steps specified in Setting Up Your Network.
2. Add the service source to the DNCS database.
3. Define parameters for the service source.
4. Encrypt the content coming from the service source so that it is available only to authorized subscribers.
5. Create the PPV service as defined in the SARA Application Server 3.4.1 User's Guide (part number 4012159). To obtain a copy of this guide, see Printed Resources.

   **Note:** Creating a PPV service also involves defining an Event Use Service.

6. Add both the PPV service and the Event Use Service to your IPG as defined in the SARA Application Server 3.4.1 User's Guide (part number 4012159). To obtain a copy of this guide, see Printed Resources.

   **Important:** If you do not add both services to the IPG, information about the PPV events will be missing from the IPG or from the PPV purchase barker.

7. Add the PPV service to a channel map.

   **Important:** Add only the PPV service to a channel map. If you add the Event Use Service to a channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to that channel.

8. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service. Then, try to access the service, purchase an event, and view the event.

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Add a Content Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New**

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different services from a single FOXSW signal:

You could offer the FOXSW broadcast as a clear service to all subscribers.

By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

### You Need to Know

▸ Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

▸ Time to Complete

Adding a content source takes approximately 5 minutes to complete.

▸ Performance Impact

Adding a content source does not impact network performance. You can complete this procedure at any time.

### Adding a Content Source

Complete these steps to add a source for a service.

**Note:** This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   **Note:** We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

6. Click in the **Source ID** field and type the number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters.

**Notes:**

- You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
- Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.

8. You are ready to define the source that you just added. Go to Define a Content Source.

## Define a Content Source

**Note:** These procedures do not apply to VOD services.

After you add a content source to the DNCS database for a clear, secure, or PPV service, define parameters for the source so that the system knows how to process the service content.

**Important:** If you are sending the same source through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same content source through six QAM modulators, you must define the source six times once for each modulator.

## Define an Analog Source

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Analog**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source in the DNCS. You do not need to define a source for a VOD service.

**Note:** You do not need to build a session for an analog source.

**Important:** If you are sending the same source content through more than one QAM, MQAM, or GQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator.

### You Need to Know

Before You Begin

Before you define an **analog** service source, you must have the following information:

- Name of the source as you defined it when you added the content source
- If the service source is going to only one hub, name of that hub as defined in your network (refer to your network map)
- Number of the channel where the service will be displayed

**Important:** Before you set up a **secure analog service** in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

Time To Complete

Defining an analog source takes approximately 10 minutes to complete.

Performance Impact

Defining an analog source does not impact network performance. You can complete this procedure at any time.

### Analog Source Settings

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪**Default** - Distributes the source to all hubs.<br>▪**Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪**Now** - The service is available for viewing immediately.<br>▪**Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |

### Defining an Analog Source

**Important:** Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this document, go to Printed Resources.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define.
5. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
6. Click **File > New Analog**. The Set Up Source Definition window opens.
7. Complete the fields on the screen as described in Analog Source Settings.

Use the following fields when you manage an analog source in the DNCS.

| Field | Description |
|---|---|
| Distribution | Defines how the source is distributed:<br>▪ **Default** - Distributes the source to all hubs.<br>▪ **Hub** - Distributes the source to the specific hub defined in Hub Name. |
| Hub Name | The hub name that receives content from this source.<br>This option is only activated if you selected the **Hub** option in the Distribution field. |
| Analog Channel ID | The number of the channel where you want to display this service.<br>This number must correspond to a channel number as defined by the Electronic Industries Alliance (EIA). |
| **Note:** Subscribers will see a blank channel until either the source is saved or the time that you specify arrives. | |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪ **Now** - The service is available for viewing immediately.<br>▪ **Custom** - Enter a specific date and time for service availability in the Effective Date and Effective Time fields. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>This option is only activated if you select the **Custom** option in the Date/Time field. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source. |

You must type two digits for each value.

**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.

**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

This option is only activated if you select the **Custom** option in the Date/Time field.

8. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source Definition window. The Source Definition List window updates to include the new source information.

9. Do you need to define another analog source for this service?

- If **yes**, repeat this procedure from step 6.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

10. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

11. Click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 13.
- If **no**, your next step is to register the clear service. Go to Register a Service.

13. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

### Define a Digital Source and Session

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions > File > New Digital**

After you add a content source to the DNCS for a clear, secure, or PPV service, define parameters for that source. Then build a session from the source definition. You do not need to define a source and session for a VOD service.

**Important:**

- If you are sending the same source through more than one QAM, MQAM, GQAM, or GoQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six QAM modulators, you must define the source six times once for each modulator. This also applies to GQAM stat mux dejitter groups (SMDGs).
- If you are setting up a CF session as a **stat mux dejitter group (SMDG)** session, the session must use the same input port and output port that the SMDG uses. Otherwise, the session may fail. You can set up a maximum of 60 sessions on an SMDG. For assistance setting up an SMDG, see Setting Up Stat Mux Dejitter Groups.

**You Need to Know**

Before You Begin

Before you define a digital service source, you must have the following information:

- Name of the service source as you defined it when you added the content source
- Number of the channel where the service will be displayed
- Service source ID as you defined it when you added the content source
- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)
- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)
- As part of defining a digital session, you will identify the bandwidth that the session requires and the QAM carrier that the session uses. When assigning sessions to a QAM carrier, use the following guidelines to ensure that the throughput is sized appropriately for the carrier.
  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

**Example:** Placing 10 video streams at 3.75 Mbps on a single QAM carrier would require 37.5 Mbps, plus an additional 0.375 Mbps (for overhead), resulting in a total of 37.875 Mbps bandwidth used. In this example, a 256-QAM modulator would have 0.936 Mbps of unused bandwidth on the QAM carrier, and no additional services could be placed on this carrier without resulting in a loss of quality.

Time To Complete

Defining a digital content source and building a session from the source definition takes approximately 20 minutes to complete.

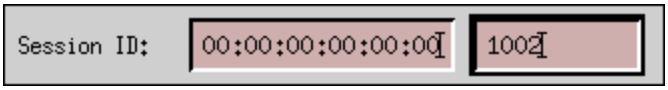
Performance Impact

Defining a digital content source and building a session from the source definition does not impact network

performance. You can complete this procedure at any time.

### Digital Source and Session Settings

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br><br>**Right Session ID field** - The source ID you used when you added the content source.<br><br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br><br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br><br>You must type two digits for the month and day, and four digits for the year.<br><br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br><br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br><br>You must type two digits for each value.<br><br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br><br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br><br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br><br>Select the **Broadcast programming** option because this source will provide broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br><br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.

| | |
|---|---|
| | ▪Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>▪For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| Wrap-up | See below for more information pertinent to the specific output device you selected. |

| | |
|---|---|
| ASI ports on a QAM, MQAM, or GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| GbE ports on a GQAM modulator | ▪**MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Standard MPEG video streams use 2 or 3 Mbps.<br>○HDTV streams use 13 |

| | |
|---|---|
| | Mbps.<br>○Audio streams use 0.2 Mbps.<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪**Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪**GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪**MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪**Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○Modulators using 256-QAM support a total bandwidth of 38.811 Mbps |

for each QAM carrier.

○For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

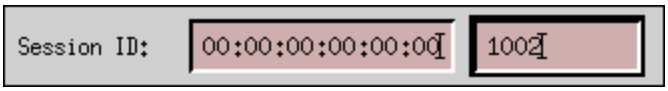
▪**Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.

▪**Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

### Defining a Digital Source and Session

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define and click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
5. Click **File > New Digital**. The Digital Source Set Up window opens.
6. Complete the fields on the screen as described in Digital Source and Session Settings.

Use the following fields when you manage digital sources and sessions in the DNCS. Be sure to click **Next** to move between session screens.

| Field | Description |
|---|---|
| Session ID | **Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).<br>**Right Session ID field** - The source ID you used when you added the content source.<br>Your final entry will look similar to the following example:<br>  |
| Specify effective date and time | Allows you to define when subscribers can start viewing content from this source.<br>If left unselected, subscribers can start viewing content immediately. |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** For July 4, 2007, type **07042007**. The system inputs the slashes for you and displays **07/04/2007**.<br>**Note:** You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**.<br>You can also represent time in the 24-hour format. For example, **18:30:00** would represent 6:30 p.m.<br>This option is only activated if you select the **Select effective date and time** option. |
| Define Session | Define the session programming.<br>Select the **Broadcast programming** option because this source will provide |

| | |
|---|---|
| | broadcast (audio/video) programming rather than system information. |
| Input Device | The type of device (the MPEG source) that will provide the service content (for example, an MDR or IRT).<br>You defined the MPEG source when you set up your network. |
| Select Outputs | The carrier that will receive content from this source. |

**Important:** When you assign sessions to a QAM carrier, use the following information to make sure that the throughput bandwidth is appropriate for the carrier.

- Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
- Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
- For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

| | | |
|---|---|---|
| Wrap-up | See below for more information pertinent to the specific output device you selected. | |
| | ASI ports on a QAM, MQAM, or GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions. |
| | GbE ports on a GQAM modulator | ▪ **MPEG Program Number** - The MPEG program number being fed into the transport stream. This number must match the program |

| | |
|---|---|
| | number of the MPEG source as defined by your content provider.<br>▪ **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.<br>**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:<br>○ Standard MPEG video streams use 2 or 3 Mbps.<br>○ HDTV streams use 13 Mbps.<br>○ Audio streams use 0.2 Mbps.<br>○ Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.<br>○ Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.<br>○ For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.<br>▪ **Source Output** - The destination UDP port number on the GQAM modulator where the source is output.<br>▪ **GQAM Input** - The destination UDP port number on the GQAM modulator where the source is input.<br>**Important:** If the session is being set up as an SMDG session, the session's input and output ports must match the input and output ports of the SMDG. Otherwise, the session may fail. |
| Input ports on a GoQAM modulator | ▪ **MPEG Program Number** - The MPEG program number of the clear stream that the GoQAM modulator sends to the transport network or the UpConverter (if used).<br>▪ **Incumbent MPEG Program Number** - The MPEG program number of the encrypted, or third-party, stream that the GoQAM modulator sends to the transport network or the |

UpConverter (if used).

- **Bandwidth** - The amount of bandwidth (in Mbps) that the system should allow for this service.

**Note:** This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:

  - Modulators using 64-QAM support a total bandwidth of 26.971 Mbps for each QAM carrier.
  - Modulators using 256-QAM support a total bandwidth of 38.811 Mbps for each QAM carrier.
  - For each QAM carrier, allocate 1% overhead for PSI and ECM insertions.

- **Audio Encryption Percentage** - Leave the default value of **5** so that the modulator will use PowerKEY encryption to partially encrypt the audio portion of the stream.
- **Video Encryption Percentage** - Leave the default value of **2** so that the modulator will use PowerKEY encryption to partially encrypt the video portion of the stream.

7. On the Save Source Definition window, click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

8. Do you need to define another digital source for this service?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

**Note:** You would define more than one digital service source if you have more than one MPEG source feeding the same content into different portions of your network.

9. Is this a secure or PPV service?

- If **yes**, your next step is to encrypt the content that comes from this service source so that it is available only to authorized subscribers. Go to Encrypt a Service.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

10. Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to step 11.
- If **no**, your next step is to register the clear service. Go to Register a Service.

11. Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to Add a Service Package.

## Encrypt a Service

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Security Modes > File > New**

**Note:** This procedure applies to secure and PPV services. It does not apply to clear or VOD services.

After you define a secure or PPV service source, you must set the system to encrypt all of the content coming from that source. Encryption ensures that this content is available only to authorized subscribers.

### You Need to Know

Time to Complete

Encrypting a service takes approximately 10 minutes to complete.

Performance Impact

Encrypting a service does not impact network performance. You can complete this procedure at any time.

### Service Encryption Settings

Use the following fields when you encrypt a service in the DNCS.

| Field | Description |
|---|---|
| Security Mode | Determines whether the service is encrypted. |
| Security Mode | The security mode of the service:<br>▪Select the **Clear** option to distribute the service in the clear (unencrypted)<br>▪Select the **Encrypted** option to distribute the service as an encrypted service |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪**Now** - The service is available for viewing immediately<br>▪**Custom** - Set a specific date and time for service availability in the **Effective Date a**nd **Effective Time** fields |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** Type July 4, 2008, as **07042008**. The system inputs the slashes for you and displays 07/04/2003.<br>This option is only activated if you select the **Custom** option in Date/Time. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** Type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>**Notes:**<br>▪Make sure the time you enter is at least 15 minutes into the future.<br>▪You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in Date/Time. |
| AM/PM | Establishes which portion of the day you want the system to begin encrypting this service.<br>Select either **AM** or **PM** from the list. |

### Encrypting a Service

Complete these steps to encrypt service content.

**Note:** This procedure applies to secure and PPV services. It does not apply to clear or VOD services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you want to encrypt.
5. Click **File > Security Modes**. The Security Mode List window opens for the service source you selected.
6. Click **File > New**. The Set Up Security Mode window opens.
7. Complete the fields on the screen as described in Service Encryption Settings.

Use the following fields when you encrypt a service in the DNCS.

| Field | Description |
|---|---|
| Security Mode | Determines whether the service is encrypted. |
| Security Mode | The security mode of the service:<br>▪ Select the **Clear** option to distribute the service in the clear (unencrypted)<br>▪ Select the **Encrypted** option to distribute the service as an encrypted service |
| Date/Time | Allows you to define when subscribers can start viewing content from this source:<br>▪ **Now** - The service is available for viewing immediately<br>▪ **Custom** - Set a specific date and time for service availability in the **Effective Date a**nd **Effective Time** fields |
| Effective Date | The month, day, and year you want subscribers to be able to start viewing content from this source.<br>You must type two digits for the month and day, and four digits for the year.<br>**Example:** Type July 4, 2008, as **07042008**. The system inputs the slashes for you and displays 07/04/2003.<br>This option is only activated if you select the **Custom** option in Date/Time. |
| Effective Time | The hour, minute, and second you want subscribers to be able to start seeing content from this source.<br>You must type two digits for each value.<br>**Example:** Type eight o'clock as **080000**. The system inputs the colons for you and displays 08:00:00.<br>**Notes:**<br>▪ Make sure the time you enter is at least 15 minutes into the future.<br>▪ You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.<br>This option is only activated if you select the **Custom** option in |

| | |
|---|---|
| | Date/Time. |
| AM/PM | Establishes which portion of the day you want the system to begin encrypting this service.<br><br>Select either **AM** or **PM** from the list. |

8. Click **Save**. The system saves the encryption information in the DNCS database and closes the Set Up Security Mode window. The Security Mode List window updates to include the new encryption information.

9. Do you need to set up another security mode for this service source? For example, you may want to allow all of your subscribers to have access to a normally encrypted service (such as HBO) for a limited time (such as a weekend) in an attempt to entice more people to purchase the service.

- If **yes**, repeat this procedure from step 6.
- If **no**, go to step 10.

10. Click **File > Close** to close the Security Mode List window and return to the Source List window.

11. Is this a secure service?

- If **yes**, your next step is to add an unlimited segment for the service source. Go to Add an Unlimited Segment.
- If **no**, click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

12. Your next step is to create the PPV service and add it to the IPG as described in the SARA Application Server 3.4.1 User's Guide (part number 4012159). To obtain this guide, refer to Printed Resources. When finished, go to Add a Service to a Channel Map.

## Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.

8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?

- If **yes**, go to Split a Channel.
- If **no**, go to step 9.

9. Do you need to add another service to this channel map?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.

10. Do you need to add a service to another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

11. Do you need to include the service on your IPG?

- If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
- If **no**, go to step 12.

12. Is this is a VOD service?

- If **yes**, complete any additional procedures required by the vendor of your VOD server.
- If **no**, go to step 13.

13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.

8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?

- If **yes**, go to Split a Channel.
- If **no**, go to step 9.

9. Do you need to add another service to this channel map?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.

10. Do you need to add a service to another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

11. Do you need to include the service on your IPG?

- If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
- If **no**, go to step 12.

12. Is this is a VOD service?

- If **yes**, complete any additional procedures required by the vendor of your VOD server.
- If **no**, go to step 13.

13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

## Test a Service

**Note:** Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops for services with your billing system vendor.

After you have completed all the steps in setting up a particular type of service, verify that you set up the service successfully by using a test set-top and a television.

Is the new service packaged?

- If **yes**, first authorize the set-top to receive the package.
- If **no**, verify a successful service setup by trying to access the service.

**Related Topics**

- Authorize a Set-Top for a Service
- Verify a Successful Service Setup
- Locating a Set-Top MAC Address

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Locating a Set-Top MAC Address

To locate the MAC address of a set-top, do one of the following:

- Display the set-top diagnostic screens.
- Look on the back of the set-top for a label with the MAC address recorded on it.

# VOD Services

Video-on-demand (VOD) services make up one type of interactive services that you can offer to your subscribers through our DBDS. Interactive services allow each subscriber to actively control how a service is used.

In the case of VOD, the subscriber can use the remote control to select, purchase, and view an event. After the subscriber has purchased the event, the reverse path allows the viewer to forward, reverse, pause, and play the event just as he or she would with a VCR.

**Note:** We offer two software products that enable you to further control and exploit your VOD and premium service offerings: session-based encrypted VOD and Subscription VOD (SVOD). For more information about these software products, contact the representative who handles your account.

**Related Topics**

Before You Begin

Before you set up VOD services in the DNCS, you must make sure all of the network elements responsible for processing the service content are physically installed in your system. In addition to our standard DBDS equipment, you must have at least one VOD controller and video server.

We do not provide or install VOD controllers or video servers. You must contact other vendors and follow their instructions for installing these elements into your network.

After you have installed all of these physical elements, you must add them to the DNCS database. If necessary, refer to Setting Up Your Network.

Finally, you want to have your network map available.

Time to Complete

Setting up a VOD service takes approximately 45 minutes to an hour to complete.

Performance Impact

Setting up a VOD service does not impact network performance. You can complete this procedure at any time.

## Process Overview

Complete these procedures to set up a VOD service in your network. For step- by-step instructions for a particular procedure, click on that procedure.

**Note:** After you set up VOD services in the DNCS, you must complete additional procedures according to the vendor of your VOD server.

1. Make sure you have completed all of the necessary steps specified in Setting Up Your Network, including setting up VOD service groups. Pay special attention to the steps for adding a VASP entry, adding an MPEG source, adding a QAM, adding a MQAM, or a GQAM modulator, and adding a service group.
2. Add a service package specifically for the VOD service.
3. Determine and convert the package Entitlement Identifier (EID) from a hexadecimal to a decimal value.

4. Register the service.

5. Add the service to a channel map.

6. Do you want to include the service on your IPG?

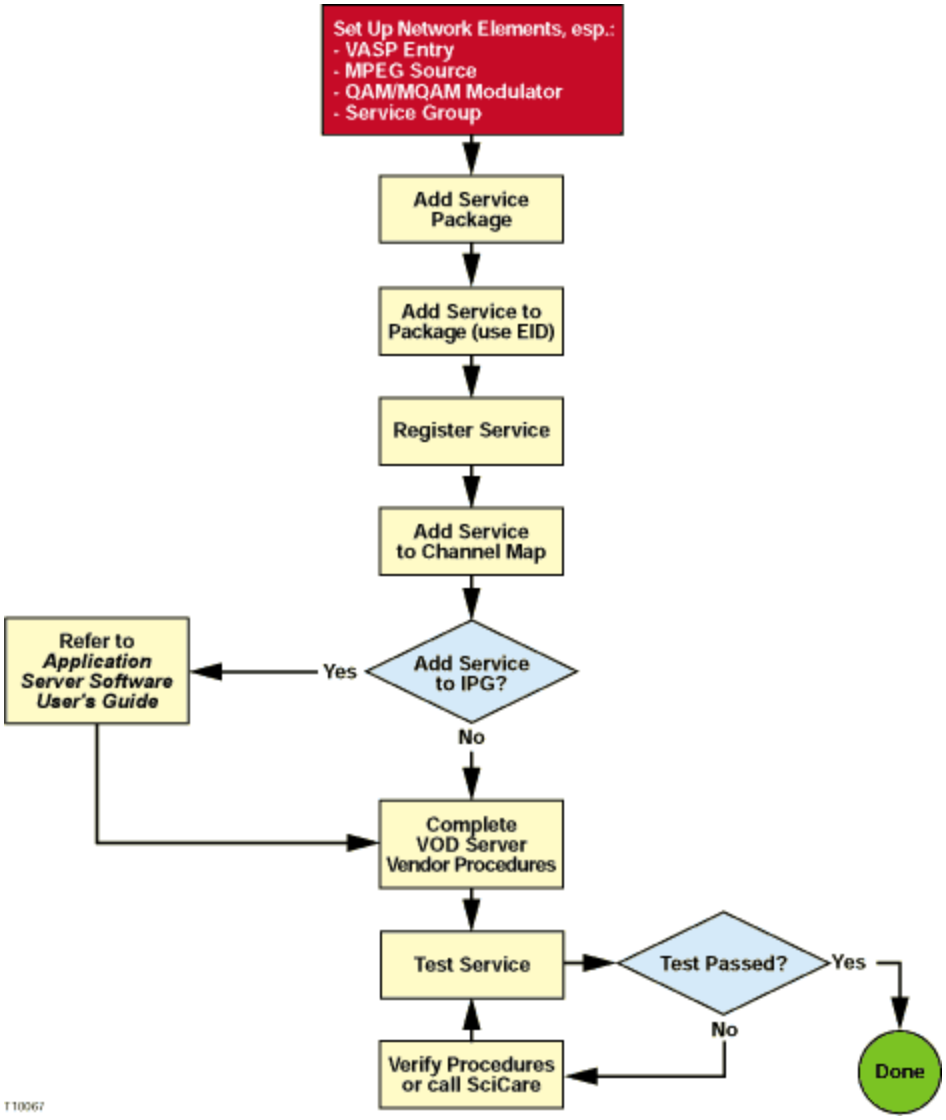
   - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for instructions. To obtain a copy of this guide, see Printed Resources.
   - If **no**, go to step 7.

7. Complete any additional procedures required by the vendor of your VOD server.

8. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

## Setting Up VOD Services Flow Diagram

The following diagram illustrates the process of setting up a VOD service.



## Process Overview

Complete these procedures to set up a VOD service in your network. For step- by-step instructions for a particular procedure, click on that procedure.

**Note:** After you set up VOD services in the DNCS, you must complete additional procedures according to the vendor of your VOD server.

1. Make sure you have completed all of the necessary steps specified in Setting Up Your Network, including setting up VOD service groups. Pay special attention to the steps for adding a VASP entry, adding an MPEG source, adding a QAM, adding a MQAM, or a GQAM modulator, and adding a service group.
2. Add a service package specifically for the VOD service.
3. Determine and convert the package Entitlement Identifier (EID) from a hexadecimal to a decimal value.
4. Register the service.
5. Add the service to a channel map.
6. Do you want to include the service on your IPG?
   - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for instructions. To obtain a copy of this guide, see Printed Resources.
   - If **no**, go to step 7.
7. Complete any additional procedures required by the vendor of your VOD server.
8. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

# VOD Services

Video-on-demand (VOD) services make up one type of interactive services that you can offer to your subscribers through our DBDS. Interactive services allow each subscriber to actively control how a service is used.

In the case of VOD, the subscriber can use the remote control to select, purchase, and view an event. After the subscriber has purchased the event, the reverse path allows the viewer to forward, reverse, pause, and play the event just as he or she would with a VCR.

**Note:** We offer two software products that enable you to further control and exploit your VOD and premium service offerings: session-based encrypted VOD and Subscription VOD (SVOD). For more information about these software products, contact the representative who handles your account.

**Related Topics**

Before You Begin

Before you set up VOD services in the DNCS, you must make sure all of the network elements responsible for processing the service content are physically installed in your system. In addition to our standard DBDS equipment, you must have at least one VOD controller and video server.

We do not provide or install VOD controllers or video servers. You must contact other vendors and follow their instructions for installing these elements into your network.

After you have installed all of these physical elements, you must add them to the DNCS database. If necessary, refer to Setting Up Your Network.

Finally, you want to have your network map available.

Time to Complete

Setting up a VOD service takes approximately 45 minutes to an hour to complete.

Performance Impact

Setting up a VOD service does not impact network performance. You can complete this procedure at any time.

## Process Overview

Complete these procedures to set up a VOD service in your network. For step- by-step instructions for a particular procedure, click on that procedure.

**Note:** After you set up VOD services in the DNCS, you must complete additional procedures according to the vendor of your VOD server.

1. Make sure you have completed all of the necessary steps specified in Setting Up Your Network, including setting up VOD service groups. Pay special attention to the steps for adding a VASP entry, adding an MPEG source, adding a QAM, adding a MQAM, or a GQAM modulator, and adding a service group.
1. Add a service package specifically for the VOD service.
1. Determine and convert the package Entitlement Identifier (EID) from a hexadecimal to a decimal

value.

1. Register the service.

1. Add the service to a channel map.

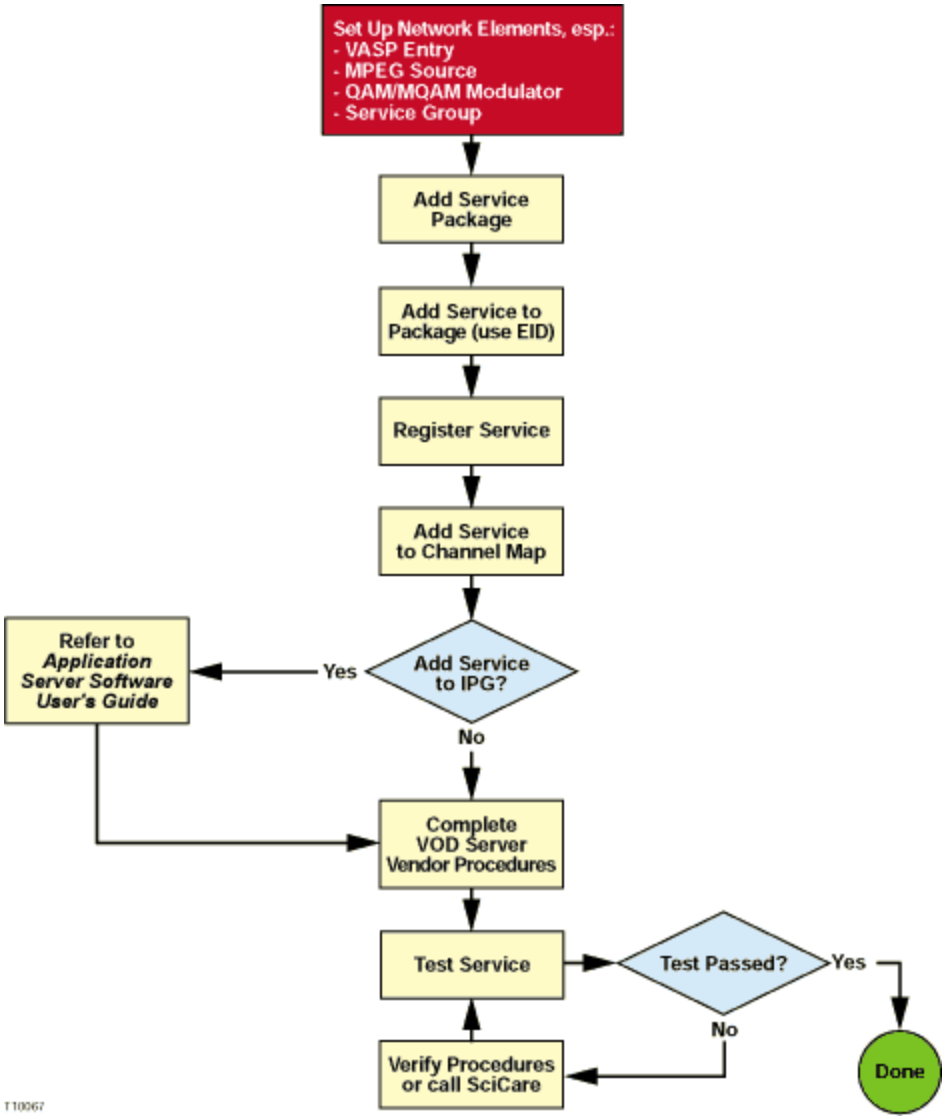
1. Do you want to include the service on your IPG?
   - If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for instructions. To obtain a copy of this guide, see Printed Resources.
   - If **no**, go to step 7.

1. Complete any additional procedures required by the vendor of your VOD server.

1. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

## Setting Up VOD Services Flow Diagram

The following diagram illustrates the process of setting up a VOD service.



## Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

### You Need to Know

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

### Guidelines for Adding Services

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.
- You must add a service package for each VOD service. Otherwise, your authorized subscribers will not be able to access the VOD service.
- Because clear services are not encrypted, packaging a clear service does not protect it from being

accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

**Related Topics**

- Service Package Settings
- Adding a Service Package

## Add a Service Package

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New**

**Notes:**

- This procedure applies to secure, VOD, packaged clear services, and default staging packages when using InstaStaging.
- Do not use this procedure for PPV or unpackaged clear services.

**Important:** If you are using our RCS solution, create a package for each site that will receive the service this package provides.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's DHCT to receive the package, and so forth, just as you would for a secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

### You Need to Know

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

### Guidelines for Adding Services

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.
- You must add a service package for each VOD service. Otherwise, your authorized subscribers will not be able to access the VOD service.
- Because clear services are not encrypted, packaging a clear service does not protect it from being

accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

**Related Topics**

- Service Package Settings
- Adding a Service Package

### Service Package Settings

Use the following fields when you manage a service package in the DNCS.

| Field | Description |
|---|---|
| Package Name | The name that identifies this package.<br><br>You can use up to 20 alphanumeric characters.<br><br>**Important:** The package name that you enter must be compatible with the package name rules that your billing system uses. Default packages (those used for InstaStaging) are the only exception.<br><br>**Notes:**<br><br>▪The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br><br>▪Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Default Staging Package | Allows you to define a package as a default staging package.<br><br>This option appears only if you have enabled InstaStaging on the DNCS.<br><br>**Notes:**<br><br>▪The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br><br>▪Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Duration | Allows subscribers to have unlimited access to the package.<br><br>The **Unlimited** option in the Duration field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services. |
| Pay Per View | Not supported at this time. |
| Impulse Pay Per View | Not supported at this time. |
| Allow Event Extension | Not supported at this time. |

### Related Topics

- Adding a Service Package
- Guidelines for Adding Services

### Adding a Service Package

Complete these steps to add a new service package to the DNCS.

**Note:** This procedure applies to secure, VOD, and packaged clear services and default staging packages when using InstaStaging. It does not apply to PPV or unpackaged clear services.

**Packages for InstaStaging:** If you are adding default packages for use with InstaStaging, be aware that you can specify multiple default packages. In addition, if your site is a SARA site and uses a Service Disconnect package (sometimes referred to as a "brick mode" package), be sure that the default staging option is selected for the Service Disconnect package.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.

   **Note:** By default, the Package List window shows only non-PPV packages (Subscription Only). To view the list of all packages, click the **Show** button and select **All Packages**.

4. Click **File > New**. The Set Up Package window opens.
5. Complete the fields on the screen as described in Service Package Settings.

Use the following fields when you manage a service package in the DNCS.

| Field | Description |
|---|---|
| Package Name | The name that identifies this package.<br><br>You can use up to 20 alphanumeric characters.<br><br>**Important:** The package name that you enter must be compatible with the package name rules that your billing system uses. Default packages (those used for InstaStaging) are the only exception.<br><br>**Notes:**<br>▪ The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br>▪ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Default Staging Package | Allows you to define a package as a default staging package.<br><br>This option appears only if you have enabled InstaStaging on the DNCS.<br><br>**Notes:**<br>▪ The **Unlimited** option in the **Duration** field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services.<br>▪ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The DNCS does not support these options at this time. |
| Duration | Allows subscribers to have unlimited access to the package.<br><br>The **Unlimited** option in the Duration field is selected by default. This option |

| | |
|---|---|
| | allows the subscriber to have unlimited access to the package. Do not change this option without first consulting Cisco Services. |
| Pay Per View | Not supported at this time. |
| Impulse Pay Per View | Not supported at this time. |
| Allow Event Extension | Not supported at this time. |

**Related Topics**

- Adding a Service Package
- Guidelines for Adding Services

6.Click **Save**. The system saves the package information in the DNCS database and closes the Set Up Package window. The Package List window updates to include the new package.

**Note:** If you are using InstaStaging and have created a default staging package, an asterisk (*) appears next to this package to indicate it is a default staging package.

7.Are you using our RCS solution?

- If **yes**, go to step 8.
- If **no**, go to step 9.

8.Are there other RCS sites that will use the third-party application that this package provides?

- If **yes**, repeat this procedure from step 4 to add a package to another site.
- If **no**, go to step 9.

9.Do you need to add a secure service to this package?

- If **yes**, go to Adding a Secure Service to a Package.
- If no, go to step 10.

10.Do you need to add a VOD or clear service to this package?

- If **yes**, go to Determine and Convert a Package EID.
- If **no**, go to step 11.

11.Are you setting up Instastaging?

- If **yes**, you need to Identify Existing Packages as Default Packages.
- If **no**, go to step 12.

12.Click **File > Close** to close the Package List window.

13.Go to Registering a Service.

## Determine and Convert a Package EID

**Important:**

- This procedure applies to VOD services. It also applies to clear services that you want to package. It does not apply to secure, PPV, or unpackaged clear services.
- Because clear services are not encrypted, packaging a clear service does not protect it from being accessed (stolen) by unauthorized users.

When you add a service package to your system, the DNCS automatically assigns an Entitlement Identifier (EID) to the package. To package a VOD or clear service, you must first determine the package EID, and then convert it from a hexadecimal value to a decimal value. Then, you use the decimal value when you register the service. Among other things, registering the service associates it with the specified package.

By making this association, DHCTs are able to use data from the SAM Service List to link the service with a particular package. If you do not make this association, all DHCTs will receive the service even those DHCTs that are not authorized to receive it.

You must add a VOD service to a package to make it available to your authorized subscribers. Each VOD service must have its own package.

You can also add a clear service to a package to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble (or decrypt) services. Some examples of clear services that you might want to offer on a package basis include the following:

- Unscrambled analog video
- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

**You Need to Know**

Before You Begin

Before you can add a VOD or clear service to a new package, you must first add the package to the DNCS. If necessary, go to Adding a Service Package before you begin this procedure.

Time to Complete

Determining a package EID and converting it from hexadecimal to decimal takes approximately 20 minutes to complete.

Performance Impact

Determining a package EID and converting it from hexadecimal to decimal does not impact network performance. You can complete this procedure at any time.

### Determining a Package EID

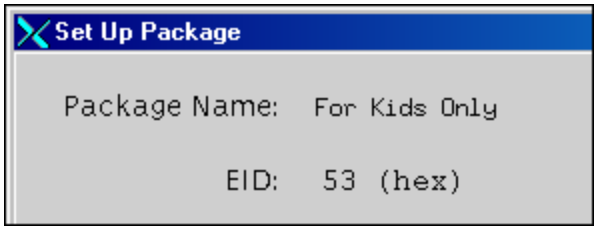
**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > [Package Name] > File > Open**

**Important:** This procedure applies to VOD services and clear services that you want to package. It does not apply to secure, PPV, or unpackaged clear services.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.

   **Note:** By default, the Package List window shows only non-PPV packages (Subscription Only). To view the list of all packages, click the **Show** button and select **All Packages**.

4. Click once on the row containing the package to which you want to add the service.
5. Click **File > Open**. The Set Up Package window opens for the package you selected.
6. Record the number shown in the EID field. In the following example, the package EID is 53.




7. Click **Cancel** to close the Set Up Package window and return to the Package List window.
8. Click **File > Close** to close the Package List window and return to the DNCS Administrative Console.
9. Your next step is to convert the EID from hexadecimal value to a decimal value. Go to Converting a Package EID to Decimal.

### Converting a Package EID to Decimal

**Important:** This procedure applies to VOD services and clear services that you want to package. It does not apply to secure, PPV, or unpackaged clear services.

The SAM Service List recognizes only decimal formats. However, the Set Up Package window displays the package EID in hexadecimal format. After you determine the package EID, for the SAM Service List to be able to link a VOD or a clear service with a particular package, you must convert the EID to decimal format.

Hexadecimal values derive from the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9, followed by the letters a to f. Once you reach the letter f, you continue counting with 1a, 1b, 1c, and so on until you reach 1f. Then, you continue with 2a, 2b, 2c, and so on.

In contrast, decimal values derive from the base-10 number system, which consists only of the numbers 0 to 9. Once you reach the number 9, you continue counting with 10, 11, 12, and so on until you reach 19. Then, you continue with 20, 21, 22, and so on.

Each hexadecimal number corresponds to a decimal number. For example, in the following tables, the hexadecimal (HEX) 53 corresponds with the decimal (DEC) 83. You would use the number 83 to associate the service with the package when you register the service.

Use the following procedure to convert a package EID to a decimal value.

1. After you determine the DNCS package EID, use the following table to locate the EID in the **HEX** column.
2. Then, locate the corresponding decimal value in the **DEC** column.

For example, if the package EID is **1f**, the decimal value is **31**.

| HEX | DEC | HEX | DEC | HEX | DEC | HEX | DEC | HEX | DEC | HEX | DEC | HEX | DEC | HEX | DEC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 20 | 32 | 40 | 64 | 60 | 96 | 80 | 128 | a0 | 160 | c0 | 192 | e0 | 224 |
| 1 | 1 | 21 | 33 | 41 | 65 | 61 | 97 | 81 | 129 | a1 | 161 | c1 | 193 | e1 | 225 |
| 2 | 2 | 22 | 34 | 42 | 66 | 62 | 98 | 82 | 130 | a2 | 162 | c2 | 194 | e2 | 226 |
| 3 | 3 | 23 | 35 | 43 | 67 | 63 | 99 | 83 | 131 | a3 | 163 | c3 | 195 | e3 | 227 |
| 4 | 4 | 24 | 36 | 44 | 68 | 64 | 100 | 84 | 132 | a4 | 164 | c4 | 196 | e4 | 228 |
| 5 | 5 | 25 | 37 | 45 | 69 | 65 | 101 | 85 | 133 | a5 | 165 | c5 | 197 | e5 | 229 |
| 6 | 6 | 26 | 38 | 46 | 70 | 66 | 102 | 86 | 134 | a6 | 166 | c6 | 198 | e6 | 230 |
| 7 | 7 | 27 | 39 | 47 | 71 | 67 | 103 | 87 | 135 | a7 | 167 | c7 | 199 | e7 | 231 |
| 8 | 8 | 28 | 40 | 48 | 72 | 68 | 104 | 88 | 136 | a8 | 168 | c8 | 200 | e8 | 232 |
| 9 | 9 | 29 | 41 | 49 | 73 | 69 | 105 | 89 | 137 | a9 | 169 | c9 | 201 | e9 | 233 |
| a | 10 | 2a | 42 | 4a | 74 | 6a | 106 | 8a | 138 | aa | 170 | ca | 202 | ea | 234 |
| b | 11 | 2b | 43 | 4b | 75 | 6b | 107 | 8b | 139 | ab | 171 | cb | 203 | eb | 235 |
| c | 12 | 2c | 44 | 4c | 76 | 6c | 108 | 8c | 140 | ac | 172 | cc | 204 | ec | 236 |
| d | 13 | 2d | 45 | 4d | 77 | 6d | 109 | 8d | 141 | ad | 173 | cd | 205 | ed | 237 |

| e | 14 | 2e | 46 | 4e | 78 | 6e | 110 | 8e | 142 | ae | 174 | ce | 206 | ee | 238 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| f | 15 | 2f | 47 | 4f | 79 | 6f | 111 | 8f | 143 | af | 175 | cf | 207 | ef | 239 |
| 10 | 16 | 30 | 48 | 50 | 80 | 70 | 112 | 90 | 144 | b0 | 176 | d0 | 208 | f0 | 240 |
| 11 | 17 | 31 | 49 | 51 | 81 | 71 | 113 | 91 | 145 | b1 | 177 | d1 | 209 | f1 | 241 |
| 12 | 18 | 32 | 50 | 52 | 82 | 72 | 114 | 92 | 146 | b2 | 178 | d2 | 210 | f2 | 242 |
| 13 | 19 | 33 | 51 | 53 | 83 | 73 | 115 | 93 | 147 | b3 | 179 | d3 | 211 | f3 | 243 |
| 14 | 20 | 34 | 52 | 54 | 84 | 74 | 116 | 94 | 148 | b4 | 180 | d4 | 212 | f4 | 244 |
| 15 | 21 | 35 | 53 | 55 | 85 | 75 | 117 | 95 | 149 | b5 | 181 | d5 | 213 | f5 | 245 |
| 16 | 22 | 36 | 54 | 56 | 86 | 76 | 118 | 96 | 150 | b6 | 182 | d6 | 214 | f6 | 246 |
| 17 | 23 | 37 | 55 | 57 | 87 | 77 | 119 | 97 | 151 | b7 | 183 | d7 | 215 | f7 | 247 |
| 18 | 24 | 38 | 56 | 58 | 88 | 78 | 120 | 98 | 152 | b8 | 184 | d8 | 216 | f8 | 248 |
| 19 | 25 | 39 | 57 | 59 | 89 | 79 | 121 | 99 | 153 | b9 | 185 | d9 | 217 | f9 | 249 |
| 1a | 26 | 3a | 58 | 5a | 90 | 7a | 122 | 9a | 154 | ba | 186 | da | 218 | fa | 250 |
| 1b | 27 | 3b | 59 | 5b | 91 | 7b | 123 | 9b | 155 | bb | 187 | db | 219 | fb | 251 |
| 1c | 28 | 3c | 60 | 5c | 92 | 7c | 124 | 9c | 156 | bc | 188 | dc | 220 | fc | 252 |
| 1d | 29 | 3d | 61 | 5d | 93 | 7d | 125 | 9d | 157 | bd | 189 | dd | 221 | fd | 253 |
| 1e | 30 | 3e | 62 | 5e | 94 | 7e | 126 | 9e | 158 | be | 190 | de | 222 | fe | 254 |
| 1f | 31 | 3f | 63 | 5f | 95 | 7f | 127 | 9f | 159 | bf | 191 | df | 223 | ff | 255 |

## Register a Service

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > File > New**

**Note:** This procedure does not apply to PPV services.

Registering a service with the SAM achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's DHCT
- Communicates the operation attributes to the DHCTs in your network
- Registers the service and its operation attributes with the BFS

For example, to access a standard audio/video program service, a DHCT must download the WatchTV application. The WatchTV application contains the operation attributes that tell the DHCT how to tune to and display a standard audio/video program service so that subscribers can hear and view the service. In the case of a VOD service, a DHCT must download a PTV (PowerTV) file to serve the same purpose.

In addition, if the service is to be included as part of a package, registering the service associates it with the specified package.

**Important:** Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot.

**Note:** If you want to adjust how often the SAM communicates service operation attributes to the DHCTs in your network, go to Scheduling Service Updates.

### You Need to Know

When to Register a Service

When you register a service depends on the following factors:

- If you are setting up an **unpackaged clear service**, register the service after you have defined the service source.
- If you are setting up a **packaged clear service** or a **VOD service**, register the service after you have added the desired service package, determined the package EID, and converted the EID to a decimal value
- If you are setting up a **secure service**, register the service after you have added the desired service package and then added the service segment to that package.

Before You Begin

Before you can register a service, you must have the following information:

- Short description to identify the service on the IPG and channel banner (for example, the short description for the Discovery Kids service might be **DSCK**)
- Name of the software application or file that contains the operation attributes for the service (for example, **ippv**, **watchtv**, **ptv**, or **music**)
- Path on the BFS where the software application or file resides (for example, **bfs://resapp/watchtv** or **bfs:///apps/Smilpd.ptv**)

**Note:** This path is dependent upon how your system is configured

- Number of the logo associated with the service, if applicable (you can get a list of logo numbers from the representative who handles your account, or you can have us create a logo for you and assign it a number)
- For clear and secure services, the service source ID that you assigned when you added the service source
- For VOD services and packaged clear services, the decimal conversion of the package EID that the system assigned when you added the service package

### Service Registration Settings

Use the following fields when you register a service in the DNCS.

| Field | Description |
|---|---|
| Service Name | The name you want to use to identify this service (for example, Discovery Kids).<br>You can use up to 20 alphanumeric characters. |
| Short Description | A brief description of this service.<br>You can use up to 5 alphanumeric characters.<br>**Example:** For the Discovery Kids service, you might type **DSCK**.<br>This description will appear on the IPG and on the channel banner on the subscriber's television screen. |
| Long Description | A detailed description of this service.<br>You can use up to 32 alphanumeric characters.<br>This information is for your benefit only. Subscribers will not see this information. |
| Application URL | Path on the BFS where the software file resides.<br>Type the following information:<br>▪Path on the BFS where the software file resides (for example, **bfs://resapp/watchtv**)<br>▪**Note:** You can also click **Select** to select the path from the list that appears.<br>▪If the service is a VOD service, type a semicolon (**;**) and then **EID=<decimal equivalent of EID>** (if necessary, refer to Determine and Convert a Package EID)<br>▪If the service is a VOD service, type a semicolon (**;**) and then **level2-TRUE**<br>Your final entry should look similar to the following example: **bfs://resapp/watchtv;EID=83;level2-TRUE** for VOD services or **bfs://resapp/watchtv** for non-VOD services.<br>**Note:** You can also click **Select** to select the path from the list that appears. |
| Logo | The number for the logo associated with this service, if required. |
| Parameter | Define the type of service:<br>▪For a VOD service, type **0**.<br>▪For a clear or secure service, type the **service source ID** that you assigned when you added the service source. |

### Registering a Service

Complete these steps to register a service.

**Note:** This procedure does not apply to PPV services.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens.
3. Click **File > New**. The Set Up SAM Service window opens.
4. Complete the fields on the screen as described in Service Registration Settings.

Use the following fields when you register a service in the DNCS.

| Field | Description |
|---|---|
| Service Name | The name you want to use to identify this service (for example, Discovery Kids).<br>You can use up to 20 alphanumeric characters. |
| Short Description | A brief description of this service.<br>You can use up to 5 alphanumeric characters.<br>**Example:** For the Discovery Kids service, you might type **DSCK**.<br>This description will appear on the IPG and on the channel banner on the subscriber's television screen. |
| Long Description | A detailed description of this service.<br>You can use up to 32 alphanumeric characters.<br>This information is for your benefit only. Subscribers will not see this information. |
| Application URL | Path on the BFS where the software file resides.<br>Type the following information:<br>▪ Path on the BFS where the software file resides (for example, **bfs://resapp/watchtv**)<br>▪ **Note:** You can also click **Select** to select the path from the list that appears.<br>▪ If the service is a VOD service, type a semicolon (**;**) and then **EID=<decimal equivalent of EID>** (if necessary, refer to Determine and Convert a Package EID)<br>▪ If the service is a VOD service, type a semicolon (**;**) and then **level2-TRUE**<br>Your final entry should look similar to the following example: **bfs://resapp/watchtv;EID=83;level2-TRUE** for VOD services or **bfs://resapp/watchtv** for non-VOD services.<br>**Note:** You can also click **Select** to select the path from the list that appears. |
| Logo | The number for the logo associated with this service, if required. |
| Parameter | Define the type of service:<br>▪ For a VOD service, type **0**.<br>▪ For a clear or secure service, type the **service source ID** that |

you assigned when you added the service source.

5.Click **Save**. The system saves the service information in the DNCS database, registers the service with the BFS, and closes the Set Up SAM Service window. The SAM Service List window updates to include the new service with its Service ID.

6.Record the Service ID that the system assigns to the service. You will need it when you add the service to the IPG. In the following example, the Service ID is 196.

| Short Description | Service Name | Service ID | URL Tag |
|---|---|---|---|
| HPPV | PPV HBO | 196 | ippv |

7.Do you need to register another service with the SAM?

- If yes, repeat this procedure from step 3.
- If no, click **File > Close** to close the SAM Service List window and return to the DNCS Administrative Console.

8.Your next step is to add the service to a channel map. Does a channel map already exist to which you want to add this service?

- If **yes**, go to Add a Service to a Channel Map.
- If **no**, go to Add a Channel Map.

## Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.

8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?

- If **yes**, go to Split a Channel.
- If **no**, go to step 9.

9. Do you need to add another service to this channel map?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.

10. Do you need to add a service to another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

11. Do you need to include the service on your IPG?

- If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
- If **no**, go to step 12.

12. Is this is a VOD service?

- If **yes**, complete any additional procedures required by the vendor of your VOD server.
- If **no**, go to step 13.

13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

# Add a Service to a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open**

### You Need to Know

Before You Begin

Before you add a service to a channel map, you must answer the following questions:

- Are you adding this service to a new channel map? If so, you must first add the new channel map. Go to Add a Channel Map before you begin this procedure.
- On which channel on the channel map will this service be displayed?
- Do you need to split the channel to show this service during one period of the day and another service during the remainder of the day?

In addition, you must have the name of the service as you defined it when you registered it. In the case of a PPV service, use the name you defined when you created the PPV service on the SARA Server.

Time to Complete

Adding a service to a channel map takes approximately 25 minutes to complete, including the time it takes for channel changes to appear on DHCTs.

Performance Impact

Adding a service to a channel map does not impact network performance. You can complete this procedure at any time. However, it takes approximately 10 minutes for channel changes to take effect and appear on DHCTs.

### Adding a Service to a Channel Map

**Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   **Note:** If you select the Default channel map, this service will be available to all hubs.

4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   **Important:** If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.

6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.

8. Do you need to split this channel to show one service during one period of the day and another service during the remainder of the day?

- If **yes**, go to Split a Channel.
- If **no**, go to step 9.

9. Do you need to add another service to this channel map?

- If **yes**, repeat this procedure from step 5.
- If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.

10. Do you need to add a service to another channel map?

- If **yes**, repeat this procedure from step 3.
- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

11. Do you need to include the service on your IPG?

- If **yes**, refer to the SARA Application Server 3.4.1 User's Guide (part number 4012159) for further instructions. To obtain this guide, refer to Printed Resources.
- If **no**, go to step 12.

12. Is this is a VOD service?

- If **yes**, complete any additional procedures required by the vendor of your VOD server.
- If **no**, go to step 13.

13. Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to Test a Service.

## Define Session Signaling Parameters

**Quick Path: DNCS Administrative Console > System Provisioning tab > DNCS System > DSM-CC tab**

When a subscriber requests an interactive service, such as VOD, the DHCT, DNCS, and VOD server communicate with each other. The DNCS allows you to manually define key parameters for these communications so that they suit the needs of your system. These parameters are defined when your system is upgraded or installed; however, you can change these values to keep up with any system modifications.

### Session Signaling Parameter Settings

The following table describes each field in the DSM-CC tab and provides the range of values that we recommend.

| Field | Description |
|---|---|
| **DHCT Session Signaling Parameters** | |
| Send 'Session in Progress' Every | Enter a time (in minutes) that defines how often a DHCT tells the DNCS that a VOD event is in progress. The Session in Progress (SIP) message prevents the system from tearing down sessions while a DHCT receives an event.<br>**Warning:** A reduction in VOD performance may occur when a large number of SIP messages are generated at the same time.<br>We recommend that you generate SIP messages at least every 120 minutes, but no more than 180 minutes. |
| Retry Requests Up To | How many times a DHCT should send a session request to the DNCS .<br>We recommend that you set this value to **1** for one, but no more than 2 retries.<br>Setting this value to two or more times results in subscribers having to wait longer for a response. In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For Network Response After | How long (in seconds) a DHCT should wait for confirmation that the DNCS is processing the session request<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| **Network Session Signal Parameters** | |
| Send 'Setup Proceeding' Every | How long (in seconds) a DHCT must wait to receive confirmation from the DNCS that it is processing the session request that the DHCT sent.<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| Retry Requests Up To | How many times the DNCS should request tuning information from the VOD server for a particular event.<br>We recommend that you set this value to be equal to or greater than the **Retry Requests Up To** parameter for DHCTs.<br>Setting this value to two or more times results in subscribers having to wait longer for a response.<br>In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For User Response After | How long (in seconds) the DNCS should wait for the VOD server to respond after the tuning information is requested.<br>We strongly recommend that you set this parameter to be greater than the **Stop Waiting For Network Response After** parameter for DHCTs. Doing so ensures that a DHCT initiates the teardown of a session before the DNCS does. |
| Highest Program Bandwidth | The maximum allowable bandwidth for VOD sessions. |
| Reuse Expired | How long (in seconds) the system must wait to reuse a session ID after the ID has |

| | |
|---|---|
| Session IDs After | expired<br><br>We recommend that you set this value to at least **3**, but no longer than **5** seconds. |

### Defining Session Signaling Parameters

**Quick Path: DNCS Administrative Console > System Provisioning tab > DNCS System > DSM-CC tab**

Follow these steps to modify existing settings for VOD session signaling.

1. If you have not already done so, follow the **Quick Path** shown above to display the **DSM- CC** (Digital Storage Media - Communication and Control) tab within the DNCS System Configuration window.
2. Enter a new setting in any of the following fields. See Session Signaling Parameter Settings for a description each field in the **DSM- CC** tab and the range of values that we recommend for those fields.

   The following table describes each field in the DSM-CC tab and provides the range of values that we recommend.

| Field | Description |
|---|---|
| **DHCT Session Signaling Parameters** | |
| Send 'Session in Progress' Every | Enter a time (in minutes) that defines how often a DHCT tells the DNCS that a VOD event is in progress. The Session in Progress (SIP) message prevents the system from tearing down sessions while a DHCT receives an event.<br>**Warning:** A reduction in VOD performance may occur when a large number of SIP messages are generated at the same time.<br>We recommend that you generate SIP messages at least every 120 minutes, but no more than 180 minutes. |
| Retry Requests Up To | How many times a DHCT should send a session request to the DNCS .<br>We recommend that you set this value to **1** for one, but no more than 2 retries.<br>Setting this value to two or more times results in subscribers having to wait longer for a response. In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For Network Response After | How long (in seconds) a DHCT should wait for confirmation that the DNCS is processing the session request<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| **Network Session Signal Parameters** | |
| Send 'Setup Proceeding' Every | How long (in seconds) a DHCT must wait to receive confirmation from the DNCS that it is processing the session request that the DHCT sent.<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| Retry Requests Up To | How many times the DNCS should request tuning information from the VOD server for a particular event.<br>We recommend that you set this value to be equal to or greater than the **Retry Requests Up To** parameter for DHCTs.<br>Setting this value to two or more times results in subscribers having to wait longer for a response.<br>In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |

| | |
|---|---|
| Stop Waiting For User Response After | How long (in seconds) the DNCS should wait for the VOD server to respond after the tuning information is requested.<br><br>We strongly recommend that you set this parameter to be greater than the **Stop Waiting For Network Response After** parameter for DHCTs. Doing so ensures that a DHCT initiates the teardown of a session before the DNCS does. |
| Highest Program Bandwidth | The maximum allowable bandwidth for VOD sessions. |
| Reuse Expired Session IDs After | How long (in seconds) the system must wait to reuse a session ID after the ID has expired<br><br>We recommend that you set this value to at least **3**, but no longer than **5** seconds. |

3. Click **Save**. The DNCS saves the information you entered and displays the message "Save complete" at the bottom of the DNCS System Configuration window.

4. Click **Close** to close the DNCS System Configuration window.

### Modifying Existing VOD Session Signaling Parameters

Follow these steps to modify existing settings for VOD session signaling.

1. From the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **DNCS System**. The DNCS System Configuration window opens.
3. Click the **DSM-CC** (Digital Storage Media - Communication and Control) tab.
4. Enter a new setting in any of the fields listed in the table in Session Signaling Parameter Settings.

The following table describes each field in the DSM-CC tab and provides the range of values that we recommend.

| Field | Description |
|---|---|
| **DHCT Session Signaling Parameters** | |
| Send 'Session in Progress' Every | Enter a time (in minutes) that defines how often a DHCT tells the DNCS that a VOD event is in progress. The Session in Progress (SIP) message prevents the system from tearing down sessions while a DHCT receives an event.<br>**Warning:** A reduction in VOD performance may occur when a large number of SIP messages are generated at the same time.<br>We recommend that you generate SIP messages at least every 120 minutes, but no more than 180 minutes. |
| Retry Requests Up To | How many times a DHCT should send a session request to the DNCS .<br>We recommend that you set this value to **1** for one, but no more than 2 retries.<br>Setting this value to two or more times results in subscribers having to wait longer for a response. In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For Network Response After | How long (in seconds) a DHCT should wait for confirmation that the DNCS is processing the session request<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| **Network Session Signal Parameters** | |
| Send 'Setup Proceeding' Every | How long (in seconds) a DHCT must wait to receive confirmation from the DNCS that it is processing the session request that the DHCT sent.<br>We recommend that you set this to at least **5**, but no longer than **10** seconds. |
| Retry Requests Up To | How many times the DNCS should request tuning information from the VOD server for a particular event.<br>We recommend that you set this value to be equal to or greater than the **Retry Requests Up To** parameter for DHCTs.<br>Setting this value to two or more times results in subscribers having to wait longer for a response.<br>In most cases, if the request fails, retries do not resolve the issue, and subscribers have to wait longer for failure notification. If the session request is successful, a retry never occurs. |
| Stop Waiting For | How long (in seconds) the DNCS should wait for the VOD server to respond after |

| | |
|---|---|
| User Response After | the tuning information is requested.<br>We strongly recommend that you set this parameter to be greater than the **Stop Waiting For Network Response After** parameter for DHCTs. Doing so ensures that a DHCT initiates the teardown of a session before the DNCS does. |
| Highest Program Bandwidth | The maximum allowable bandwidth for VOD sessions. |
| Reuse Expired Session IDs After | How long (in seconds) the system must wait to reuse a session ID after the ID has expired<br>We recommend that you set this value to at least **3**, but no longer than **5** seconds. |

5. After you have updated the fields with new data, click **Save**. The DNCS saves the information you entered and displays the message "Save complete" at the bottom of the DNCS System Configuration window.

6. Click **Cancel** to close the DNCS System Configuration window.

## Protect On-Demand Content From Unauthorized Copying

**Quick Path - Without RCS: DNCS Administrative Console > Application Interface Modules > BFS Client > [Expand the OSM File Cabinet] > File > Delete**

**Quick Path - With RCS: DNCS Administrative Console > Application Interface Modules > Please select a site > [Select Site] > BFS Client > [Expand the OSM File Cabinet] > File > Delete**

To protect the content of an encrypted on-demand source, assign CCI to each segment that provides a service from this source. This procedure describes how to configure the Set Up Segment window to assign a level of CCI to an existing segment. To determine the level of security required for each encrypted service you offer to subscribers, contact your corporate office or the content provider.

**Notes:**

- CCI settings are effective immediately.
- In a system where PowerKEY is not used, the provider of the primary conditional access (CA) system is responsible for delivering CCI data to the DHCT.
- A content-protection method is not enforced on OpenCable Host devices that are not running the PowerTV OS. For example, you may require the HDCP to be always on, but the OpenCable Host may disable HDCP for Copy Freely content.

**Important:** If more than one segment has been created from the same source, all segments must have the same levels of content-protection. Otherwise, content-protection may not work as expected for those segments.

**You Need to Know**

Additional Information

For details on these content-protection settings, including the content-protection methods used by output ports on our DHCTs, see Enabling Content Protection for Broadcast Programming Configuration Guide (part number 4005893). To obtain a copy of this publication, see Printed Resources.

Before You Begin

Before you begin, contact your corporate office or your content provider to determine the level of security required for each encrypted service you offer subscribers.

**Important:** CCI is delivered in the ECM for a program. As a result, it may be applied to any **encrypted** source. However, it cannot be applied to a **clear** source because clear sources do not require ECMs.

Time to Complete

Adding security to one segment takes about a minute.

To accommodate earlier versions of VOD or xOD that did not support setting a content-protection level, you could enable content protection for all VOD or xOD services by adding a file called no_vod_cci to the BFS. If this file is present on the BFS, DHCTs automatically activate content protection on 1394 outputs for any VOD or xOD sessions. If you want DHCTs to protect content based on the settings provided by the VOD or xOD application, remove this file from the BFS. For assistance, see Removing the no_vod_cci Flag File.

However, if your VOD provider is unable to set the content-protection settings as required, you can globally

enable content-protection for VOD by adding the no_vod_cci file to the BFS. For assistance, see Creating the no_vod_cci Flag File.

### Removing the no_vod_cci File Flag

If the no_vod_cci file is present on the BFS, DHCTs automatically activate content protection on the 1394 output for any VOD or xOD sessions. For this reason, you should remove the no_vod_cci flag from the BFS if you want DHCTs to protect content based on the settings provided by the VOD or xOD application.

To remove the no_vod_cci file from the BFS, complete the following procedure.

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **OS**. The DHCT OS List window opens.
4. Scroll through the OS list. Is the no_vod_cci file present in the list?
   - If **yes**, select the file and click **File > Delete**. The file is removed from the BFS. All VOD or xOD sessions built from this point forward use the content- protection settings specified in the session setup request.
   - If **no**, go to step 5.
5. Click **File > Close** to close the OS list.
6. Select the **Applications Interface Modules** tab.
7. Are you using our RCS Solution?
   - If **yes**, click **BFS Client**. The Please select a site window opens. Go to step 8.
   - If **no**, click **BFS Client**. The Broadcast File Server List window opens. Go to step 9.
8. Select **DNCS** from the list of sites. Then select **File > Select**. The Broadcast File Server List window opens for the site you selected.
9. Scroll down and double-click the **OSM** cabinet.
10. Is the no_vod_cci file present in the OSM cabinet?
    - If **yes**, select the file.
    - If **no**, go to step 12.
11. Click **File > Delete** to delete the file.
12. Click **File > Close** to close the Broadcast File Server List window.
13. Are you using our RCS Solution?
    - If **no**, you have successfully removed the no_vod_cci file flag.
    - If **yes**, go to step 14.
14. Do you want to remove the no_vod_cci file flag from other sites in your system?
    - If **yes**, from the Please select a site window, select the site whose no_vod_cci flag you want to remove. Then repeat this procedure from step 8 to remove the no_vod_cci flag file from this site.
    - If **no**, you have successfully removed the no_vod_cci file flag from all sites in your system. Select **File > Close** to close the Please select a site window.

### Creating the no_vod_cci File Flag

If your provider is not able to set up content protection for your server, complete the following instructions to set up a VOD file flag (no_vod_cci) to set all content to "copy never."

1. Open an xterm window.
2. At the dncs user prompt, type **pwd** and press **Enter**. The system displays the working directory.
3. Did the system display **/export/home/dncs** as the working directory?
   - If **yes**, go to step 4.
   - If **no**, type **cd /export/home/dncs** and press **Enter**. The system makes /export/home/dncs the working directory.
4. Type **touch no_vod_cci** and press **Enter**. The system creates an empty file in the directory /export/home/dncs and labels the file no_vod_cci.
5. Type **exit** and press **Enter**. The xterm window closes.
6. From the DNCS Administrative Console, select the **DNCS** tab.
7. Select the **Home Element Provisioning** tab.
8. Click **OS**. The DHCT OS List window opens.
9. Click **File > New**. The Set Up DHCT OS window opens.
10. Click **Browse**. The Select OS File window opens.
11. Click in the **Filter** field and type **/export/home/dncs/***. The files in the /export/home/dncs directory appear in the Files list.
12. Scroll down the Files list to find and select the file no_vod_cci that you created. The Selection field updates and displays the path to the no_vod_cci file.
13. Click **OK**. The Select OS File window closes and /export/home/dncs/no_vod_cci appears in the Source File field on the Set Up DHCT OS window.
14. In the **Destination File Name** field, type **bfs:///osm/no_vod_cci**.
15. In the **Description** field, type **File to Activate Content Protection on VOD**.
16. For **Format**, select **Out-of-Band File**.
17. Click **Save**. The system places the no_vod_cci file the BFS carousel and, as a result, DHCTs automatically activate content protection on 1394 outputs for any VOD or xOD sessions.

1. Open an xterm window on the DNCS.
2. Type **cd /export/home/dncs** and press **Enter**. The system makes /export/home/dncs the working directory.
3. Type **touch no_vod_cci** and press **Enter**. The system creates an empty file in the directory /export/home/dncs and labels the file no_vod_cci.
4. Type **exit** and press **Enter**. The xterm window closes.
5. From the DNCS Administration Console, select the **DNCS** tab, and then select the **Home Element Provisioning** tab.
6. Click **OS**. The DHCT OS List window opens.
7. Click **File > New**. The Set Up DHCT OS window opens.
8. Click **Browse**. The Select OS File window opens.

9. Click in the Filter field and type **/export/home/dncs/***. The files in the /export/home/dncs directory appear in the Files list.

10. Scroll down the Files list to find and select the file **no_vod_cci** that you created in step 3. The Selection field updates and displays the path to the no_vod_cci file.

11. Click **OK**. The Select OS File window closes and /export/home/dncs/no_vod_cci appears in the Source File field on the Set Up DHCT OS window.

12. In the Destination File Name field, type **bfs:///osm/no_vod_cci**.

13. In the Description field, type **File to Activate Content Protection on VOD**.

14. For Format, select **Out-of-Band File**.

15. Click **Save**. The system places the no_vod_cci file the BFS carousel and, as a result, DHCTs automatically activate content protection on 1394 outputs for any VOD or xOD sessions.

## Session-Based Encryption for VOD

If you purchased and activated your license for the Session-Based Encryption (SBE) feature, your system can provide encrypted Video-on-demand (VOD) sessions to only the DHCTs that request them.

SBE uses a unique key to encrypt each session so that the session is accessible only to the DHCT that has requested it. Because these sessions are encrypted (secure) and because they are accessible only to the DHCT requesting the session, these sessions are referred to as secure exclusive sessions.

### Setting Up Session-Based Encryption for VOD

The set-up process involves several phases. However, the actual amount of time needed to complete the entire process varies depending on the size of the site and the complexity of the system. In addition, some of the procedures must be completed by Cisco Services engineers.

For details on setting up session-based encryption, refer to Enabling Session-Based Encryption for VOD Services For System Release 2.2/3.2 Application Guide (part number 740223). To obtain a copy of this publication, see Printed Resources.

## Session-Based Encryption for VOD

If you purchased and activated your license for the Session-Based Encryption (SBE) feature, your system can provide encrypted Video-on-demand (VOD) sessions to only the DHCTs that request them.

SBE uses a unique key to encrypt each session so that the session is accessible only to the DHCT that has requested it. Because these sessions are encrypted (secure) and because they are accessible only to the DHCT requesting the session, these sessions are referred to as secure exclusive sessions.

### Setting Up Session-Based Encryption for VOD

The set-up process involves several phases. However, the actual amount of time needed to complete the entire process varies depending on the size of the site and the complexity of the system. In addition, some of the procedures must be completed by Cisco Services engineers.

For details on setting up session-based encryption, refer to Enabling Session-Based Encryption for VOD Services For System Release 2.2/3.2 Application Guide (part number 740223). To obtain a copy of this publication, see Printed Resources.

## Test a Service

**Note:** Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops for services with your billing system vendor.

After you have completed all the steps in setting up a particular type of service, verify that you set up the service successfully by using a test set-top and a television.

Is the new service packaged?

- If **yes**, first authorize the set-top to receive the package.
- If **no**, verify a successful service setup by trying to access the service.

**Related Topics**

- Authorize a Set-Top for a Service
- Verify a Successful Service Setup
- Locating a Set-Top MAC Address

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

▸ Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

▸ Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

▸ Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Authorize a Set-Top or CableCARD Module for a Service

After a set-top or CableCARD module is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a set-top or CableCARD module must be authorized specifically to receive service packages before it can access services that are contained in those packages.

#### You Need to Know

Before You Begin

Before you can authorize a set-top or CableCARD module for a service, you must have the MAC address, IP address, or serial number of the set-top or CableCARD module. You must also connect the set-top to a television and to an RF feed into your network.

Time To Complete

Authorizing a set-top or CableCARD module for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the set-top or CableCARD module to receive the new package information.

Performance Impact

Authorizing a set-top or CableCARD module for a service does not impact network performance. You can complete this procedure any time.

#### Authorizing a DHCT or CableCARD module for a Service

Complete these steps to authorize a DHCT or CableCARD module for a particular service package.

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT or CableCARD module you are testing.

   **Note:** By default, the **Open** and **By MAC Address** options are selected when you open the DHCT Provisioning window.

   **Tip:** When entering IP addresses, type a period to move from octet to octet. Do not press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

7. Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.
8. Verify that the Admin Status field is set to either **In Service One Way** or **In Service Two Way**.
9. Click the **Secure Services** tab.
10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT or CableCARD module to be able to access.

    **Notes:**

    - You can select more than one package by holding down the **Ctrl** key as you click on each

package.

- If your system uses a Brick package, the DHCT or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:

- **IPPV Enable** - If this DHCT or CableCARD module uses IPPV services, enable this option and ensure that the credit limit field is set to a non- zero value.
- **DMS Enable** - Enable this option to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

**Note:** Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to Analog Descrambling Support for the Digital Broadband Delivery System Application Guide (part number 716370) for details. To obtain a copy of this publication, see HLINK_1.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to @.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT or CableCARD module.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT or CableCARD module.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Verify a Successful Service Setup

After you authorize a set-top for a service, you can try to access the service to verify that you set it up correctly.

### You Need to Know

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the set-top time to receive the new service information. You must also connect the set-top to a television and to an RF feed into your network.

Time to Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the set-top has had a chance to receive the service information (usually within 15 minutes).

### Verifying a Successful Service Setup

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
4. Does the service appear as expected?
   - If **yes**, go to step 5.
   - If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact Cisco Services.

### Locating a Set-Top MAC Address

To locate the MAC address of a set-top, do one of the following:

- Display the set-top diagnostic screens.
- Look on the back of the set-top for a label with the MAC address recorded on it.

# Delete a Service

If a service is no longer in use, you should delete the service to maintain a clean system.

## Time to Complete

Deleting a service takes approximately 10 minutes.

## Performance Impact

Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot. If you complete the steps in the order listed in the Process Overview, your will avoid this performance impact.

## Process Overview

To delete a service from your system, complete the following tasks in order:

1. Delete the channel associated with the service from its channel map.
2. Delete the service from the SAM.

# Delete a Service from a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > Delete**

When a service is no longer needed for a particular channel map, delete the service from the channel map.

### Time To Complete

Deleting a service from a channel map takes approximately 5 minutes to complete.

### Performance Impact

Deleting a service from a channel map does not impact network performance. You can complete this procedure at any time.

### Deleting a Service from a Channel Map

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select the service in channel slot.
6. Click **Remove**. The service is now listed under Available Services.
7. If you are removing this service from your system, your next step is to delete the service from the SAM.

# Delete a Service from a Channel Map

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > Delete**

When a service is no longer needed for a particular channel map, delete the service from the channel map.

### Time To Complete

Deleting a service from a channel map takes approximately 5 minutes to complete.

### Performance Impact

Deleting a service from a channel map does not impact network performance. You can complete this procedure at any time.

### Deleting a Service from a Channel Map

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select the service in channel slot.
6. Click **Remove**. The service is now listed under Available Services.
7. If you are removing this service from your system, your next step is to delete the service from the SAM.

## Delete a Service from the SAM

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > [Service Name] > File > Delete**

To remove a service from your system, you must delete the service from the SAM.

### Before You Begin

Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot. For information on deleting a service from a channel map, see Delete a Service from a Channel Map.

### Time To Complete

Deleting a service from the SAM takes approximately 5 minutes to complete.

### Performance Impact

Deleting a service from the SAM does not impact network performance. You can complete this procedure at any time.

### Deleting a Service from the SAM

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **SAM Service**. The SAM Service List window opens.
3. Select the service you want to delete.
4. Click **File > Delete**. A confirmation window opens.
5. Click **Yes** to delete the service from the SAM. The service is removed from the system and no longer displays in the Available Services list for any channel maps.
6. Clean up sources, sessions, and segments associated with the deleted SAM service as needed. Any sources, sessions, and segments associated with a deleted SAM service remain active unless you manually delete the source, session, or segment. In addition, any package that contains a segment associated with the deleted SAM service continues to contain that segment unless you manually delete the segment from the package.

## Delete a Service from the SAM

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Service > [Service Name] > File > Delete**

To remove a service from your system, you must delete the service from the SAM.

### Before You Begin

Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot. For information on deleting a service from a channel map, see Delete a Service from a Channel Map.

### Time To Complete

Deleting a service from the SAM takes approximately 5 minutes to complete.

### Performance Impact

Deleting a service from the SAM does not impact network performance. You can complete this procedure at any time.

### Deleting a Service from the SAM

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **SAM Service**. The SAM Service List window opens.
3. Select the service you want to delete.
4. Click **File > Delete**. A confirmation window opens.
5. Click **Yes** to delete the service from the SAM. The service is removed from the system and no longer displays in the Available Services list for any channel maps.
6. Clean up sources, sessions, and segments associated with the deleted SAM service as needed. Any sources, sessions, and segments associated with a deleted SAM service remain active unless you manually delete the source, session, or segment. In addition, any package that contains a segment associated with the deleted SAM service continues to contain that segment unless you manually delete the segment from the package.

# Maintain the Network

## Introduction

If you have ever owned a car, you know that there are certain tasks you must perform to keep a car performing at its best. The same is true for your DBDS. To provide continuous, quality service to your subscribers, you must keep your system in top condition by performing certain tasks on a regular basis. You must perform some tasks twice a day, while others must be performed only once a month or even less often.

This chapter describes the maintenance schedule of a well-maintained DBDS.

Maintenance Schedule

# Maintenance Schedule

Click on the following links as appropriate to see when you should perform certain tasks.

**Note:** Some of these maintenance tasks require you to pre-configure your system to collect certain data. This requirement is noted with each applicable task. Also, the information presented here is not exhaustive. For a more complete description of maintenance tasks, refer to the Maintenance Recommendations for the DBDS (part number 4002341). If you have questions about any of these tasks, contact Cisco Services.


- Twice a Day
- Once a Day
- Once a Week
- Every Two Weeks
- Once a Month
- Once Every Three Months
- After Every System Upgrade
- After Every EMM CD Installation
- After Every Session Change
- After Every Source Definition Change
- After Every Carousel Change
- Spring and Fall Time Changes


In addition, regularly check that the EAS is functioning properly. Refer to FCC guidelines or, if applicable, guidelines set by your local municipality to determine how often you should check the EAS functionality.

**Important:** We recommend that you run the Doctor Report every morning and every evening. However, you should always run the Doctor Report anytime you suspect or experience problems. For further information about the Doctor Report, refer to the DBDS Utilities Version 5.1 Installation Instructions and DNCS Utilities User's Guide (part number 740020). To obtain a copy of this guide, see Printed Resources.

## Twice a Day

Monitor the items in the following table twice a day. This table contains columns with the following information for each item:

- **Objective:** What you want to see to verify normal operation.
- **Doctor:** Whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the Notes column for additional information.

**Example:** Another logging capability may need to be turned on for the Doctor Report to show the item being monitored.

- **Notes:** Additional information you may need when you monitor a particular item.

| Item | Objective | Doctor | Notes |
|---|---|---|---|
| DNCS Processes | All running | Yes | saManager does not usually run on systems with Aptiv Digital Application Servers. |
| Application Server Processes | All running | Yes | Does not apply to systems with Aptiv Digital Application Servers. |
| System Time Messages (STMs) | Delivered within the last 12 seconds | Yes | Need to enable siManager logging.<br>Can also verify with a DHCT. The DHCT time comes from the STMs. Reboot a DHCT. If you see the correct time on its display, then STMs are being delivered. |
| PPV Files | Updated within the last 60 minutes | Yes | Does not apply to systems with Aptiv Digital Application Servers. |
| Entitlement Unit Table (EUT) | Updated within the last 60 minutes | Yes | If the information in the EUT is wrong, subscribers may not be able to tune to channels they are authorized to receive. |
| GBAMs | TOD and purchase GBAMs delivered within the last 60 seconds | Yes | Need to enable camPsm logging. |
| BFS Status | ▪ All carousels up<br>▪ Sessions active<br>▪ One process per carousel<br>▪ BFSDir updated within the last 60 minutes | Yes | Make sure that the out-of-band data rate is under the maximum allowed rate. |
| Alarms | No alarms present | No | |
| ECM Delivery Errors | No errors present | No | Need to enable camPsm logging. |
| QAM RPC Errors | No errors present | No | Need to enable qamManager logging. |
| 1 Minute BIG Ping | ▪ Average round-trip less than 10 microseconds<br>▪ 0% packet | No | |

| | | | |
|---|---|---|---|
| | loss | | |
| 1 Minute SARA Server Ping from DNCS | ▪ Average round-trip less than 10 microseconds<br>▪ 0% packet loss | No | Does not apply to systems that do not have a SARA server. |
| 1 Minute DNCS Ping from SARA Server | ▪ Average round-trip less than 10 microseconds<br>▪ 0% packet loss | No | Does not apply to systems that do not have a SARA server. |
| 1 Minute DHCT Ping | ▪ Average round-trip less than 10 microseconds<br>▪ 0% packet loss | No | |
| 1 Minute QAM Ping | ▪ Average round-trip less than 10 microseconds<br>▪ 0% packet loss | No | |
| 1 Minute QPSK Ping | ▪ Average round-trip less than 10 microseconds<br>▪ 0% packet loss | No | |
| PPV Events | Can purchase, view, and cancel events | No | |
| Boot DHCT | Enter advanced services within 2 minutes | No | |

## Once a Day

Monitor the items in the following table once a day. This table contains columns with the following information for each item:

- **Objective:** What you want to see to verify normal operation.
- **Doctor:** Whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the Notes column for additional information.
- **Notes:** Additional information you may need when you monitor a particular item.

| Item | Objective | Doctor | Notes |
|---|---|---|---|
| DNCS Corefiles | No core files | Yes | Capture all corefiles and deliver to Cisco Services, especially if they occur near the time of another problem. |
| SARA Server Corefiles | No core files | Yes | Capture all corefiles and deliver to Cisco Services. |
| DNCS Disk Utilization | Each volume using less than 80% | Yes | |
| SARA Server Utilization | Each volume using less than 80% | Yes | Does not apply to systems with Aptiv Digital Application Servers. |
| DNCS Swap Space | More than 200 Megabytes | Yes | |
| SARA Server Swap Space | More than 200 Megabytes | Yes | Does not apply to systems with Aptiv Digital Application Servers. |
| DHCT Software Associations | Make sure each DHCT type is set to either OSM or CVT, not both | Yes* | Doctor reports the OSM associations. You can use the Image List GUI to view CVT associations. |
| Time Sync | ▪ DNCS synchronized with an external source<br>▪ SARA Server synchronized with the DNCS | Yes | You could also synchronize the SARA Server with an external source, and then synchronize the DNCS with the SARA Server. |
| IPG | Seven days' worth of grid information available, along with long descriptions | Yes* | Doctor Report shows IPG file sizes only. An operator must manually check the IPG information through a DHCT. |
| Third-Party Applications | Applications load and run successfully | No | |
| Clear Services | All services OK | No | |
| Subscription Services | All services OK | No | |
| Purchase Report | Information collected OK | No | |
| Database Backup | Backup performed successfully | No | Use dncsDbBackup tape.<br>**Note:** For details, see Backing Up and Restoring the Informix Database (part number 740236). |
| ICMP Redirects | Low number of redirects | No | ▪ Can be done at various points in the network. |

| | | | |
|---|---|---|---|
| | | | ▪ Requires a sniffer or diagnostics on the switches or routers.<br>▪ Ping can help if you use the **-v** option with the **ping** command. |
| Subnet Routes | All routes configured properly | No | |
| QAM Resets | No resets | No | You can obtain this information from bootpd log. |
| QPSK Resets | No resets | No | You can obtain this information from bootpd log. |
| DHCT Resets | Monitor number | No | ▪ Need to enable cmd2000 or hctmMac tracing.<br>▪ Run signonCount for DHCT activity - this does not directly give reboots, but it allows you to see the consequences of any that have occurred. |
| Authorization Delays | Acceptable | No | Need CFET tools. |
| Queue Depths | Acceptable | No | Need CFET tools. |
| Number of PPV Events | Appropriate Number | Yes* | Doctor Report shows the number, but the operator must determine if the number is appropriate for the system. |
| DNCS Load Average | Less than 2.0 per CPU (compare to previous day's check) | Yes* | ▪ Doctor Report shows the previous day's average.<br>▪ Can also run the Top utility to gather this information. |
| Database Report - Poll Non-Responders | Monitor Percentage | Yes* | Doctor Report shows the database numbers. |

## Once a Week

Monitor the items in the following table once a day. This table contains columns with the following information for each item:

- **Objective:** What you want to see to verify normal operation.
- **Doctor:** Whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the Notes column for additional information.
- **Notes:** Additional information you may need when you monitor a particular item.

| Item | Objective | Doctor | Notes |
|---|---|---|---|
| DNCS Load Average | Less than 2.0 per CPU (compare to previous week's check) | Yes* | ▪ Doctor Report shows the previous day's average.<br>▪ Can also run the Top utility to gather this information. |
| SNMP Poll - Poll Non-Responders | Monitor percentage | Yes* | Doctor Report shows the database numbers. |
| Dataspace | Less than 75 percent used | Yes | Use Informix utilities and Doctor Report. |
| Tempspace | Less then 75 percent used | Yes | ▪ **Warning** - 75% to 84% used<br>▪ **Error** - 85% or greater used<br>These values vary depending on how much memory you have allocated for Tempspace. |
| Database Table Extents | Less than 10 extents per table | Yes | Defrag database by using dncsDbData (dbexport/dbimport) to move excess extents to disk. |
| Number of DHCTs | Monitor for growth | Yes | |
| Number of Source Definitions | Monitor for growth | Yes | |
| Number of QAM Modulators | Monitor for growth | Yes | |
| Number of QPSK Modulators and Demodulators | Monitor for growth | Yes | |
| BFS Carousel Rates | ▪ Less then 300 kilobits per second out-of-band<br>▪ Less than 11 Megabits per second (Mbps) for SR 1.2.x or earlier<br>▪ Less then 27 Mbps for SR 1.4 and later | Yes | |
| Number of DHCT Types | ▪ As few as possible | Yes | |

| | | |
|---|---|---|
| | ▪ No "0 DHCT" types | |
| SI_INSERT_RATE | Above calculated value | Yes |
| DCM Verification | Verify that all DCMs are set up properly | No |

## Every Two Weeks

Monitor the items in the following table once a day. This table contains columns with the following information for each item:

- **Objective:** What you want to see to verify normal operation.
- **Notes:** Additional information you may need when you monitor a particular item.

| Item | Objective | Notes |
|---|---|---|
| Run the EMM Deleter | Delete all unneeded staging EMMs | You determine which EMMs to delete based on the age of the EMMs. |

## Once a Month

Create a complete image of your system once a month, once every three months, or after every system upgrade.

## Once Every Three Months

Create a complete image of your system once a month, once every three months, or after every system upgrade.

## After Every System Upgrade

Create a complete image of your system once a month, once every three months, or after every system upgrade.

## After Every EMM CD Installation

After every EMM CD installation, run the Doctor Report to determine how many DHCT types are installed in your system. You should have as few DHCT types as possible and absolutely no "0 DHCT" types.

## After Every Session Change

After every session change and after every source definition change, run the Doctor Report to check the value of SI_INSERT_RATE. This value should be above the calculated value.

## After Every Source Definition Change

After every session change and after every source definition change, run the Doctor Report to check the value of SI_INSERT_RATE. This value should be above the calculated value.

## After Every Carousel Change

After any change in your carousel, you should calculate and change, if necessary, the out-of-band (OOB) CVT message cycle time to decrease the staging times of separable security host with CableCARD module (SSC) DHCTs. Refer to the Separable Security Host Staging Guide for System Release 4.2.1 and Earlier (part number 736107) for more information.

## Spring and Fall Time Changes

After every Spring and Fall time change, run the Doctor Report to make sure that all hubs and DHCTs have the correct DST settings.

# Schedule Service Updates

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Config**

In addition to various other functions, the SAM also communicates service operation attributes to the DHCTs in the network on a regular basis. The frequency of this communication is determined by the SAM Update Timer. The default is 1200 seconds (20 minutes).

You can adjust how many seconds the DNCS waits after you make changes to the SAM or to a channel map before the DNCS generates new SAM files to be broadcast to DHCTs. Adjusting this schedule is useful in various situations.

For example, if you perform frequent single service channel updates, then a short timer (60 seconds) is useful. On the other hand, if you are making many updates that take a long time to enter, a longer timer (5 minutes) is useful.

## Before You Begin

Before you change the SAM Update Timer setting, consult with your system administrator. Also, keep in mind that the delay time between updates should be at least 30 seconds to allow the system enough time to fully process each update.

## Time To Complete

Changing the SAM Update Timer setting takes approximately 10 minutes to complete.

## Performance Impact

Changing the SAM Update Timer setting does not impact network performance. You can complete this procedure at any time.

## Scheduling Service Updates

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Config**. The SAM Configuration window opens.
3. Click in the **Update Timer** field and enter how many seconds the DNCS should wait after you make changes to the SAM or to a channel map before generating new SAM files to broadcast to the DHCTs in your network. This value should be at least **30** seconds.
4. Click in the **Schedule Timer** field and enter a value that is at least two times the Update Timer value. The Schedule Timer is a fail-safe mechanism to ensure DHCTs get updated on a regular basis. The Schedule Timer checks the SAM database to see if there have been any changes since the last update. If so, the system generates new SAM files and broadcasts them.
5. Click **Save**. The system saves these settings in the DNCS database and reconfigures the SAM to send broadcast service updates accordingly.
6. Click **Done** to close the SAM Configuration window and return to the DNCS Administrative Console.

# Schedule Service Updates

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > SAM Config**

In addition to various other functions, the SAM also communicates service operation attributes to the DHCTs in the network on a regular basis. The frequency of this communication is determined by the SAM Update Timer. The default is 1200 seconds (20 minutes).

You can adjust how many seconds the DNCS waits after you make changes to the SAM or to a channel map before the DNCS generates new SAM files to be broadcast to DHCTs. Adjusting this schedule is useful in various situations.

For example, if you perform frequent single service channel updates, then a short timer (60 seconds) is useful. On the other hand, if you are making many updates that take a long time to enter, a longer timer (5 minutes) is useful.

## Before You Begin

Before you change the SAM Update Timer setting, consult with your system administrator. Also, keep in mind that the delay time between updates should be at least 30 seconds to allow the system enough time to fully process each update.

## Time To Complete

Changing the SAM Update Timer setting takes approximately 10 minutes to complete.

## Performance Impact

Changing the SAM Update Timer setting does not impact network performance. You can complete this procedure at any time.

## Scheduling Service Updates

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Config**. The SAM Configuration window opens.
3. Click in the **Update Timer** field and enter how many seconds the DNCS should wait after you make changes to the SAM or to a channel map before generating new SAM files to broadcast to the DHCTs in your network. This value should be at least **30** seconds.
4. Click in the **Schedule Timer** field and enter a value that is at least two times the Update Timer value. The Schedule Timer is a fail-safe mechanism to ensure DHCTs get updated on a regular basis. The Schedule Timer checks the SAM database to see if there have been any changes since the last update. If so, the system generates new SAM files and broadcasts them.
5. Click **Save**. The system saves these settings in the DNCS database and reconfigures the SAM to send broadcast service updates accordingly.
6. Click **Done** to close the SAM Configuration window and return to the DNCS Administrative Console.

# Maintain an RCS

To provide continuous, quality service to subscribers, make sure that you regularly perform maintenance for your DBDS. In addition to regular maintenance, the following tasks can also assist you in maintaining your RCS:

- View the status of key RCS processes
- Verify that RCS applications have registered with the BFS
- Verify that RCS applications are authorized
- View the hubs of a specific site
- View the headends of a specific site
- View the headends or hubs in your RCS network

## View the Headends or Hubs in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Sites Summary**

**Important:** This procedure can be used only for an RCS.

You may want to view all or the headends or hubs in your RCS network so that you can quickly monitor or modify them.

### Viewing the Headends or Hubs in Your RCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Make your next selection based on the following:
   - To view headends, click **Headends**. The Headend Summary window opens.
   - To view hubs, click **Hubs**. The Hub Summary window opens.
5. Click **Exit** to close the Headend Summary or Hub Summary window.

## View the Headends or Hubs in Your RCS

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Sites Summary**

**Important:** This procedure can be used only for an RCS.

You may want to view all or the headends or hubs in your RCS network so that you can quickly monitor or modify them.

### Viewing the Headends or Hubs in Your RCS

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Make your next selection based on the following:
   - To view headends, click **Headends**. The Headend Summary window opens.
   - To view hubs, click **Hubs**. The Hub Summary window opens.
5. Click **Exit** to close the Headend Summary or Hub Summary window.

# View the Headends of an RCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Sites Summary**

**Important:** This procedure can be used only for an RCS.

You may want to view the headends of a specific site so that you can quickly monitor or make changes to a group of headends.

### Viewing the Headends of an RCS Site

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Select** for the site whose headends you want to view.
5. Click **Headends**. The Site Summary window for the site you selected in step 4 opens. From this window, you can complete any of the following tasks:
   - Delete a headend from this site. Go to Delete a Headend in Your RCS.
   - Modify a headend that is in this site. Go to Modify a Headend in Your RCS.
   - Add a headend to this site. Go to Adding a Headend to an RCS Site.
6. Close the Site Summary window by clicking **Exit**.

# View the Headends of an RCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Sites Summary**

**Important:** This procedure can be used only for an RCS.

You may want to view the headends of a specific site so that you can quickly monitor or make changes to a group of headends.

### Viewing the Headends of an RCS Site

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Select** for the site whose headends you want to view.
5. Click **Headends**. The Site Summary window for the site you selected in step 4 opens. From this window, you can complete any of the following tasks:
   - Delete a headend from this site. Go to Delete a Headend in Your RCS.
   - Modify a headend that is in this site. Go to Modify a Headend in Your RCS.
   - Add a headend to this site. Go to Adding a Headend to an RCS Site.
6. Close the Site Summary window by clicking **Exit**.

# View the Hubs of an RCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Sites Summary**

**Important:** This procedure can be used only for an RCS.

You may want to view the hubs of a specific site so that you can quickly view or make changes to a group of hubs.

### Viewing Hubs of an RCS Site

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click the **Select** button for the site whose hubs you want to view.
5. Click **Hubs**. The Hub Summary window for the site you selected in step 4 opens. From this window, you can complete any of the following tasks:
   - Delete a hub from this site. Go Delete a Hub in Your RCS.
   - Modify a hub that is in this site. Go to Modify a Hub in Your RCS.
   - Add a hub to this site. Go to Adding a Hub to an RCS Headend.
6. Close the Site Summary window by clicking **Exit**.

# View the Hubs of an RCS Site

**Quick Path: DNCS Administrative Console > DNCS tab > System Provisioning tab > RNCS Sites > Sites Summary**

**Important:** This procedure can be used only for an RCS.

You may want to view the hubs of a specific site so that you can quickly view or make changes to a group of hubs.

### Viewing Hubs of an RCS Site

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click the **Select** button for the site whose hubs you want to view.
5. Click **Hubs**. The Hub Summary window for the site you selected in step 4 opens. From this window, you can complete any of the following tasks:
   - Delete a hub from this site. Go Delete a Hub in Your RCS.
   - Modify a hub that is in this site. Go to Modify a Hub in Your RCS.
   - Add a hub to this site. Go to Adding a Hub to an RCS Headend.
6. Close the Site Summary window by clicking **Exit**.

## Verify That RCS Applications Have Registered With the BFS

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > Select**

**Important:** This procedure can be used only for systems using our RCS Solution.

Registering applications with the BFS is critical because the BFS provides DHCTs with data they need to provide services to subscribers. The BFS is used because it provides storage for many of the files that a DHCT needs but cannot store locally because of memory limitations. In a sense, you might think of the BFS as an extended hard drive for a DHCT.

Applications that are standard to an RCS network and some non-standard, third-party applications automatically register with the BFS at system startup or when the BFS process is restarted. You can determine whether a third-party application has registered with the BFS client by viewing the BFS List window. Applications that appear in the BFS List window have registered with the BFS client. Because an RCS distributes BFS data to all the sites within the RCS, view the BFS List window of **each site in your RCS** that will use the application.

### Verifying That RCS Applications Have Registered With the BFS

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **BFS Client**. The Site selection window opens and lists each site in your RCS network.
3. Click the site that you want to check. The site is highlighted.
4. Click **File > Select**. The BFS List window appears for the site you selected in step 3 and displays all applications that have registered with the BFS.
5. Examine the applications listed in the BFS Client List window to verify that all RCS applications have registered with the BFS. The following applications are standard and should appear in the BFS Client List window of any site.
   - **IPG_eng** - Provides data in English for the interactive program guide
   - **MMMAud** - Provides audio files, such as those that may accompany an Emergency Alert Message.
   - **MMMCfg** - Provides configurations of multimedia messages, such as those in Emergency Alert Messages
   - **bootloader** - Provides DHCTs with appropriate operating system and/or applications software
   - **camPsm** - Sends conditional access information used by the pay-per-view application
   - **osm** - Used by the operating system manager to load image files onto the BFS for distribution to DHCTs
   - **ppv** - Used for pay-per-view service
   - **sam** - Used by the Service Application Manager to define the services a site provides
   - **sgm** - Used for service group mapping

   **Note:** In addition to these servers required standard applications, a site may have other servers listed to support additional applications.

   **Example:** If a site supports OpenCable standards, the **pod** server should also appear in the BFS List window of that site.

6. If any applications have not registered with the BFS, verify that the applications are authorized. Go to Verify That RCS Applications Are Authorized.

## Verify That RCS Applications Have Registered With the BFS

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > BFS Client > File > Select**

**Important:** This procedure can be used only for systems using our RCS Solution.

Registering applications with the BFS is critical because the BFS provides DHCTs with data they need to provide services to subscribers. The BFS is used because it provides storage for many of the files that a DHCT needs but cannot store locally because of memory limitations. In a sense, you might think of the BFS as an extended hard drive for a DHCT.

Applications that are standard to an RCS network and some non-standard, third-party applications automatically register with the BFS at system startup or when the BFS process is restarted. You can determine whether a third-party application has registered with the BFS client by viewing the BFS List window. Applications that appear in the BFS List window have registered with the BFS client. Because an RCS distributes BFS data to all the sites within the RCS, view the BFS List window of **each site in your RCS** that will use the application.

### Verifying That RCS Applications Have Registered With the BFS

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **BFS Client**. The Site selection window opens and lists each site in your RCS network.
3. Click the site that you want to check. The site is highlighted.
4. Click **File > Select**. The BFS List window appears for the site you selected in step 3 and displays all applications that have registered with the BFS.
5. Examine the applications listed in the BFS Client List window to verify that all RCS applications have registered with the BFS. The following applications are standard and should appear in the BFS Client List window of any site.
   - **IPG_eng** - Provides data in English for the interactive program guide
   - **MMMAud** - Provides audio files, such as those that may accompany an Emergency Alert Message.
   - **MMMCfg** - Provides configurations of multimedia messages, such as those in Emergency Alert Messages
   - **bootloader** - Provides DHCTs with appropriate operating system and/or applications software
   - **camPsm** - Sends conditional access information used by the pay-per-view application
   - **osm** - Used by the operating system manager to load image files onto the BFS for distribution to DHCTs
   - **ppv** - Used for pay-per-view service
   - **sam** - Used by the Service Application Manager to define the services a site provides
   - **sgm** - Used for service group mapping

   **Note:** In addition to these servers required standard applications, a site may have other servers listed to support additional applications.

   **Example:** If a site supports OpenCable standards, the **pod** server should also appear in the BFS List window of that site.

6. If any applications have not registered with the BFS, verify that the applications are authorized. Go to Verify That RCS Applications Are Authorized.

# Verify That RCS Applications Are Authorized

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > Select**

**Important:** This procedure can be used only for an RCS.

For an application to register with the BFS client on the DNCS, the application first must be authorized on the BFS Administration window. If you are installing a third-party application on your RCS, authorize the application from the BFS Administration window so that the application can register with the BFS client. Because an RCS distributes BFS data to all sites within the network, view the BFS Administration window for each site whose applications you want to verify.

**Notes:**

- If you determine that a third-party application has not automatically registered with the BFS client, manually register the application with the BFS client by registering the application's server.
- For an overview of all steps required to install a third-party application, see Supporting a Third-Party Application.

**Verifying That RCS Applications Are Authorized**

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The Site selection window opens and lists each site in your RCS network.
3. Click the site that you want to check. The site is highlighted.
4. Click **File > Select**. The BFS Administration window appears for the site you selected in step 3.
5. Click the **Servers** tab. The servers of this site that have been authorized to register with the BFS appear in the list.
6. If any servers are missing, the application has not automatically registered with the BFS client. To correct this, manually register the application with the BFS client.

# Verify That RCS Applications Are Authorized

**Quick Path: DNCS Administrative Console > Application Interface Modules tab > BFS Admin > File > Select**

**Important:** This procedure can be used only for an RCS.

For an application to register with the BFS client on the DNCS, the application first must be authorized on the BFS Administration window. If you are installing a third-party application on your RCS, authorize the application from the BFS Administration window so that the application can register with the BFS client. Because an RCS distributes BFS data to all sites within the network, view the BFS Administration window for each site whose applications you want to verify.

**Notes:**

- If you determine that a third-party application has not automatically registered with the BFS client, manually register the application with the BFS client by registering the application's server.
- For an overview of all steps required to install a third-party application, see Supporting a Third-Party Application.

**Verifying That RCS Applications Are Authorized**

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The Site selection window opens and lists each site in your RCS network.
3. Click the site that you want to check. The site is highlighted.
4. Click **File > Select**. The BFS Administration window appears for the site you selected in step 3.
5. Click the **Servers** tab. The servers of this site that have been authorized to register with the BFS appear in the list.
6. If any servers are missing, the application has not automatically registered with the BFS client. To correct this, manually register the application with the BFS client.

# Database Backup and Restore

The Informix database on the DNCS contains all headend configuration information, as well as data needed to provision and authorize set-tops. In the event of a power failure, for instance, you might need to restore the database. Only through regular daily backups of your database can you ensure the integrity and persistence of your system data.

For more information and specific instructions for backing up and restoring the Informix database, refer to Backing Up and Restoring the Informix Database (part number 740236).

**Related Topics**

- Database Backup and Restore Recommendations
- Power Failure Recovery

## Recommendations

Consider the following recommendations before you backup and restore your Informix database.

**Note:** For specific procedures concerning any of these recommendations, refer to Backing Up and Restoring the Informix Database (part number 740236).

### Related Topics

- DNCS Recommendations
- Database Backup Recommendations
- Database Restore Recommendations
- Tape Recommendations

### DNCS Recommendations

We strongly recommend that you connect the DNCS to a Uninterruptible Power Supply (UPS) to prevent unexpected and abrupt power failures of the DNCS.

### Related Topics

- Introduction
- Database Backup Recommendations
- Database Restore Recommendations
- Tape Recommendations
- Power Failure Recovery

### Database Backup Recommendations

Consider the following recommendations when you backup your database.

- We strongly recommend that you backup your database once each day, preferably early in the morning or late at night, when system activity is usually at a minimum.
- Avoid backing up your database while you are performing any of the following system tasks:
  - Running the Interactive Program Guide (IPG) Collector
  - Loading an Entitlement Management Message (EMM) CD
  - Staging Set-Tops
- To back up the Informix database, you must have a tape drive connected to or included in your system. Some platforms contain internal tape drives, others must use external tape drives. Refer to Backing Up and Restoring the Informix Database (part number 740236) for procedures to add and verify a tape drive on your system.
- You do not have to shut down the DNCS or the Application Server to back up your Informix database. All system components can be running while you back up the database.
- It can take up to 30 minutes to back up a typical database with approximately 100,000 set-tops.

### Related Topics

- DNCS Recommendations
- Database Restore Recommendations
- Tape Recommendations
- Power Failure Recovery

### Database Restore Recommendations

You need the tapes from your most recent database backup to restore the Informix database.

### Related Topics

- DNCS Recommendations
- Database Backup Recommendations
- Tape Recommendations
- Power Failure Recovery

### Tape Recommendations

Consider the following recommendations concerning your tape drives and the tapes that you use for the database backup.

- Use seven tapes (or sets of tapes) for the database backup, one for each day of the week.

**Important:** The tapes that you use to back up your Informix database wear out over time. Be sure to replace your tapes at least once a year.

- You can back up your Informix database to either a 4-mm or an 8-mm data tape. The type of tape you choose depends upon the type of tape drive installed on your DNCS. An 8-mm tape is too big for a 4-mm tape drive; a 4-mm tape is too small for an 8-mm tape drive. Ask the person who handles your account if you are not sure which type of tape is appropriate for your system.
- You can purchase 4-mm tapes or 8-mm tapes in various lengths. While all tapes wear out over time, a longer tape is likely to wear out quicker than a shorter tape because the strength of a tape is inversely proportional to the length of the tape. Use the following guidelines when you purchase tapes to back up your Informix database:
  - 4-mm tapes: Do not exceed 150 meters
  - 8-mm tapes: Do not exceed 160 meters
- Depending on the size of your database, you may need more than one tape to do a complete backup. If you need more than one tape to back up your database, the backup script will prompt you to remove the existing tape and to insert a new tape at the appropriate time.
- The script used by the DNCS to back up the Informix database uses the following default tape drive configuration:
  - Tape size: 5859375 KB
  - Block size: 16
  - Device name: /dev/rmt/0h

This tape drive configuration is in use on a majority of systems. Occasionally, the tape drive on a system may be configured with a different device name, such as /dev/rmt/1h.

**Note:** The 'h' that appears at the end of device name /dev/rmt/0h or /dev/rmt/1h indicates that the system is to use a high density format when writing to the tape.

### Related Topics

DNCS Recommendations

Database Backup Recommendations

Database Restore Recommendations

Power Failure Recovery

# Power Failure Recovery

## Power Failure Recovery Process

If the DNCS fails due to a power failure (or for any other reason), follow these steps to ensure a graceful return to service.

1. Check the database logs for errors. Go to Checking the Database Log for Errors for more information.
2. Does the database log contain errors?
   - If **yes**, locate your latest database backup tapes and contact Cisco Services.
   - If **no**, restart the DNCS and recheck the log to see if other problems are indicated.
3. Are other problems indicated by the database log?
   - If **yes**, locate your latest database backup tapes and contact Cisco Services.
   - If **no**, your database should work correctly.

# Power Failure Recovery

## Power Failure Recovery Process

If the DNCS fails due to a power failure (or for any other reason), follow these steps to ensure a graceful return to service.

1. Check the database logs for errors. Go to Checking the Database Log for Errors for more information.
2. Does the database log contain errors?
   - If **yes**, locate your latest database backup tapes and contact Cisco Services.
   - If **no**, restart the DNCS and recheck the log to see if other problems are indicated.
3. Are other problems indicated by the database log?
   - If **yes**, locate your latest database backup tapes and contact Cisco Services.
   - If **no**, your database should work correctly.

## Checking the Database Log for Errors

Solaris panics are logged in the /var/adm/messages file, and Informix assertion failures are logged in the export/home/informix/online.log. To determine whether you should contact Cisco Services, look for messages in the /export/home/informix/online.log stating that Informix performed work during fast recovery.

## Example: Defrag not necessary

The following example indicates that your tables do not need to be defragmented. Messages indicate that no work was needed or performed during the recovery. This example shows what you will see upon startup after a graceful shutdown.

```
15:16:36 Physical Recovery Started.
15:16:36 Physical Recovery Complete: 0 Pages Restored.

15:16:36 Logical Recovery Started.
15:16:36 20 recovery worker threads will be started.
15:16:39 Logical Recovery Complete.
0 Committed, 0 Rolled Back, 0 Open, 0 Bad Locks
```

In this case, you should restart the system and verify that there are no other problems, then check the log files once again for errors.

## Example: Defrag necessary

The following example indicates that you should contact Cisco Services. Messages indicate that 1776 pages were restored, 2995 records were committed, and 14 records were rolled back. This example shows what you will see upon startup after an uncontrolled shutdown.

```
12:09:11 Physical Recovery Started.
12:09:12 Physical Recovery Complete: 1776 Pages Restored.

12:09:12 Logical Recovery Started.
12:09:12 20 recovery worker threads will be started.
12:09:17 Logical Recovery Complete.
2995 Committed, 14 Rolled Back, 0 Open, 0 Bad Locks
```

In cases like this, you should contact Cisco Services to defragment your tables and rebuild your indexes.

# Help Not Available

Online Help is not available for this feature. If you have questions about this feature, please refer to the printed documentation for this feature.

# Monitor the Network

## Introduction

The topics in this chapter can help you use tools on the digital network control system (DNCS) to monitor your digital broadband delivery system (DBDS).

Introduction

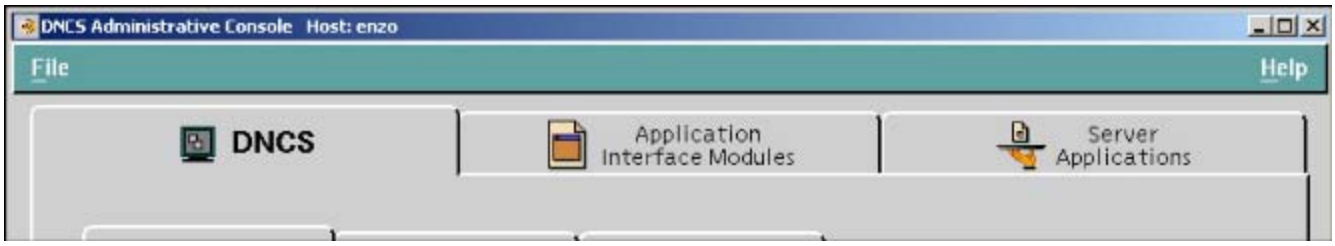
# Overview

The following topics can help you use tools on the DNCS to monitor your DBDS:

- DNCS Administrative Console Status window - The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server. In addition, if your DBDS uses Spectrum Network Management System (NMS), you can monitor most of the devices in your network.
- Monitoring DNCS Processes - The DNCS Control window provides a list of all the major processes on the DNCS workstation along with the working state of each, giving you an at-a-glance status of the DNCS.
- Monitoring SARA Server Processes - The AppServer Control window provides a list of all the major processes on the SARA Server workstation along with the working state of each, giving you an at-a-glance status of the SARA Server.
- Monitoring Network Elements With Spectrum NMS - If your DBDS uses Spectrum NMS, you can monitor most of the devices in your network and use the Alarm Manager to obtain an at-a-glance status of network elements.
- DHCT Performance - You can monitor DHCT performance by turning on the performance monitoring function. The DHCT performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of DHCTs.
- VOD Performance - If your system supports VOD, you can monitor VOD performance by turning on the performance monitoring function. The VOD performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of a VOD exclusive session.
- UI Servers - You can obtain an at-a-glance status of DNCS User Interface (UI) Servers or configure a UI Server.

# DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.




For more information, click on a specific tab name in the following list.

- DNCS tab
- Application Interface Modules tab
- Server Applications tab

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console Status window also displays the Network Management tab.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Administrative Console Status

The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.


For more information, click on a specific section name in the following list.

- DNCS section
- AppServer section

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console window also displays the **NMS** and **Alarms** sections.


- The **NMS** section indicates whether or not the Spectrum NMS software is in operation.
- The **Alarms** section indicates the number of critical, major, and minor alarm conditions, if any, which are present in the DBDS as reported by the Spectrum NMS.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Status

The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- **Running** the DNCS software package is present and in operation
- **Inactive** the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

## Application Server Status

The **AppServer** section of the Administrative Console Status window indicates whether or not the Application Server is in operation based on the following conditions:

- **Running** the Application Server software package is present and in operation
- **Inactive** the Application Server software package is present, but not in operation
- **Not Responding** the Application Server does not respond when the DNCS tries to communicate with it
- **Not Installed** a Application Server host is defined in the host table, but the Application Server software package is not present; this usually indicates that you are not using our Application Server, but the

application server of another vendor

- **Blank** no Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using our Application Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the Application Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major Application Server processes.

**WARNING:**

**Do NOT attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.**

The Application Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server (DHCT Configuration Server**) Generates the files containing the global, hub-specific, and staging configuration values and places the files on the broadcast server.
- **IPGServer - language supported (Interactive Program Guide Server)** Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, and Japanese.

**Note:** Each language that is supported has its own application. For example, if English is supported, the application would be listed as **IPGServer- eng**.

- **ppvfileserver (Pay-per-view File Server)** Generates PPV files and places those files on the Broadcast File Server.
- **ppvServer (Pay-per-view Server)** Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.
- **vcServer (Virtual Channel Server)** Places the files for all configured virtual channels on the Broadcast File Server.
- **bfsRouter (Broadcast File Server Router)** For a Regional Control System (RCS), routes BFS Application Program Interface (API) calls from the SARA Server, such as IPG, PPV, or VCS, to the BFS on the DNCS at the central RCS site. The BFS Server on the central RCS site is site-aware. The BFS router converts any non-site BFS calls to site-specific calls and passes them along to the BFS server. This includes calls from Application Server processes, such as IPG, PPV, VCS, and any other third-party applications using the BFS API.

For more information on the SARA Server, refer to the SARA Application Server 3.4.1 User Guide (part number 4012159). See Printed Resources for information on obtaining documentation.

## Monitoring Alarms

If you are using the Spectrum NMS, you can use the Alarm Manager to check on the status of your network elements Monitor button in the NMS area of the DNCS Administrative Console Status window.

The Alarms area of the DNCS Administrative Console Status window indicates the number of critical (**Cr**), major (**Mj** ), and minor (**Mn**) alarm conditions present in the DBDS. When you click the **Monitor** button in the Alarms area of the DNCS Administrative Console Status window, the Alarm Manager window opens.

The following example shows no critical alarms, so the associated box is **gray**. If there were any critical alarms, the **Cr** box would be **red**. Major alarms (Mj) appear as **orange**, and minor alarms (Mn) appear as **yellow**.


The following table describes each alarm severity level.

| Alarm Severity | Indicator | Description |
|---|---|---|
| Critical | Cr | A condition has occurred that is affecting service. |
| Major | Mj | A condition has occurred that will affect service if not corrected. |
| Minor | Mn | A condition has occurred that is not affecting service, but that could degrade system performance if not corrected. |

You can monitor alarm conditions within the DBDS by clicking the **Monitor** button in the Alarms area of the DNCS Administrative Console Status window to open the Alarm Manager window. The Alarm Manager window lists each alarm that occurs in the network, along with the element that generated the alarm. A color code indicates the condition of each element. This color code is identical to the color code used on the SpectroGRAPH.

The Alarm Manager window also includes other information, such as the following:

- Date and time the alarm occurred
- Model number of the affected element
- Description and probable cause of the alarm
- Troubleshooter option to help isolate the problem

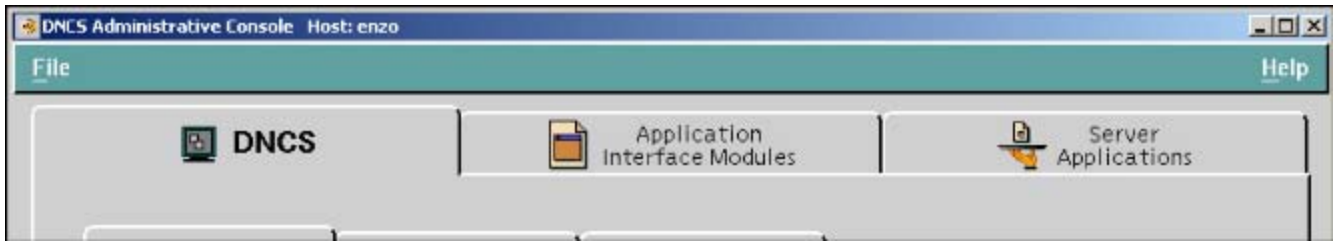
You do not need to do anything to remove an alarm from the Alarm Manager window. When you correct the alarm condition, the alarm automatically disappears from the window.

Use the Alarm Manager window to monitor alarms within the DBDS, including alarms for specific DHCTs. This is especially helpful if you are having problems with only a few DHCTs in the field.

**Note:** The Alarm Manager is part of the Spectrum NMS. The Spectrum NMS contains its own Help documentation. If you have questions on how to use the Alarm Manager beyond this discussion, click the **Help** menu that appears in the toolbar at the top of the Alarm Manager window.

# DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.




For more information, click on a specific tab name in the following list.

- DNCS tab
- Application Interface Modules tab
- Server Applications tab

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console Status window also displays the Network Management tab.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

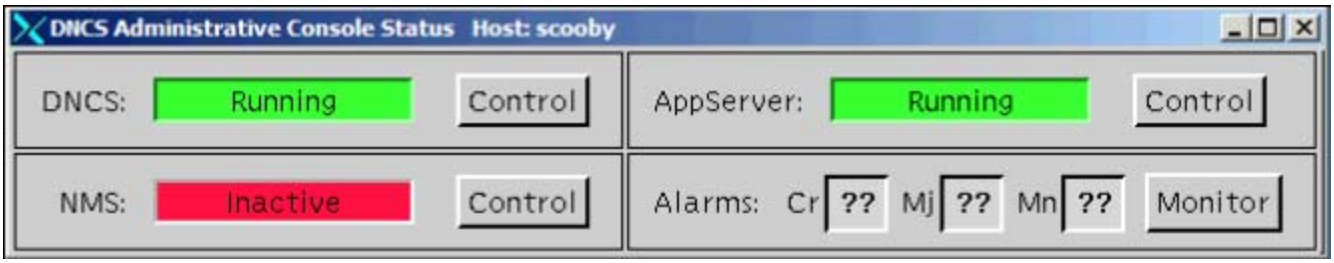
## DNCS Administrative Console Status

The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.


For more information, click on a specific section name in the following list.

- DNCS section
- AppServer section

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console window also displays the **NMS** and **Alarms** sections.




- The **NMS** section indicates whether or not the Spectrum NMS software is in operation.
- The **Alarms** section indicates the number of critical, major, and minor alarm conditions, if any, which are present in the DBDS as reported by the Spectrum NMS.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Status

The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- **Running** — the DNCS software package is present and in operation
- **Inactive** — the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

## Application Server Status

The **AppServer** section of the Administrative Console Status window indicates whether or not the Application Server is in operation based on the following conditions:

- **Running** — the Application Server software package is present and in operation
- **Inactive** — the Application Server software package is present, but not in operation
- **Not Responding** — the Application Server does not respond when the DNCS tries to communicate with it
- **Not Installed** — a Application Server host is defined in the host table, but the Application Server software package is not present; this usually indicates that you are not using our Application Server, but the application server of another vendor
- **Blank** — no Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using our Application Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the Application Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major Application Server processes.

**WARNING:**

**Do NOT attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.**

The Application Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server (DHCT Configuration Server**) — Generates the files containing the global, hub-specific, and staging configuration values and places the files on the broadcast server.
- **IPGServer - language supported (Interactive Program Guide Server)** — Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, and Japanese.

  **Note:** Each language that is supported has its own application. For example, if English is supported, the application would be listed as **IPGServer- eng**.

- **ppvfileserver (Pay-per-view File Server)** — Generates PPV files and places those files on the Broadcast File Server.
- **ppvServer (Pay-per-view Server)** — Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.
- **vcServer (Virtual Channel Server)** — Places the files for all configured virtual channels on the Broadcast File Server.
- **bfsRouter (Broadcast File Server Router)** — For a Regional Control System (RCS), routes BFS Application Program Interface (API) calls from the SARA Server, such as IPG, PPV, or VCS, to the BFS on the DNCS at the central RCS site. The BFS Server on the central RCS site is site-aware. The BFS router converts any non-site BFS calls to site-specific calls and passes them along to the BFS server. This includes calls from Application Server processes, such as IPG, PPV, VCS, and any other third-party applications using the BFS API.

For more information on the SARA Server, refer to the SARA Application Server 3.4.1 User Guide (part number 4012159). See Printed Resources for information on obtaining documentation.

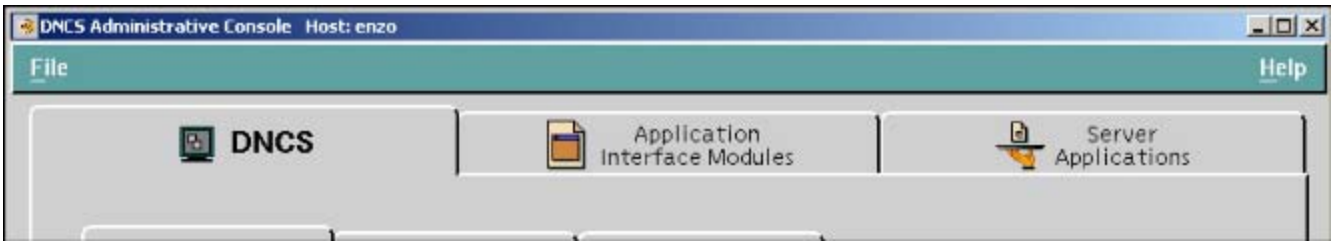
# Overview

The following topics can help you use tools on the DNCS to monitor your DBDS:

- DNCS Administrative Console Status window - The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server. In addition, if your DBDS uses Spectrum Network Management System (NMS), you can monitor most of the devices in your network.
- Monitoring DNCS Processes - The DNCS Control window provides a list of all the major processes on the DNCS workstation along with the working state of each, giving you an at-a-glance status of the DNCS.
- Monitoring SARA Server Processes - The AppServer Control window provides a list of all the major processes on the SARA Server workstation along with the working state of each, giving you an at-a-glance status of the SARA Server.
- Monitoring Network Elements With Spectrum NMS - If your DBDS uses Spectrum NMS, you can monitor most of the devices in your network and use the Alarm Manager to obtain an at-a-glance status of network elements.
- DHCT Performance - You can monitor DHCT performance by turning on the performance monitoring function. The DHCT performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of DHCTs.
- VOD Performance - If your system supports VOD, you can monitor VOD performance by turning on the performance monitoring function. The VOD performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of a VOD exclusive session.
- UI Servers - You can obtain an at-a-glance status of DNCS User Interface (UI) Servers or configure a UI Server.

# DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.




For more information, click on a specific tab name in the following list.

- DNCS tab
- Application Interface Modules tab
- Server Applications tab

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console Status window also displays the Network Management tab.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Administrative Console Status

The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.


For more information, click on a specific section name in the following list.

- DNCS section
- AppServer section

In addition, if you are using the Spectrum NMS, the DNCS Administrative Console window also displays the **NMS** and **Alarms** sections.


- The **NMS** section indicates whether or not the Spectrum NMS software is in operation.
- The **Alarms** section indicates the number of critical, major, and minor alarm conditions, if any, which are present in the DBDS as reported by the Spectrum NMS.

**Note:** We offer a separate product called the DBDS Alarm Management System to help you monitor your network elements instead of Spectrum. For more information, contact the representative who handles your account.

## DNCS Status

The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- **Running** — the DNCS software package is present and in operation
- **Inactive** — the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

## Application Server Status

The **AppServer** section of the Administrative Console Status window indicates whether or not the Application Server is in operation based on the following conditions:

- **Running** — the Application Server software package is present and in operation
- **Inactive** — the Application Server software package is present, but not in operation
- **Not Responding** — the Application Server does not respond when the DNCS tries to communicate with it
- **Not Installed** — a Application Server host is defined in the host table, but the Application Server software package is not present; this usually indicates that you are not using our Application Server, but the

application server of another vendor

- **Blank** — no Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using our Application Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the Application Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major Application Server processes.

**WARNING:**

**Do NOT attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.**

The Application Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server (DHCT Configuration Server**) — Generates the files containing the global, hub-specific, and staging configuration values and places the files on the broadcast server.
- **IPGServer - language supported (Interactive Program Guide Server)** — Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, and Japanese.

  **Note:** Each language that is supported has its own application. For example, if English is supported, the application would be listed as **IPGServer- eng**.

- **ppvfileserver (Pay-per-view File Server)** — Generates PPV files and places those files on the Broadcast File Server.
- **ppvServer (Pay-per-view Server)** — Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.
- **vcServer (Virtual Channel Server)** — Places the files for all configured virtual channels on the Broadcast File Server.
- **bfsRouter (Broadcast File Server Router)** — For a Regional Control System (RCS), routes BFS Application Program Interface (API) calls from the SARA Server, such as IPG, PPV, or VCS, to the BFS on the DNCS at the central RCS site. The BFS Server on the central RCS site is site-aware. The BFS router converts any non-site BFS calls to site-specific calls and passes them along to the BFS server. This includes calls from Application Server processes, such as IPG, PPV, VCS, and any other third-party applications using the BFS API.

For more information on the SARA Server, refer to the SARA Application Server 3.4.1 User Guide (part number 4012159). See Printed Resources for information on obtaining documentation.

## Monitoring Alarms

If you are using the Spectrum NMS, you can use the Alarm Manager to check on the status of your network elements Monitor button in the NMS area of the DNCS Administrative Console Status window.

The Alarms area of the DNCS Administrative Console Status window indicates the number of critical (**Cr**), major (**Mj** ), and minor (**Mn**) alarm conditions present in the DBDS. When you click the **Monitor** button in the Alarms area of the DNCS Administrative Console Status window, the Alarm Manager window opens.

The following example shows no critical alarms, so the associated box is **gray**. If there were any critical alarms, the **Cr** box would be **red**. Major alarms (Mj) appear as **orange**, and minor alarms (Mn) appear as **yellow**.


The following table describes each alarm severity level.

| Alarm Severity | Indicator | Description |
|---|---|---|
| Critical | Cr | A condition has occurred that is affecting service. |
| Major | Mj | A condition has occurred that will affect service if not corrected. |
| Minor | Mn | A condition has occurred that is not affecting service, but that could degrade system performance if not corrected. |

You can monitor alarm conditions within the DBDS by clicking the **Monitor** button in the Alarms area of the DNCS Administrative Console Status window to open the Alarm Manager window. The Alarm Manager window lists each alarm that occurs in the network, along with the element that generated the alarm. A color code indicates the condition of each element. This color code is identical to the color code used on the SpectroGRAPH.

The Alarm Manager window also includes other information, such as the following:

- Date and time the alarm occurred
- Model number of the affected element
- Description and probable cause of the alarm
- Troubleshooter option to help isolate the problem

You do not need to do anything to remove an alarm from the Alarm Manager window. When you correct the alarm condition, the alarm automatically disappears from the window.

Use the Alarm Manager window to monitor alarms within the DBDS, including alarms for specific DHCTs. This is especially helpful if you are having problems with only a few DHCTs in the field.

**Note:** The Alarm Manager is part of the Spectrum NMS. The Spectrum NMS contains its own Help documentation. If you have questions on how to use the Alarm Manager beyond this discussion, click the **Help** menu that appears in the toolbar at the top of the Alarm Manager window.

# DNCS Processes

## Monitoring DNCS Processes

You can monitor all of the major DNCS processes by clicking the **Control** button in the DNCS area of the DNCS Administrative Console Status window to open the DNCS Control window. The DNCS Control window provides a list of all the major processes on the DNCS workstation, along with the working state of each.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

We recommend that you leave the DNCS Control window open and visible at all times to help you monitor your system. For more information on monitoring DNCS processes, click here.

### Descriptions of DNCS Processes

The following table describes each of the processes listed on the DNCS Control window.

| Process | Description |
|---|---|
| alarmCollector | **Alarm Collector** Retrieves alarms from all network elements, and then sends the alarms to the Spectrum NMS.<br>This process shows only when the Spectrum Network Management System (NMS) is used.<br>For more information about the DBDS Alarm Management System, contact your the representative who handles your account. |
| bfsRemote | **Broadcast File System (BFS) Remote** Manages the processes (dataPump processes) that continuously transmit BFS data.<br>The BFS facilitates delivery of information to DHCTs. |
| bfsServer | **BFS Server** Manages the addition and deletion of files from the BFS. |
| bigManager | **Broadband Integrated Gateway (BIG) Manager** Monitors and manages the operation of BIGs, including establishing sessions and allocating MPEG program-specific information (PSI). |
| bossDiagnosticsServer | **Business Operations Support System (BOSS) Diagnostics Server** Acts as an SNMP proxy agent between the billing system and DHCTs by going through the DNCS to retrieve information from DHCTs for the billing system. |
| bossServer | **BOSS Server** Communicates with the billing system, the DHCT Manager, and the DNCS Administrative Console. |
| bsm | **Broadcast Segment Manager** Receives notification from the SI Manager when broadcast sources start, and then forwards the notifications to the Conditional Access (CA) system. |
| caaServer | CA Authority (CAA) Server Creates and sends the CAA and entitlement authorization (EA) entitlement management messages (EMMs) required for staging DHCTs.<br>**Note:** The caaServer process was called the **Caa** process in system releases prior to 1.4. |
| camAm | **CA Manager (CAM) Authorization Manager** Creates EMMs for security elements to authorize DHCTs to receive secure events. |
| camAuditor | **CAM Auditor** Refreshes or creates EMMs on DHCTs, which allow the |

| | |
|---|---|
| | subscriber to view secure events. |
| camEx | **CAM Exclusive Sessions** Provides conditional access for VOD sessions; generates interactive session keys (ISKs) for each session and ISK EMMs for delivery to the QAM modulators and DHCTs; generates entitlement control messages (ECMs) for the QAM modulators so they can encrypt these sessions. |
| camFastRefresh | **CAM Fast Refresh** Queries the database for EMMs, puts the EMMs in files, and puts the files on the BFS (files are refreshed periodically when EMMs are changed in the system); sends staging EMMs over inband BFS to DHCTs that are candidates for the Fast Refresh List. |
| camPsm | **CAM Program Segment Manager (PSM)** Sends PPV and CA Time-of-Day global broadcast authenticated messages (GBAMs); inserts CA information, including ECMs into the program segment at the QAM modulator level. |
| camTEDChecker | **CAM Transaction Encryption Device (TED) Checker** indicates whether or not the TED is running as follows:<br>▪Green the TED is in service and the keys have been initialized<br>▪Yellow the TED software is running, but the keys have not been initialized<br>▪Red the TED software is not running<br>For more information about the TED, refer to Transaction Encryption Device FX Server Installation and Operation Guide (part number 736138). To obtain a copy of this guide, see Printed Resources.<br>This process was first introduced in SR 2.1.1. |
| CCardServer | **CableCARD Server** Creates and maintains the PowerKEY CableCARD Module BFS file of CableCARD Module/host pair authorizations; also provides global configuration information to the CableCARD Module population.<br>This process was first introduced in SR 2.2 and SR 3.2. |
| dbSync | **Database Synchronizer** Ensures that databases on the DNCS and on each RNCS/LIONN are correctly updated with the most recent information. |
| dncsSnmpAgent | **DNCS Simple Network Management Protocol (SNMP) Agent** - Retrieves alarms from all network elements, and then sends the alarms to our DBDS Alarm Management System (NMS) or to a third-party NMS.<br>For more information about the DBDS Alarm Management System, contact the representative who handles your account. |
| dncs-snmpd-big<br>dncs-snmpd-qam<br>dncs-snmpd-qpsk | **DNCS SNMP** Ensures that network elements that are not SNMP-compliant (BIGs and QAM modulators, MQAM modulators and QPSK modulators) can communicate with the Spectrum NMS through SNMP protocol.<br>In other words, the dncs-snmp acts as a proxy agent for each of these elements. |
| drm | **Digital Resource Manager** Manages the allocation of DBDS resources for setting up sessions.<br>The drm process was part of the dsm process in system releases prior to 1.4. |

| | |
|---|---|
| dsm | **Digital Session Manager** Manages digital video sessions (broadcast and exclusive) on the DNCS.<br><br>When using Overlay technology, the DSM manages sessions for only our DHCTs. |
| EARS | **Emergency Alert The Emergency Alert Receiver Server** Monitors a designated port on the DNCS to receive Emergency Alert Messages (EAMs). After receiving an EAM, EARS processes it differently, depending upon whether EARS is operating in an RCS site or in a non-RCS site. |
| emmDistributor | **EMM Distributor** Distributes EMMs to DHCTs over the out-of-band path. |
| eventManager | **Event Manager** Ensures that events critical to RCS processes are routed to the appropriate processes.<br><br>**Example:** When an RNCS/LIONN receives an Emergency Alert Message (EAM), Event Manager is notified of the EAM and passes an "EAM event" on to the MMMserver process on the DNCS. By notifying Event Manager, all appropriate DHCTs those deployed in the central site as well as those deployed in remote sites receive the EAM. |
| hctmConfig | **Home Communications Terminal (HCTM) Configuration** Exchanges and periodically transmits user-to-network configuration (UNconfig) information to DHCTs.<br><br>UNconfig information is configuration information that is exchanged between the DHCT as the user (U) and the network (N). This information tells DHCTs where to find system information, program information, and so on. |
| hctmInd | **HCTM Indications** Handles the periodic UNConfigIndications that were previously part of the hctmConfig process. |
| hctmMac | **HCTM Media Access Control (MAC)** Verifies connections and disconnections of DHCTs and modulators; associates an Internet protocol (IP) address with each DHCT. |
| hctmProvision | **HCTM Provisioning** Ensures that setup information is in the database and available for DHCTs |
| idm | **Inventory and Directory Manager** Provides a repository for public key certificates for DHCTs and service providers. |
| ippvManager | **Impulse-Pay-Per-View (IPPV) Manager** Polls DHCTs for PPV information for those orders made using the remote control for the television. |
| ippvReceiver | **IPPV Receiver** Receives purchased event information from the DHCT, then forwards or returns this information to the billing system upon request. |
| loadDhctServer | **Web Interface Proxy** Provides an interface to the DNCS using a SOAP/XML web service. It receives the mini PIMS file from DTAOM, parses the mini PIMS file and stores the relevant data in the DNCS database, and also flags the CAM processes to regenerate the staging EMMs. |
| logManager | **Logging Manager** Enables the configuration of logging levels on a DNCS and RNCS/LIONN through the Logging Summary window on the DNCS. |
| mgrUIServer | **GUI Server Manager** This process operates as a proxy for messages going to/from the DNCS Presentation Layer (that is, the Graphical User Interface [GUI]) and Web User Interface (WUI) screens. It receives |

| | |
|---|---|
| | XML/Soap messages and transmits those message on via RPC IPC to other process layer components, which will, in turn, operate on those messages. |
| MMMServer | **Multi-Media Message Server** Processes Emergency Alert Messages (EAMs) and dispatches them to the targeted geographic area, based on the Federal Information Processing System (FIPS) code information contained in the message.<br>An EAM may contain text, audio, and force-tune information. |
| ocdlManager | **OCAP Common Download Manager** Manages carousel setup and images the OCAP CDL. |
| osm | **Operating System (OS) Manager** Allows you to load image files into the BFS that can then be distributed to DHCTs.<br>**Example:** OS images, resident application images, and other application images. |
| oxaitMgr | **OCAP (tru2way) XAIT Manager** Provides XAIT information to tru2way devices. Only available if the OCAP (tru2way) license is enabled. |
| pasm | **Pre-Allocated Session Resource Manager (PASM)** Indicates the state of communication between the DNCS and session resource managers. |
| PassThru | **PassThru** Sends pass-thru Digital Storage Media Command and Control (DSM-CC) messages to DHCTs. |
| qamManager | **Quadrature Amplitude Modulation (QAM) Manager** Delivers setup information to QAM, MQAM, and GQAM modulators. |
| qpskManager | **Quaternary Phase-Shift Keyed (QPSK) Manager** Delivers setup information to QPSK modulators; also delivers out-of-band SI data to DHCTs. |
| pkeManager | **PowerKEY Element Manager** Manages and maintains requests/reservations for stream/session encryption on our Netcrypt devices. |
| ResAppServer | **Resident Application Server** Provides miscellaneous services for the SARA Server, including access to data in the DNCS database. |
| saManager | **Service Application Manager (more commonly referred to as SAM)** Defines a service, which is the combination of an application (WatchTV, music, PPV, and so forth) and the application parameters (source number, URL, and so forth). |
| sgManager | **Service Group Manager** Provides information about service groups to VOD servers and DHCTs.<br>The following information is processed by the sgManager:<br>▪Places data onto a BFS carousel that a DHCT can access to automatically determine to which service group the DHCT belongs.<br>▪Provides data to servers through either SNMP or a flat file; in either case, a server can use the data to determine which modulator the server should use to send data to a specific service group. |
| siManager | **System Information (SI) Manager** Facilitates the distribution of system information.<br>The following types of information are distributed by the siManager: |

| | |
|---|---|
| | ▪SI tuning table information to QAM modulators, along with the QAM Manager process.<br>▪Out-of-band SI information to QPSK modulators, along with the QPSK Manager process. |
| sseManager | **Server Site Entitlement Manager** Retrieves SA/Cisco entitlement information and provides it to a third-party application (Client-Side Entitlement Manager) in a format required by this application. The application then matches the information to its entitlement information so authorized CPEs can view the service provided by the given application (for example, VOD). |

### Working States of DNCS Processes

A colored circle in the **State** column indicates the working state of a particular process as described in the following list:

- Green The process as a whole is running, although a subprocess may be paused.
- Yellow The process has not finished starting up or shutting down, or is waiting on a subprocess to finish starting up or shutting down.
- Red The process has stopped or did not start.

After the DNCS is up and running, all of these processes should have a **green** working state. Some processes restart automatically in response to an error. If this happens, the status indicator cycles through red, yellow, and green as the process shuts itself down, restarts itself, and then becomes active.

However, if a process remains in a red or yellow working state, this indicates that the process is not functioning properly. Click here for instructions on the corrective action to take.

**WARNING:** Do **NOT** attempt to start or stop a DNCS process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.

## Monitoring DNCS Processes

You can monitor all of the major DNCS processes by clicking the **Control** button in the DNCS area of the DNCS Administrative Console Status window to open the DNCS Control window. The DNCS Control window provides a list of all the major processes on the DNCS workstation, along with the working state of each.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

We recommend that you leave the DNCS Control window open and visible at all times to help you monitor your system. For more information on monitoring DNCS processes, click here.

### Descriptions of DNCS Processes

The following table describes each of the processes listed on the DNCS Control window.

| Process | Description |
|---|---|
| alarmCollector | **Alarm Collector** — Retrieves alarms from all network elements, and then sends the alarms to the Spectrum NMS.<br><br>This process shows only when the Spectrum Network Management System (NMS) is used.<br><br>For more information about the DBDS Alarm Management System, contact your the representative who handles your account. |
| bfsRemote | **Broadcast File System (BFS) Remote** — Manages the processes (dataPump processes) that continuously transmit BFS data.<br><br>The BFS facilitates delivery of information to DHCTs. |
| bfsServer | **BFS Server** — Manages the addition and deletion of files from the BFS. |
| bigManager | **Broadband Integrated Gateway (BIG) Manager** — Monitors and manages the operation of BIGs, including establishing sessions and allocating MPEG program-specific information (PSI). |
| bossDiagnosticsServer | **Business Operations Support System (BOSS) Diagnostics Server** — Acts as an SNMP proxy agent between the billing system and DHCTs by going through the DNCS to retrieve information from DHCTs for the billing system. |
| bossServer | **BOSS Server** — Communicates with the billing system, the DHCT Manager, and the DNCS Administrative Console. |
| bsm | **Broadcast Segment Manager** — Receives notification from the SI Manager when broadcast sources start, and then forwards the notifications to the Conditional Access (CA) system. |
| caaServer | CA Authority (CAA) Server — Creates and sends the CAA and entitlement authorization (EA) entitlement management messages (EMMs) required for staging DHCTs.<br><br>**Note:** The caaServer process was called the **Caa** process in system releases prior to 1.4. |
| camAm | **CA Manager (CAM) Authorization Manager** — Creates EMMs for security elements to authorize DHCTs to receive secure events. |
| camAuditor | **CAM Auditor** — Refreshes or creates EMMs on DHCTs, which allow the subscriber to view secure events. |
| camEx | **CAM Exclusive Sessions** — Provides conditional access for VOD sessions; generates interactive session keys (ISKs) for each session and ISK EMMs for delivery to the QAM modulators and DHCTs; generates entitlement control messages (ECMs) for the QAM modulators so they can encrypt these sessions. |
| camFastRefresh | **CAM Fast Refresh** — Queries the database for EMMs, puts the EMMs in files, and puts the files on the BFS (files are refreshed periodically when EMMs are changed in the system); sends staging EMMs over inband BFS to DHCTs that are candidates for the Fast Refresh List. |
| camPsm | **CAM Program Segment Manager (PSM)** — Sends PPV and CA Time-of-Day global broadcast authenticated messages (GBAMs); inserts CA information, including ECMs into the program segment at the QAM modulator level. |

| | |
|---|---|
| camTEDChecker | **CAM Transaction Encryption Device (TED) Checker** — indicates whether or not the TED is running as follows:<br>▪Green — the TED is in service and the keys have been initialized<br>▪Yellow — the TED software is running, but the keys have not been initialized<br>▪Red — the TED software is not running<br>For more information about the TED, refer to Transaction Encryption Device FX Server Installation and Operation Guide (part number 736138). To obtain a copy of this guide, see Printed Resources.<br>This process was first introduced in SR 2.1.1. |
| CCardServer | **CableCARD Server** — Creates and maintains the PowerKEY CableCARD Module BFS file of CableCARD Module/host pair authorizations; also provides global configuration information to the CableCARD Module population.<br>This process was first introduced in SR 2.2 and SR 3.2. |
| dbSync | **Database Synchronizer** — Ensures that databases on the DNCS and on each RNCS/LIONN are correctly updated with the most recent information. |
| dncsSnmpAgent | **DNCS Simple Network Management Protocol (SNMP) Agent** - Retrieves alarms from all network elements, and then sends the alarms to our DBDS Alarm Management System (NMS) or to a third-party NMS.<br>For more information about the DBDS Alarm Management System, contact the representative who handles your account. |
| dncs-snmpd-big<br>dncs-snmpd-qam<br>dncs-snmpd-qpsk | **DNCS SNMP** — Ensures that network elements that are not SNMP-compliant (BIGs and QAM modulators, MQAM modulators and QPSK modulators) can communicate with the Spectrum NMS through SNMP protocol.<br>In other words, the dncs-snmp acts as a proxy agent for each of these elements. |
| drm | **Digital Resource Manager** — Manages the allocation of DBDS resources for setting up sessions.<br>The drm process was part of the dsm process in system releases prior to 1.4. |
| dsm | **Digital Session Manager** — Manages digital video sessions (broadcast and exclusive) on the DNCS.<br>When using Overlay technology, the DSM manages sessions for only our DHCTs. |
| EARS | **Emergency Alert The Emergency Alert Receiver Server** — Monitors a designated port on the DNCS to receive Emergency Alert Messages (EAMs). After receiving an EAM, EARS processes it differently, depending upon whether EARS is operating in an RCS site or in a non-RCS site. |
| emmDistributor | **EMM Distributor** — Distributes EMMs to DHCTs over the out-of-band path. |
| eventManager | **Event Manager** — Ensures that events critical to RCS processes are routed to the appropriate processes.<br>**Example:** When an RNCS/LIONN receives an Emergency Alert Message (EAM), Event Manager is notified of the EAM and passes an "EAM event" |

| | |
|---|---|
| | on to the MMMserver process on the DNCS. By notifying Event Manager, all appropriate DHCTs—those deployed in the central site as well as those deployed in remote sites—receive the EAM. |
| hctmConfig | **Home Communications Terminal (HCTM) Configuration** — Exchanges and periodically transmits user-to-network configuration (UNconfig) information to DHCTs.<br><br>UNconfig information is configuration information that is exchanged between the DHCT as the user (U) and the network (N). This information tells DHCTs where to find system information, program information, and so on. |
| hctmInd | **HCTM Indications** — Handles the periodic UNConfigIndications that were previously part of the hctmConfig process. |
| hctmMac | **HCTM Media Access Control (MAC)** — Verifies connections and disconnections of DHCTs and modulators; associates an Internet protocol (IP) address with each DHCT. |
| hctmProvision | **HCTM Provisioning** — Ensures that setup information is in the database and available for DHCTs |
| idm | **Inventory and Directory Manager** — Provides a repository for public key certificates for DHCTs and service providers. |
| ippvManager | **Impulse-Pay-Per-View (IPPV) Manager** — Polls DHCTs for PPV information for those orders made using the remote control for the television. |
| ippvReceiver | **IPPV Receiver** — Receives purchased event information from the DHCT, then forwards or returns this information to the billing system upon request. |
| loadDhctServer | **Web Interface Proxy** — Provides an interface to the DNCS using a SOAP/XML web service. It receives the mini PIMS file from DTAOM, parses the mini PIMS file and stores the relevant data in the DNCS database, and also flags the CAM processes to regenerate the staging EMMs. |
| logManager | **Logging Manager** — Enables the configuration of logging levels on a DNCS and RNCS/LIONN through the Logging Summary window on the DNCS. |
| mgrUIServer | **GUI Server Manager** — This process operates as a proxy for messages going to/from the DNCS Presentation Layer (that is, the Graphical User Interface [GUI]) and Web User Interface (WUI) screens. It receives XML/Soap messages and transmits those message on via RPC IPC to other process layer components, which will, in turn, operate on those messages. |
| MMMServer | **Multi-Media Message Server** — Processes Emergency Alert Messages (EAMs) and dispatches them to the targeted geographic area, based on the Federal Information Processing System (FIPS) code information contained in the message.<br><br>An EAM may contain text, audio, and force-tune information. |
| ocdlManager | **OCAP Common Download Manager** — Manages carousel setup and images the OCAP CDL. |
| osm | **Operating System (OS) Manager** — Allows you to load image files into the BFS that can then be distributed to DHCTs.<br><br>**Example:** OS images, resident application images, and other application images. |

| | |
|---|---|
| oxaitMgr | **OCAP (tru2way) XAIT Manager** — Provides XAIT information to tru2way devices. Only available if the OCAP (tru2way) license is enabled. |
| pasm | **Pre-Allocated Session Resource Manager (PASM)** — Indicates the state of communication between the DNCS and session resource managers. |
| PassThru | **PassThru** — Sends pass-thru Digital Storage Media Command and Control (DSM-CC) messages to DHCTs. |
| qamManager | **Quadrature Amplitude Modulation (QAM) Manager** — Delivers setup information to QAM, MQAM, and GQAM modulators. |
| qpskManager | **Quaternary Phase-Shift Keyed (QPSK) Manager** — Delivers setup information to QPSK modulators; also delivers out-of-band SI data to DHCTs. |
| pkeManager | **PowerKEY Element Manager** — Manages and maintains requests/reservations for stream/session encryption on our Netcrypt devices. |
| ResAppServer | **Resident Application Server** — Provides miscellaneous services for the SARA Server, including access to data in the DNCS database. |
| saManager | **Service Application Manager (more commonly referred to as SAM)** — Defines a service, which is the combination of an application (WatchTV, music, PPV, and so forth) and the application parameters (source number, URL, and so forth). |
| sgManager | **Service Group Manager** — Provides information about service groups to VOD servers and DHCTs.<br>The following information is processed by the sgManager:<br>▪Places data onto a BFS carousel that a DHCT can access to automatically determine to which service group the DHCT belongs.<br>▪Provides data to servers through either SNMP or a flat file; in either case, a server can use the data to determine which modulator the server should use to send data to a specific service group. |
| siManager | **System Information (SI) Manager** — Facilitates the distribution of system information.<br>The following types of information are distributed by the siManager:<br>▪SI tuning table information to QAM modulators, along with the QAM Manager process.<br>▪Out-of-band SI information to QPSK modulators, along with the QPSK Manager process. |
| sseManager | **Server Site Entitlement Manager** — Retrieves SA/Cisco entitlement information and provides it to a third-party application (Client-Side Entitlement Manager) in a format required by this application. The application then matches the information to its entitlement information so authorized CPEs can view the service provided by the given application (for example, VOD). |

# DNCS Processes

## Monitoring DNCS Processes

You can monitor all of the major DNCS processes by clicking the **Control** button in the DNCS area of the DNCS Administrative Console Status window to open the DNCS Control window. The DNCS Control window provides a list of all the major processes on the DNCS workstation, along with the working state of each.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

We recommend that you leave the DNCS Control window open and visible at all times to help you monitor your system. For more information on monitoring DNCS processes, click here.

### Descriptions of DNCS Processes

The following table describes each of the processes listed on the DNCS Control window.

| Process | Description |
|---|---|
| alarmCollector | **Alarm Collector** — Retrieves alarms from all network elements, and then sends the alarms to the Spectrum NMS.<br>This process shows only when the Spectrum Network Management System (NMS) is used.<br>For more information about the DBDS Alarm Management System, contact your the representative who handles your account. |
| bfsRemote | **Broadcast File System (BFS) Remote** — Manages the processes (dataPump processes) that continuously transmit BFS data.<br>The BFS facilitates delivery of information to DHCTs. |
| bfsServer | **BFS Server** — Manages the addition and deletion of files from the BFS. |
| bigManager | **Broadband Integrated Gateway (BIG) Manager** — Monitors and manages the operation of BIGs, including establishing sessions and allocating MPEG program-specific information (PSI). |
| bossDiagnosticsServer | **Business Operations Support System (BOSS) Diagnostics Server** — Acts as an SNMP proxy agent between the billing system and DHCTs by going through the DNCS to retrieve information from DHCTs for the billing system. |
| bossServer | **BOSS Server** — Communicates with the billing system, the DHCT Manager, and the DNCS Administrative Console. |
| bsm | **Broadcast Segment Manager** — Receives notification from the SI Manager when broadcast sources start, and then forwards the notifications to the Conditional Access (CA) system. |
| caaServer | CA Authority (CAA) Server — Creates and sends the CAA and entitlement authorization (EA) entitlement management messages (EMMs) required for staging DHCTs.<br>**Note:** The caaServer process was called the **Caa** process in system releases prior to 1.4. |
| camAm | **CA Manager (CAM) Authorization Manager** — Creates EMMs for security elements to authorize DHCTs to receive secure events. |
| camAuditor | **CAM Auditor** — Refreshes or creates EMMs on DHCTs, which allow the |

| | |
|---|---|
| | subscriber to view secure events. |
| camEx | **CAM Exclusive Sessions** — Provides conditional access for VOD sessions; generates interactive session keys (ISKs) for each session and ISK EMMs for delivery to the QAM modulators and DHCTs; generates entitlement control messages (ECMs) for the QAM modulators so they can encrypt these sessions. |
| camFastRefresh | **CAM Fast Refresh** — Queries the database for EMMs, puts the EMMs in files, and puts the files on the BFS (files are refreshed periodically when EMMs are changed in the system); sends staging EMMs over inband BFS to DHCTs that are candidates for the Fast Refresh List. |
| camPsm | **CAM Program Segment Manager (PSM)** — Sends PPV and CA Time-of-Day global broadcast authenticated messages (GBAMs); inserts CA information, including ECMs into the program segment at the QAM modulator level. |
| camTEDChecker | **CAM Transaction Encryption Device (TED) Checker** — indicates whether or not the TED is running as follows:<br>▪Green — the TED is in service and the keys have been initialized<br>▪Yellow — the TED software is running, but the keys have not been initialized<br>▪Red — the TED software is not running<br>For more information about the TED, refer to Transaction Encryption Device FX Server Installation and Operation Guide (part number 736138). To obtain a copy of this guide, see Printed Resources.<br>This process was first introduced in SR 2.1.1. |
| CCardServer | **CableCARD Server** — Creates and maintains the PowerKEY CableCARD Module BFS file of CableCARD Module/host pair authorizations; also provides global configuration information to the CableCARD Module population.<br>This process was first introduced in SR 2.2 and SR 3.2. |
| dbSync | **Database Synchronizer** — Ensures that databases on the DNCS and on each RNCS/LIONN are correctly updated with the most recent information. |
| dncsSnmpAgent | **DNCS Simple Network Management Protocol (SNMP) Agent** - Retrieves alarms from all network elements, and then sends the alarms to our DBDS Alarm Management System (NMS) or to a third-party NMS.<br>For more information about the DBDS Alarm Management System, contact the representative who handles your account. |
| dncs-snmpd-big<br>dncs-snmpd-qam<br>dncs-snmpd-qpsk | **DNCS SNMP** — Ensures that network elements that are not SNMP-compliant (BIGs and QAM modulators, MQAM modulators and QPSK modulators) can communicate with the Spectrum NMS through SNMP protocol.<br>In other words, the dncs-snmp acts as a proxy agent for each of these elements. |
| drm | **Digital Resource Manager** — Manages the allocation of DBDS resources for setting up sessions.<br>The drm process was part of the dsm process in system releases prior to 1.4. |

| | |
|---|---|
| dsm | **Digital Session Manager** — Manages digital video sessions (broadcast and exclusive) on the DNCS.<br><br>When using Overlay technology, the DSM manages sessions for only our DHCTs. |
| EARS | **Emergency Alert The Emergency Alert Receiver Server** — Monitors a designated port on the DNCS to receive Emergency Alert Messages (EAMs). After receiving an EAM, EARS processes it differently, depending upon whether EARS is operating in an RCS site or in a non-RCS site. |
| emmDistributor | **EMM Distributor** — Distributes EMMs to DHCTs over the out-of-band path. |
| eventManager | **Event Manager** — Ensures that events critical to RCS processes are routed to the appropriate processes.<br><br>**Example:** When an RNCS/LIONN receives an Emergency Alert Message (EAM), Event Manager is notified of the EAM and passes an "EAM event" on to the MMMserver process on the DNCS. By notifying Event Manager, all appropriate DHCTs—those deployed in the central site as well as those deployed in remote sites—receive the EAM. |
| hctmConfig | **Home Communications Terminal (HCTM) Configuration** — Exchanges and periodically transmits user-to-network configuration (UNconfig) information to DHCTs.<br><br>UNconfig information is configuration information that is exchanged between the DHCT as the user (U) and the network (N). This information tells DHCTs where to find system information, program information, and so on. |
| hctmInd | **HCTM Indications** — Handles the periodic UNConfigIndications that were previously part of the hctmConfig process. |
| hctmMac | **HCTM Media Access Control (MAC)** — Verifies connections and disconnections of DHCTs and modulators; associates an Internet protocol (IP) address with each DHCT. |
| hctmProvision | **HCTM Provisioning** — Ensures that setup information is in the database and available for DHCTs |
| idm | **Inventory and Directory Manager** — Provides a repository for public key certificates for DHCTs and service providers. |
| ippvManager | **Impulse-Pay-Per-View (IPPV) Manager** — Polls DHCTs for PPV information for those orders made using the remote control for the television. |
| ippvReceiver | **IPPV Receiver** — Receives purchased event information from the DHCT, then forwards or returns this information to the billing system upon request. |
| loadDhctServer | **Web Interface Proxy** — Provides an interface to the DNCS using a SOAP/XML web service. It receives the mini PIMS file from DTAOM, parses the mini PIMS file and stores the relevant data in the DNCS database, and also flags the CAM processes to regenerate the staging EMMs. |
| logManager | **Logging Manager** — Enables the configuration of logging levels on a DNCS and RNCS/LIONN through the Logging Summary window on the DNCS. |
| mgrUIServer | **GUI Server Manager** — This process operates as a proxy for messages going to/from the DNCS Presentation Layer (that is, the Graphical User Interface [GUI]) and Web User Interface (WUI) screens. It receives |

| | |
|---|---|
| | XML/Soap messages and transmits those message on via RPC IPC to other process layer components, which will, in turn, operate on those messages. |
| MMMServer | **Multi-Media Message Server** — Processes Emergency Alert Messages (EAMs) and dispatches them to the targeted geographic area, based on the Federal Information Processing System (FIPS) code information contained in the message.<br><br>An EAM may contain text, audio, and force-tune information. |
| ocdlManager | **OCAP Common Download Manager** — Manages carousel setup and images the OCAP CDL. |
| osm | **Operating System (OS) Manager** — Allows you to load image files into the BFS that can then be distributed to DHCTs.<br><br>**Example:** OS images, resident application images, and other application images. |
| oxaitMgr | **OCAP (tru2way) XAIT Manager** — Provides XAIT information to tru2way devices. Only available if the OCAP (tru2way) license is enabled. |
| pasm | **Pre-Allocated Session Resource Manager (PASM)** — Indicates the state of communication between the DNCS and session resource managers. |
| PassThru | **PassThru** — Sends pass-thru Digital Storage Media Command and Control (DSM-CC) messages to DHCTs. |
| qamManager | **Quadrature Amplitude Modulation (QAM) Manager** — Delivers setup information to QAM, MQAM, and GQAM modulators. |
| qpskManager | **Quaternary Phase-Shift Keyed (QPSK) Manager** — Delivers setup information to QPSK modulators; also delivers out-of-band SI data to DHCTs. |
| pkeManager | **PowerKEY Element Manager** — Manages and maintains requests/reservations for stream/session encryption on our Netcrypt devices. |
| ResAppServer | **Resident Application Server** — Provides miscellaneous services for the SARA Server, including access to data in the DNCS database. |
| saManager | **Service Application Manager (more commonly referred to as SAM)** — Defines a service, which is the combination of an application (WatchTV, music, PPV, and so forth) and the application parameters (source number, URL, and so forth). |
| sgManager | **Service Group Manager** — Provides information about service groups to VOD servers and DHCTs.<br><br>The following information is processed by the sgManager:<br><br>▪Places data onto a BFS carousel that a DHCT can access to automatically determine to which service group the DHCT belongs.<br><br>▪Provides data to servers through either SNMP or a flat file; in either case, a server can use the data to determine which modulator the server should use to send data to a specific service group. |
| siManager | **System Information (SI) Manager** — Facilitates the distribution of system information.<br><br>The following types of information are distributed by the siManager: |

| | |
|---|---|
| | ▪SI tuning table information to QAM modulators, along with the QAM Manager process.<br>▪Out-of-band SI information to QPSK modulators, along with the QPSK Manager process. |
| sseManager | **Server Site Entitlement Manager** — Retrieves SA/Cisco entitlement information and provides it to a third-party application (Client-Side Entitlement Manager) in a format required by this application. The application then matches the information to its entitlement information so authorized CPEs can view the service provided by the given application (for example, VOD). |

### Working States of DNCS Processes

A colored circle in the **State** column indicates the working state of a particular process as described in the following list:

- Green — The process as a whole is running, although a subprocess may be paused.
- Yellow — The process has not finished starting up or shutting down, or is waiting on a subprocess to finish starting up or shutting down.
- Red — The process has stopped or did not start.

After the DNCS is up and running, all of these processes should have a **green** working state. Some processes restart automatically in response to an error. If this happens, the status indicator cycles through red, yellow, and green as the process shuts itself down, restarts itself, and then becomes active.

However, if a process remains in a red or yellow working state, this indicates that the process is not functioning properly. Click here for instructions on the corrective action to take.

**WARNING:** Do **NOT** attempt to start or stop a DNCS process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.

## Stopping DNCS Processes

Complete these steps to stop all of the processes on the DNCS.

**Warning:** When you stop DNCS processes, two-way communication also stops in the DBDS. You will not be able to offer any PPV, VOD, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage DHCTs or update modulator/demodulator code.

**Important:** If you are restarting the DNCS, complete this procedure only after you stop the network management system and the SARA Server processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click the **Control** button in the DNCS area. The DNCS Control (or Monitor) window opens with a list of all the DNCS processes and their working states. A **green** working state indicates that a process is running.

   **Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

2. Press the middle mouse button and then select **DNCS Stop**. A confirmation message appears.
3. Click **Yes**.
4. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**. The Dncs Control window appears.
5. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all DNCS processes.

   **Note:** The system updates the display periodically, or you can press **Enter** to force an update.

6. When the **Curr Stt** (Current State) field of the Dncs Control window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the Dncs Control window.

   **Important:** Do not go to the next step until all processes are stopped.

7. Are you in the process of restarting the DNCS?
   - If **yes**, your next step is to restart all DNCS processes.
   - If **no**, you are finished with this procedure.

## Restarting DNCS Processes

After you stop all of the processes on the DNCS, complete these steps to restart them.

**Important:** You must restart the DNCS and its processes in the correct order. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click the **Control** button in the DNCS area. The DNCS Control window opens with a list of all the DNCS processes and their working states. A **red** state indicates that a process is not running.

   **Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

2. Use the mouse to place the cursor on any open area on the DNCS desktop, but not on the DNCS Administrative Console, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **DNCS Start**. On the DNCS Control window, all of the processes change to a **green** state, which indicates that they are running.

   **Note:** It may take several minutes before all processes show a green state. Do not go to the next step until all of the processes are in a green state.

4. Your next step is to restart all of the processes on the SARA Server.

# Dashboard

The DashBoard gives you an at-a-glance view of the health of your system. Graphs of key indicators provide real-time information that assist you in monitoring your system. To help you ensure the system performs as expected, troubleshooting assistance is provided for each key indicator.

## What do you want to do?

- Review the Dashboard Indicators that the DashBoard monitors
- Display Dashboard Indicators
- Troubleshoot with Dashboard Indicators

## Dashboard Indicators

The DashBoard provides a graph of each of the following key indicators. Each graph is displayed in a rolling 24-hour window (if 24 hours of data is available). The DashBoard begins collecting data as soon as the DNCS processes are started.

**Note:** For troubleshooting actions, see Troubleshoot with Dashboard Indicators.

- **DNCS Idle CPU %** - Shows the percentage of the CPU that is currently not being consumed.

  **Target:** 20% or less for a 15-minute period. If outside this target, take troubleshooting action.

- **DNCS Database Process CPU %** - Shows the percentage of the CPU that the DNCS database is currently consuming.

  **Target:** 30% or less for a 15-minute period. If outside this target, take troubleshooting action.

- **DNCS Process CPU %** - Shows the percentage of the CPU that DNCS processes are currently consuming.

  **Target:** 50% or less for a 15-minute period. If outside this target, take troubleshooting action.

- **Free Memory %** - Shows the percentage of total memory that is available for use.

  **Target:** Actual percentage will vary from system to system, but should show a fairly level trend from day to day. If the trend continues to rise over a period of days (indicting an upward trend), take troubleshooting action.

**Note:** To learn how to display each of these indicators, see Display Dashboard Indicators.

## Display Dashboard Indicators

**Quick Path: DNCS Administrative Console Status > DashBoard area > Launch**

Follow these instructions to view any of the DashBoard indicators:

1. From the DNCS Administrative Console Status, click the **Launch** button in the DashBoard area. The DashBoard window opens and displays a list of the indicators.

   **Note:** For a description of each indicator, see DashBoard Indicators.

2. To display a DashBoard indicator, click the **+** button to the left of the indicator. A graph opens and shows the status of the indicator being monitored. All graphs show the following data:
   - Each graph is displayed in a rolling 24-hour window (if 24 hours of data is available).
   - Time is shown along the X-axis in one-minute increments.
   - The **Page** tool appears beneath each graph. This tool shows the number of pages the graph spans and allows you to move through the pages of the graph to view all of the data.

3. Follow these instructions to move through the pages of the graph and display data from any time within the last 24 hours:
   - To move backward in time, click the **<** arrow.
   - To move forward in time, click the **>** arrow.
   - To move forward to the most recent data available, click the **>|** arrow.
   - To move backward to the oldest data available, click the **|<** arrow.
   - To move to other data, enter a number in the **Page** field and click **Go**.

   **Note:** For assistance troubleshooting, see Troubleshoot with DashBoard Indicators.

4. To close the DashBoard window, click **File > Close**.

**Related Topics**

- Troubleshoot with Dashboard Indicators

## Troubleshoot with Dashboard Indicators

**Quick Path: DNCS Administrative Console Status > DashBoard area > Launch > Troubleshoot**

This section provides troubleshooting assistance for DashBoard indicators that are outside of their target ranges.

### DNCS Idle CPU %

When this indicator shows 20% or less for a 15-minute period or more, take the following actions. Otherwise, the system is operating as expected.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Display the DashBoard indicator for **DNCS Process CPU %** and determine the status of this indicator:<br>▪If the DNCS Process CPU % is less than 50% over a 15-minute period, the system is functioning within normal operating levels and does not require further troubleshooting.<br>▪If the DNCS Process CPU % is more than 50% consistently over a 15-minute period, use the **prstat** command to identify the DNCS processes that contribute to the high utilization. Then check the DNCS Database Process CPU %.<br>**Note:** Refer to the UNIX man page (man prstat) for usage and options for this command. |

### DNCS Database Process CPU %

When this indicator shows 30% or greater consistently over a 15-minute period or more, contact Cisco Services. In other instances, use the following table to troubleshoot.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Use the **prstat** command to identify the DNCS processes that contribute to the high utilization.<br>**Note:** Refer to the main page for usage and options for this command. |

### DNCS Process CPU %

When this indicator shows 50% or greater for a 15-minute period or more, take the following actions. If they do not resolve the memory issue, contact Cisco Services.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running | Use the **prstat** command to identify the DNCS processes that contribute to the high utilization.<br>**Note:** Refer to the main page for usage and |

| | |
|---|---|
| ▪Insufficient CPU resources | options for this command. |

### Free Memory %

When this indicator shows an upward trend over a period of several days, take the following actions.

| Possible Causes | Check and Correct |
|---|---|
| ▪Memory leaking | Use the **prstat** command to identify the process or processes that contribute to the trend by manually recording the data over several days.<br><br>**Note:** Refer to the main page for usage and options for this command.<br><br>Check the absolute memory size of the processes. If any single process is using more than 250 Mbyte of memory, contact Cisco Services for assistance. |

### DNCS Idle CPU %

When this indicator shows 20% or less for a 15-minute period or more, take the following actions. Otherwise, the system is operating as expected.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Display the DashBoard indicator for **DNCS Process CPU %** and determine the status of this indicator:<br>▪If the DNCS Process CPU % is less than 50% over a 15-minute period, the system is functioning within normal operating levels and does not require further troubleshooting.<br>▪If the DNCS Process CPU % is more than 50% consistently over a 15-minute period, use the **prstat** command to identify the DNCS processes that contribute to the high utilization. Then check the DNCS Database Process CPU %.<br>**Note:** Refer to the UNIX man page (man prstat) for usage and options for this command. |

### DNCS Database Process CPU %

When this indicator shows 30% or greater consistently over a 15-minute period or more, contact Cisco Services. In other instances, use the following table to troubleshoot.

| Possible Causes | Check and Correct |
| --- | --- |
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Use the **prstat** command to identify the DNCS processes that contribute to the high utilization.<br>**Note:** Refer to the main page for usage and options for this command. |

### DNCS Process CPU %

When this indicator shows 50% or greater for a 15-minute period or more, take the following actions. If they do not resolve the memory issue, contact Cisco Services.

| Possible Causes | Check and Correct |
| --- | --- |
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Use the **prstat** command to identify the DNCS processes that contribute to the high utilization.<br>**Note:** Refer to the main page for usage and options for this command. |

## Troubleshoot with Dashboard Indicators

**Quick Path: DNCS Administrative Console Status > DashBoard area > Launch > Troubleshoot**

This section provides troubleshooting assistance for DashBoard indicators that are outside of their target ranges.

### DNCS Idle CPU %

When this indicator shows 20% or less for a 15-minute period or more, take the following actions. Otherwise, the system is operating as expected.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Display the DashBoard indicator for **DNCS Process CPU %** and determine the status of this indicator:<br>▪If the DNCS Process CPU % is less than 50% over a 15-minute period, the system is functioning within normal operating levels and does not require further troubleshooting.<br>▪If the DNCS Process CPU % is more than 50% consistently over a 15-minute period, use the **prstat** command to identify the DNCS processes that contribute to the high utilization. Then check the DNCS Database Process CPU %.<br>**Note:** Refer to the UNIX man page (man prstat) for usage and options for this command. |

### DNCS Database Process CPU %

When this indicator shows 30% or greater consistently over a 15-minute period or more, contact Cisco Services. In other instances, use the following table to troubleshoot.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running<br>▪Insufficient CPU resources | Use the **prstat** command to identify the DNCS processes that contribute to the high utilization.<br>**Note:** Refer to the main page for usage and options for this command. |

### DNCS Process CPU %

When this indicator shows 50% or greater for a 15-minute period or more, take the following actions. If they do not resolve the memory issue, contact Cisco Services.

| Possible Causes | Check and Correct |
|---|---|
| ▪A runaway process or processes<br>▪Too many processes are running | Use the **prstat** command to identify the DNCS processes that contribute to the high utilization. |

| | |
|---|---|
| ▪Insufficient CPU resources | **Note:** Refer to the main page for usage and options for this command. |

### Free Memory %

When this indicator shows an upward trend over a period of several days, take the following actions.

| Possible Causes | Check and Correct |
|---|---|
| ▪Memory leaking | Use the **prstat** command to identify the process or processes that contribute to the trend by manually recording the data over several days.<br><br>**Note:** Refer to the main page for usage and options for this command.<br><br>Check the absolute memory size of the processes. If any single process is using more than 250 Mbyte of memory, contact Cisco Services for assistance. |

# SARA Application Server Processes

## Monitoring Application Server Processes

You can monitor all of the major SARA Server processes by clicking the **Control** button in the AppServer area of the DNCS Administrative Console Status window to open the AppServer Control window.

The AppServer Control window provides a list of all the major processes on the SARA Server workstation, along with the working state of each. We recommend that you leave the AppServer Control window open and visible at all times to help you monitor your system.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

For assistance on monitoring SARA Application Server processes, refer to the Application Server 3.6 User Guide (part number 4028820). To obtain this guide, see Printed Resources.

# SARA Application Server Processes

## Monitoring Application Server Processes

You can monitor all of the major SARA Server processes by clicking the **Control** button in the AppServer area of the DNCS Administrative Console Status window to open the AppServer Control window.

The AppServer Control window provides a list of all the major processes on the SARA Server workstation, along with the working state of each. We recommend that you leave the AppServer Control window open and visible at all times to help you monitor your system.

**Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

For assistance on monitoring SARA Application Server processes, refer to the Application Server 3.6 User Guide (part number 4028820). To obtain this guide, see Printed Resources.

## Stopping Application Server Processes

Complete these steps to stop all of the processes on the SARA Server. If you are using an application server from a vendor other than us, stop your application server according to the vendor's instructions.

**Important:** If you are restarting the DNCS, complete this procedure only after you stop your network management system. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. Press the middle mouse button on the Application Server and select **App Serv Stop**.
2. From an xterm window on the Application Server, type **appControl** and then press **Enter**. The Applications Control window appears.
3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**. The system displays all Application Server processes.

   **Note:** The system updates the display periodically, or you can press **Enter** to force an update.

4. When the **Curr Stt** (Current State) field of the Applications Control window indicates that all of the Application Server processes have stopped, follow the on-screen instructions to close the Applications Control window.This takes approximately 2 minutes to complete.

   **Important:** Do not go to the next step until all processes are stopped.

5. Are you restarting the DNCS?
   - If **yes**, your next step is to stop all of the processes on the DNCS.
   - If **no**, you are finished with this procedure.

## Restarting Application Server Processes

Complete these steps to restart all of the processes on the SARA Server. If you are using an application server from a vendor other than us, restart your application server according to the vendor's instructions.

**Important:** If you are in the process of restarting the DNCS, complete this procedure only after you restart all the DNCS processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. Is the xterm window open on the SARA Server that shows the working states of all SARA Server processes?
   - If **yes**, go to step 6.
   - If **no**, go to step 2.
2. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.
3. Click the left mouse button and select **xterm**. An xterm window opens.
4. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
5. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. A list appears of all the SARA Server processes and shows their current working states.
6. Do all processes show **Curr Stt: running(2)**?
   - If **yes**, go to step 13.
   - If **no**, go to step 7.
7. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.
8. Click the left mouse button and select **App Serv Start**. The SARA Server begins to restart all of its processes. This takes approximately 2 minutes to complete.
9. Press **Enter** every few seconds to update the working states until all processes show **Curr Stt: running(2)**.
10. Type **x** and press **Enter** to return to the Applications Control main menu.
11. Type **x** and press **Enter** again to close both the Applications Control main menu and the second xterm window.
12. In the first xterm window, type **exit** and press **Enter** to close the first xterm window.
13. Are you in the process of restarting the DNCS?
    - If **yes**, your next step is to restart the network management system.
    - If **no**, you are finished with this procedure.

# Network Elements With Spectrum

## Monitoring Network Elements With Spectrum NMS

If you are using the Spectrum Network Management System (NMS), you can monitor most of the devices in your network by clicking the **Control** button in the NMS area of the DNCS Administrative Console Status window to open the Spectrum Control Panel window. Any changes that you make in the DNCS to the configuration of a network element are reflected automatically in the NMS.

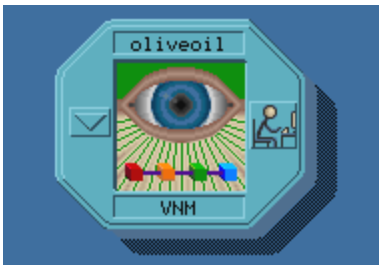
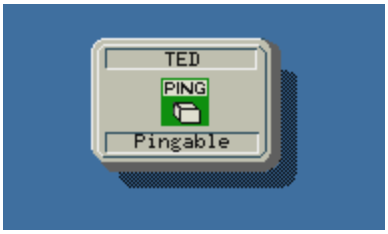
The Spectrum Control Panel window provides access to the Spectrum NMS. Some of the features available through the NMS include the following:

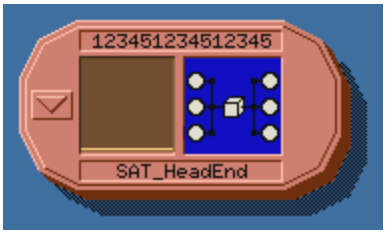
- An illustration (SpectroGRAPH) of all of your network elements, where they reside, and the working state of each
- An illustration of any alarm conditions existing in the network
- On-demand data retrieval from specific network elements
- Automatic polling to see if a specific device is available
- The Spectrum NMS contains its own Help documentation. If you have questions on how to use the Spectrum NMS beyond this discussion, click the **Help** button that appears in the upper right corner of the Spectrum Control Panel.

**Note:** We offer the DBDS Alarm Management System to help you monitor your network elements instead of using Spectrum. For more information, contact the representative who handles your account.

### SpectroGRAPH

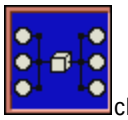
If you click the SpectroGRAPH button on the Spectrum Control Panel window, a picture of your network topology appears. The SpectroGRAPH shows all of your network elements, where they reside in the network, and the working state of each. The following table describes the kinds of graphics you might see in the SpectroGRAPH.

| Graphic | Description |
|---|---|
|  | The octagonal graphic with the eye in the center represents the DNCS.<br><br>Double-click the arrow  to see the topology view for the DNCS.<br><br>Double-click the user graphic  to see a user editor window inside of which attributes for the DNCS can be modified.<br><br>The color above the eye  changes to reflect the working state of the DNCS.<br><br>**Note:** The Spectrum NMS refers to the DNCS as the virtual network machine (VNM). |
|  | Rectangular graphics represent individual network elements, such as TEDs, BIGs, QAM modulators, IRTs, and QPSK modulators.<br><br>The name of the element appears at the top of the graphic.<br><br>The color in the center  changes to reflect the working state of the element. |




Twelve-sided graphics represent a group of connected elements, such as headends, hubs, and node sets.

Double-click the arrow  to see the elements and connections that make up the group.

The color on the right side of the graphic  changes to reflect the working state of the group of elements.


Diamond-shaped graphics represent SONET rings.

The color in the center of the graphic 

changes to reflect the working state of the ring.

### Working States of Network Elements

The colors of the graphics in the SpectroGRAPH provide information about the working state of the corresponding element as indicated in the following table.

| Graphic Color | Element Status |
|---|---|
| Green | Communicating with the element; element operating normally. |
| Yellow | Communicating with the element; minor alarm condition exists. |
| Orange | Communicating with the element; major alarm condition exists. |
| Red | Cannot communicate with the element. |
| Gray | Cannot communicate with the element due to an error on another network element. |
| Blue | Initializing; communication with the element not yet established. |

## Monitoring Network Elements With Spectrum NMS

If you are using the Spectrum Network Management System (NMS), you can monitor most of the devices in your network by clicking the **Control** button in the NMS area of the DNCS Administrative Console Status window to open the Spectrum Control Panel window. Any changes that you make in the DNCS to the configuration of a network element are reflected automatically in the NMS.

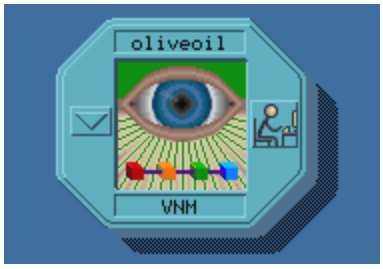
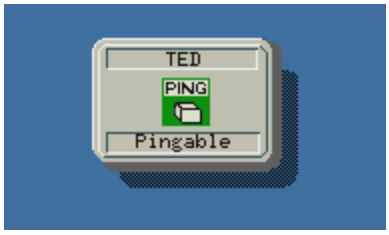
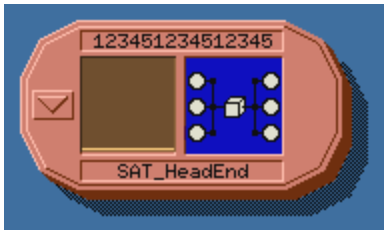
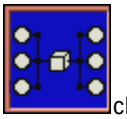
The Spectrum Control Panel window provides access to the Spectrum NMS. Some of the features available through the NMS include the following:

- An illustration (SpectroGRAPH) of all of your network elements, where they reside, and the working state of each
- An illustration of any alarm conditions existing in the network
- On-demand data retrieval from specific network elements
- Automatic polling to see if a specific device is available
- The Spectrum NMS contains its own Help documentation. If you have questions on how to use the Spectrum NMS beyond this discussion, click the **Help** button that appears in the upper right corner of the Spectrum Control Panel.

**Note:** We offer the DBDS Alarm Management System to help you monitor your network elements instead of using Spectrum. For more information, contact the representative who handles your account.

## SpectroGRAPH

If you click the SpectroGRAPH button on the Spectrum Control Panel window, a picture of your network topology appears. The SpectroGRAPH shows all of your network elements, where they reside in the network, and the working state of each. The following table describes the kinds of graphics you might see in the SpectroGRAPH.

| Graphic | Description |
|---|---|
|  | The octagonal graphic with the eye in the center represents the DNCS.<br><br>Double-click the arrow  to see the topology view for the DNCS.<br><br>Double-click the user graphic  to see a user editor window inside of which attributes for the DNCS can be modified.<br><br>The color above the eye  changes to reflect the working state of the DNCS.<br><br>**Note:** The Spectrum NMS refers to the DNCS as the virtual network machine (VNM). |
|  | Rectangular graphics represent individual network elements, such as TEDs, BIGs, QAM modulators, IRTs, and QPSK modulators.<br><br>The name of the element appears at the top of the graphic.<br><br>The color in the center  changes to reflect the working state of the element. |
|  | Twelve-sided graphics represent a group of connected elements, such as headends, hubs, and node sets.<br><br>Double-click the arrow  to see the elements and connections that make up the group.<br><br>The color on the right side of the graphic  changes to reflect the working state of the group of elements. |
|  | Diamond-shaped graphics represent SONET rings.<br><br>The color in the center of the graphic  changes to reflect the working state of the ring. |

# Network Elements With Spectrum

## Monitoring Network Elements With Spectrum NMS

If you are using the Spectrum Network Management System (NMS), you can monitor most of the devices in your network by clicking the **Control** button in the NMS area of the DNCS Administrative Console Status window to open the Spectrum Control Panel window. Any changes that you make in the DNCS to the configuration of a network element are reflected automatically in the NMS.

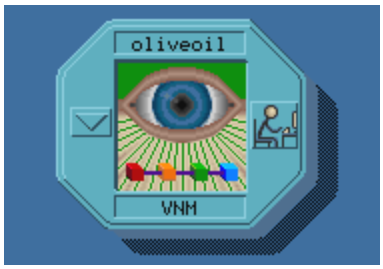
The Spectrum Control Panel window provides access to the Spectrum NMS. Some of the features available through the NMS include the following:

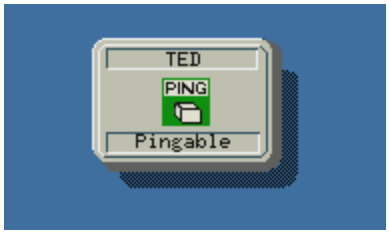
- An illustration (SpectroGRAPH) of all of your network elements, where they reside, and the working state of each
- An illustration of any alarm conditions existing in the network
- On-demand data retrieval from specific network elements
- Automatic polling to see if a specific device is available
- The Spectrum NMS contains its own Help documentation. If you have questions on how to use the Spectrum NMS beyond this discussion, click the **Help** button that appears in the upper right corner of the Spectrum Control Panel.

**Note:** We offer the DBDS Alarm Management System to help you monitor your network elements instead of using Spectrum. For more information, contact the representative who handles your account.

### SpectroGRAPH

If you click the SpectroGRAPH button on the Spectrum Control Panel window, a picture of your network topology appears. The SpectroGRAPH shows all of your network elements, where they reside in the network, and the working state of each. The following table describes the kinds of graphics you might see in the SpectroGRAPH.

| Graphic | Description |
|---|---|
|  | The octagonal graphic with the eye in the center represents the DNCS.<br><br>Double-click the arrow  to see the topology view for the DNCS.<br><br>Double-click the user graphic  to see a user editor window inside of which attributes for the DNCS can be modified.<br><br>The color above the eye  changes to reflect the working state of the DNCS.<br><br>**Note:** The Spectrum NMS refers to the DNCS as the virtual network machine (VNM). |




Rectangular graphics represent individual network elements, such as TEDs, BIGs, QAM modulators, IRTs, and QPSK modulators.

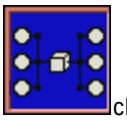
The name of the element appears at the top of the graphic.

The color in the center 

changes to reflect the working state of the element.


Twelve-sided graphics represent a group of connected elements, such as headends, hubs, and node sets.

Double-click the arrow  to see the elements and connections that make up the group.

The color on the right side of the graphic  changes to reflect the working state of the group of elements.


Diamond-shaped graphics represent SONET rings.

The color in the center of the graphic 

changes to reflect the working state of the ring.

### Working States of Network Elements

The colors of the graphics in the SpectroGRAPH provide information about the working state of the corresponding element as indicated in the following table.

| Graphic Color | Element Status |
|---|---|
| Green | Communicating with the element; element operating normally. |
| Yellow | Communicating with the element; minor alarm condition exists. |
| Orange | Communicating with the element; major alarm condition exists. |
| Red | Cannot communicate with the element. |
| Gray | Cannot communicate with the element due to an error on another network element. |
| Blue | Initializing; communication with the element not yet established. |

### Stopping Spectrum

Complete these steps to stop the Spectrum network management system (NMS). If you are using an NMS from a vendor other than us, stop your NMS according to the vendor's instructions.

**Important:** If you are restarting the DNCS, you must complete this procedure first. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click **Control** in the NMS area. The Select Host Machine window opens with the Spectrum Control Panel in the background.

   **Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

2. Click **OK**. The Select Host Machine window closes and the Spectrum Control Panel window is in the forefront.
3. Click **Stop SpectroSERVER**. A confirmation window opens.
4. Click **OK**. The system begins shutting down the Spectrum NMS. When finished, the **Status** field at the bottom of the Spectrum Control Panel changes to "Inactive."
5. Click **Exit**. A confirmation window opens.
6. Click **OK**. The Spectrum Control Panel window closes.
7. Are you restarting the DNCS?
   - If **yes**, go to step 8.
   - If **no**, you are finished with this procedure.
8. Your next step is to stop all of the processes on the SARA Server.

### Restarting Spectrum

Complete these steps to restart the Spectrum NMS. If you are using an NMS from a vendor other than us, restart your NMS according to the vendor's instructions.

**Important:** If you are in the process of restarting the DNCS, complete this procedure only after you restart the SARA Server processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click **Control** in the NMS area. The Select Host Machine window opens with the Spectrum Control Panel in the background.

   **Note:** Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

2. Click **OK**. The Select Host Machine window closes and the Spectrum Control Panel window is in the forefront.
3. Click **Start SpectroSERVER**. The system begins restarting the Spectrum NMS. When finished, the **Status** field at the bottom of the Spectrum Control Panel changes to "Running."
4. Click **Exit**. A confirmation window opens.
5. Click **OK**. The Spectrum Control Panel window closes.

# Session List Filter

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

The Session List Filter window shows the devices in your system that carry sessions. The window groups devices into lists organized by device type. For example, table-based QAM modulators are listed separately from regular QAM modulators. These organized lists make it easier for you to find specific devices for session monitoring.

After you display the sessions you are interested in, you can perform a variety of tasks, such as viewing details for a specific session or tearing down sessions.

## What do you want to do?

From the Session Filter window, you can perform any of the following tasks for the devices in your system that carry sessions:

- Use the Session Filter to display information about the sessions in your system
- Learn about Session data that the filter lists in the Session Summary window
- Tear down sessions on QAM modulators that carry content

## Use the Filter to Display Sessions

1.Click the **By Field** arrow and select one of the following options:

- **All** - Select to display all types of sessions.
- **Continuous feed sessions** - Select to display sessions used for broadcast or pay-per-view services
- **Exclusive sessions** - Select to display sessions used for video-on-demand (VOD) or anything-on-demand (xOD) services
- **Interactive** - Select to display sessions used for data, such as web browsing
- **Unlisted** - Select to display sessions used for sessions that are listed as "active" and may be functioning, but are not correctly configured. For example, any sessions with an invalid VASP association would display when this option is selected.

2.Click in the **By Value** field and select one of the following options:

- **All** - Select to display all of the following session states.
- **Active** - Select to display sessions that are currently running.
- **Pending** - Select to display sessions that have been set up but have not yet reached their start times.
- **Completed** - Select to display sessions that have successfully completed, or have been torn down by the user.

3.To view active sessions for a few specific devices, select the devices from the appropriate list, then complete one of the following steps:

**Important:** Select devices from only one list. Do not select devices from multiple lists.

- To select a group of adjacent devices, hold down the **Shift** key while selecting the first and last device in the group.
- To select devices that are not adjacent, hold down the **Ctrl** key while selecting each device.

4.Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the Session Summary window.

**Notes:**

- For information about the data displayed in the Session Summary window, see Session Data.
- You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: Session ID or Type. Clicking the same heading again displays the column in descending order.

## Session Summary

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Display Sessions]**

From the Session Summary window, you can display detailed information about a specific session, or tear down a session that is no longer needed.

## What do you want to do?

- Display details about a session
- Display details about a resource for a session
- Tear down sessions on QAM modulators that carry content

### Session Data

The Session Summary window provides the following information about the sessions you display:

1. **Session ID** - Lists the session ID that was assigned by the system administrator when the session was set up.
2. **Type** - Lists the following types of sessions:
   - **Continuous feed sessions** - Select to display sessions used for broadcast or pay-per-view services
   - **Exclusive sessions** - Select to display sessions used for video-on-demand (VOD) or anything-on-demand (xOD) services
   - **Interactive** - Select to display sessions used for data, such as web browsing
   - **Unlisted** - Select to display sessions used for sessions that are listed as "active" and may be functioning, but are not correctly configured. For example, any sessions with an invalid VASP association would display when this option is selected.
3. **State** - Lists the current state of the session. The DNCS lists the following states:
   - **Active** - Select to display sessions that are currently running.
   - **Pending** - Select to display sessions that have been set up but have not yet reached their start times.
   - **Completed** - Select to display sessions that have successfully completed, or have been torn down by the user.
4. **VASP Name** - Lists the Value Added Service Provider (VASP) that provides a service or functionality to elements of the session.
5. **Name** - Lists the name of the device that carries the session, as well as the frequency of the channel being used to send data from the device to the hubs on your system.
6. **Start Time** - Lists the time that the session began.
7. **Video Partial Encryption Percentage** - If the session is carried on a GoQAM modulator, the DNCS lists the percentage of the video portion of the session that is encrypted.
8. **Audio Partial Encryption Percentage** - If the session is carried on a GoQAM modulator,the DNCS lists the percentage of the audio portion of the session that is encrypted.
9. **Teardown Reason** - Lists the reason that the session has been torn down, for example, "user initiated."

### Display Details About a Session

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Filter > [Select Devices in List] > Display > [Select Session ID]**

After you have used the filter to display session data, complete these steps to display details about a session.

1. If you have not already done so, display the session for which you want to view details. For assistance, see Use the Filter to Display Sessions.
2. From the Session Summary window, click the **session ID** for the session that you want to examine in more detail. The Session Details window opens and displays the following information about the session:

- **MPEG Program Table Data**
  - **MPEG Program number of the session** - The MPEG program number given to this session when it was built.
  - **PMT PID** - The packet identifier (PID) that carries the program map table (PMT) for this program. The PMT gives details about a program and the elementary streams that comprise it.
  - **PCR PID** - The PID that carries the program clock reference (PCR) for this program so the DHCT can synchronize video and audio elementary streams.
  - **ECM PID** - The PID that carries the entitlement control message (ECM) for the program. ECMs enable an event to be encrypted for transmission to a DHCT and allow the event to be decrypted by the DHCT if the DHCT is properly provisioned. ECMs are generated by the DBDS whenever a package starts and its segments are active.

  **Note:** A PID distinguishes transport packets containing the data of one elementary stream from those carrying the data of other elementary streams.

- **Session Elements Data**
  - **Device Name** - the name of the element that carries the session
  - **Input Port** - the number of the port that receives the session
  - **Input TSID** - the identifier of the transport stream as it enters the device that carries this session
  - **Input Program Number** - the number of the program as it enters the device
  - **Output Port** - the number of the port where the session exits the device
  - **Output TSID** - the identifier of the transport stream as it exits the device that carries this session
  - **Output Program Number** - the number of the program as it exits the device
- **Session Resources Data**
  - **Resource Number** - The number assigned to the resource you selected.
  - **Resource Type** - The type of resources the session uses.
  - **State** - Lists the current state of the resource. The DNCS lists the following states:
    - Active resources for session that are currently running.
    - Pending resources for sessions that have been set up but have not yet reached their start times.
    - Completed resources for sessions that have successfully completed, or have been torn down by the user.

3. When you have finished examining the details, you can perform either of the following tasks:
   - To view details about a resource shown in the Session Details window, go to Display Details About a Resource.
   - To close the Session Details window, click **File > Close**.

### Display Details About a Resource

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Filter > [Select Devices in List] > Display > [Select Session ID] > [Select Resource Number]**

After you have used the filter to display session data, complete these steps to display details about a session.

1. If you have not already done so, display the details for the session whose resources you want to view. For assistance, see Display Details About a Session.
2. From the Session Details window, click the **resource number** for the resource that you want to examine in more detail. The Session Resource Details window opens and displays the following information about the resource you selected:

**Note:** The details that display vary according to the resource you select. The following lists all possible details in alphabetical order for easy reference.

- **Allocation Time** - A time stamp indicating when the session-setup request is sent to the DNCS.
- **ATM VCI** - The virtual circuit identifier of the ATM card in the BFS BIG. (Shown only for the ATM Connection resource.)
- **ATM VPI** - The virtual path identifier of the ATM card in the BFS BIG. The VPI identifies a bundle of virtual circuits that may be switched as a single unit. (Shown only for the ATM Connection resource.)
- **Audio Encryption** - The percentage of encryption applied to the session's audio stream. (This field appears only for sessions on GoQAM modulators.)
- **Bandwidth** - The amount of bandwidth used by the selected transport stream ID (TSID).
- **Direction** - The direction of the physical channel. A value of 1 indicates that the direction is downstream. Currently this is the only value for a physical channel resource.
- **Forward Error Correction** - The type of FEC used. The following lists all possible values:
  - 0 = FEC transmission system
  - 1 = FEC DAVIC (Digital Audio Visual Council)
- **Frequency** - The frequency (in Hz) that the physical channel uses.
- **Headend Flag** - The headend that transmits the session to the access network. A value of 1 indicates the headend named by the headend ID.
- **Headend NSAP** - The network service access point address of the headend transmitting the session.
- **Inner Coding Mode** - Per DSM-CC ISO/IEC 138-18-6, Generic coding of moving pictures and associated audio information -- Part 6: Extensions for DSM-CC, the inner coding mode always shows a fixed value of 15, indicating that trellis-coding is used.
- **Interleave Depth** - The level of interleaving used by the QAM modulator carrying this session. A value of 0 indicates a depth of 128:1.
- **Modulation Format** - The modulation used for this session. The following lists possible values.
  - 6 = QAM 16
  - 7 = QAM 32
  - 8 = QAM 64
  - 12 = QAM 128
  - 16 = QAM 256
- **Modulation Mode** - Per DSM-CC ISO/IEC 138-18-6, Generic coding of moving pictures and

associated audio information -- Part 6: Extensions for DSM-CC, the modulation mode always shows a value of 0, which indicates no modulation mode.

- **NSAP Address** - The network service access point address of the ATM connection. (Shown only for the ATM Connection resource.)
- **PCR PID** - The PID that carries the program clock reference (PCR) for this program so the DHCT can synchronize video and audio elementary streams.
- **PMT PID** - The packet identifier (PID) that carries the program map table (PMT) for this program. The PMT gives details about a program and the elementary streams that comprise it.
- **Program Number** - The number of the MPEG program that the session carries.
- **Rel Time** - A time stamp indicating when session resources are released by the DNCS.
- **Resource State** - The current state of the resource you selected. The following lists possible values.
  - Active = sessions that are currently running.
  - Completed = sessions that have successfully completed, or have been torn down by the user
  - Failed = sessions that have stopped running
- **Session ID** - The session identifier for the selected resource.
- **Split BIG Stream Mode** - Per DSM-CC ISO/IEC 138-18-6, Generic coding of moving pictures and associated audio information -- Part 6: Extensions for DSM-CC, the split BIG stream mode always shows a fixed value of 0.
- **Symbol Rate (Baud Rate)** - Per DSM-CC ISO/IEC 138-18-6, Generic coding of moving pictures and associated audio information -- Part 6: Extensions for DSM-CC, the symbol rate always shows a fixed value of 5,000,000.
- **Transmission System** - The type of system used to deliver the session. The following lists possible values:
  - 0 = unknown transmission system
  - 1 = Our Digital Video Broadcast system
  - 2 = General Instrument (Motorola) transmission system
- **TSID** - The number identifying the transport stream that carries the session.
- **Video Encryption** - The percentage of encryption applied to the session's video stream. (This field appears only for sessions on GoQAM modulators.)

3. Do you want to view details of another resource?
   - If **yes**, click Session Details from the navigation path at the top of the window. Then repeat step 2 to display the details of another resource.
   - If **no**, click **File > Close** to close the Resource Details window.

## Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

1. If you have not already done so, display the appropriate sessions. For assistance, refer to Use the Filter to Display Sessions.

2. When the list of sessions displays, use one of the following methods to select the sessions you would like to tear down:

   - To tear down specific sessions, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete.
   - To tear down all sessions, click **Select All Displayed Sessions**.

**Note:** If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.

3. Click **Tear Down**. The system tears down the sessions you selected and updates the status of all sessions.

4. Click **File > Close** to close the Session Data window.

5. Depending on your reason for tearing down the session, you may decide to complete one of the following tasks:

   - If you tore down the session in order to delete a QAM modulator, you can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind. For assistance, see Delete a Content QAM Modulator.
   - If you deleted the session in order to correct an unlisted, active session, restart the session. For assistance, see Restart a Session.

## Restart a Session

**Quick Path: DNCS Administrative Console > System Provisioning tab > Source > [Select Source for Session] > File > Source Definition > [Select Source Definition] > Start Session > [Follow Set Up Digital Source Definition Window Prompts]**

After you tear down a session, follow this procedure to restart it from the Set Up Digital Source Definition window. Tearing down and restarting a session is helpful in correcting unlisted, active sessions.

**Note:** Restarting a session from the Set Up Digital Source Definition window automatically opens the Define Session window with predefined values for most settings based on the data you used to set up the session. This method allows you to easily identify and change any incorrect information as you use the Define Session window to restart the session with correct parameters.

1. On the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **Source**. The Source List window opens.
3. Select the source for the session, click **File > Source Definition**. The Source Definition List opens for the source you selected.

   **Note:** You can find the source for a session by looking through the Source ID column to find the ID that corresponds to the session ID.

4. Select the source definition with the status of Tear Down and click **File > Open**. The Set Up Digital Source Definition window opens for the source definition you selected.
5. Click **Start Session**. The Define Session window opens.
6. If necessary, select the correct source type, and then click **Next**. The Session Setup window opens.
7. If necessary, select the correct input device, and then click **Next**. The Select Outputs window opens.
8. Select the modulator that will receive content from this source and click **Next**. The Wrap-Up window opens and displays settings and values for the device.

   **Note:** To select more than one modulator, hold down the **Ctrl** key on your keyboard as you click on each modulator.

9. Verify that the values shown are correct and click **Next**. The Save Source Definition window opens.

   **Note:** If any values are incorrect, change them.

10. Click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

# Monitoring DHCT Performance

You can monitor the DHCT performance by turning on the performance monitoring function. Monitoring this performance can help you in troubleshooting your system should the need arise.

The DHCT performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of DHCTs. When you activate the DHCT performance monitoring feature, the system records information in the following files:

- hctmcfgperfmon.csv
- hctmmacperfmon.csv
- hctmprovperfmon.csv

After performance monitoring is activated, the system checks these files every reporting cycle to see if any data information has changed. If so, the system updates the information.

**Important:** Before you can activate DHCT performance monitoring for the first time, you must create the **hctmpm.time** file in the /dvs/dncs/tmp/PerformanceMonitoring directory.

## What do you want to do?

- Create the hctmpm.time file
- Activate DHCT performance monitoring or modify the reporting interval
- De-activate DHCT performance monitoring
- Read DHCT performance report files

## Creating the hctmpm.time File

Before you can activate DHCT performance monitoring for the first time, you must create the **hctmpm.time** file in the /dvs/dncs/tmp/PerformanceMonitoring directory.

**WARNING:**

**Do not delete this file after you create it. Doing so could make future monitoring efforts difficult.**

**Note:** UNIX commands are case-sensitive.

1. Open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **print "0" > hctmpm.time** and press **Enter**. A prompt appears.

**Note:** The zero ("0") in the previous command indicates the number of seconds between reporting intervals. Any value that is 10 or less indicates that DHCT performance monitoring is turned off. Every three minutes (180 seconds), the DNCS checks to see if DHCT performance monitoring is turned on.

## Activating or Modifying DHCT Performance Monitoring

After you create the hctmpm.time file, you can complete these steps to activate DHCT performance monitoring. You can also use these steps to modify the reporting intervals.

**Note:** UNIX commands are case-sensitive.

1. Open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **vi hctmpm.time** and press **Enter**. The system opens the hctmpm.time file.
4. Replace the value in the top line with any number greater than 10 based on how many seconds you want the system to check for DHCT data transactions. For example, if you want the system to perform this check every 5 minutes, you would type **300**.

   **Note:** Any value of 10 or less de-activates DHCT performance monitoring.

5. Type **:wq** and press **Enter**. The system saves your change and closes the hctmpm.time file. A prompt appears.
6. Type **exit** and press **Enter**. The xterm window closes.

## De-Activating DHCT Performance Monitoring

Complete these steps to de-activate DHCT performance monitoring.

**Note:** UNIX commands are case-sensitive.

1. Open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **vi hctmpm.time** and press **Enter**. The system opens the hctmpm.time file.
4. Replace the value in the top line with any number that equals 10 or less.
5. Type **:wq** and press **Enter**. The system saves your change and closes the hctmpm.time file. A prompt appears.
6. Type **exit** and press **Enter**. The xterm window closes.

## Reading DHCT Performance Report Files

When you turn on the DHCT performance monitoring feature, the system records the number of certain types of data transactions in the following files:

- hctmcfgperfmon.csv
- hctmmacperfmon.csv
- hctmprovperfmon.csv

The fields in these files are separated by commas, hence the "csv" (comma-separated values) designation. Separating the fields by commas allows you to view this information in Microsoft Excel, if you prefer.

Each line in these files begins with a date/time stamp, which indicates when the information was gathered. The first line is a header that describes the content of the columns in the lines that appear below the header.

For example, the hctmcfgperfmon.csv file shows reported information in the following format:

```
04-30-2007 13:28:01,number of UN config receive requests,number of UN config request confirms,number of config input queue full detected

04-30-2007 13:28:31,33,0,0
```

The first line of the preceding example shows that DHCT performance monitoring was activated on 4-30-2007 at 13:28:01. The data being reported includes the following:

- Number of UN config receive requests
- Number of UN config request confirms
- Number of config input queue full detected

The second line shows that 30 seconds later, at 13:28:31, there were 33 UN config receive requests, zero UN config request confirms, and the config input queue was never detected as full during this reporting interval. While this data alone may not be a clear indication of trouble, data gathered and compared over time may help to assist in troubleshooting.

## Monitored DHCT Data Transactions

The DHCT performance monitoring feature reports on the following data transactions for the hctmConfig, hctmMac, and hctmProvision processes.

| Process | Monitored Transactions |
|---|---|
| hctmConfig | ▪Number of "UNConfig receive" requests<br>▪Number of "UNConfig request" confirms<br>▪Number of times the config input queue was detected as full |
| hctmMac | ▪Number of DAVIC connections made<br>▪Number of DAVIC connections lost<br>▪Number of "verify request" received<br>▪Number of "verify response sent"<br>▪Number of "verify response sent" errors<br>▪Number of "verify request received sent to provisioning"<br>▪Number of times hctmMac input queue was detected as full |
| hctmProvision | ▪Number of "verify request received by provisioning"<br>▪Number of "verify response sent"<br>▪Number of "verify response sent" errors |

This information is reported in the hctmcfgperfmon.csv, hctmmacperfmon.csv, and hctmprovperfmon.csv files, respectively.

# Monitoring VOD Performance

You can monitor VOD performance on your system by turning on the performance monitoring function. Monitoring this performance can help you in troubleshooting your system should the need arise. The VOD performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of an exclusive session. When you activate the VOD performance monitoring feature, the system records information in the following files:

- drmperfmon.csv
- dsmperfmon.csv
- qammgrperfmon.csv

After performance monitoring is activated, the system checks these files every reporting cycle to see if any data information has changed. If so, the system updates the information.

**Important:** Before you can activate VOD performance monitoring for the first time, you must create the **vodpm.time** file in the /dvs/dncs/tmp/PerformanceMonitoring directory.

## What do you want to do?

- Create the vodpm.time file
- Activate VOD performance monitoring or modify the reporting interval
- De-activate VOD performance monitoring
- Read VOD performance report files

## Creating the vodpm.time File

Before you can activate VOD performance monitoring for the first time, you must create the **vodpm.time** file in the /dvs/dncs/tmp/PerformanceMonitoring directory.

**WARNING:**

**Do not delete this file after you create it. Doing so could make future monitoring efforts difficult.**

Complete these steps to create the vodpm.time file.

**Note:** UNIX commands are case-sensitive.

1. Open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **print "0" > vodpm.time** and press **Enter**. A prompt appears.

**Note:** The zero ("0") in the previous command indicates the number of seconds between reporting intervals. Any value that is 10 or less indicates that VOD performance monitoring is turned off. Every three minutes (180 seconds), the DNCS checks to see if VOD performance monitoring is turned on.

## Activating or Modifying VOD Performance Monitoring

After you create the vodpm.time file, you can complete these steps to activate VOD performance monitoring. You can also use these steps to modify the reporting intervals.

**Note:** UNIX commands are case-sensitive.

1. Open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **vi vodpm.time** and press **Enter**. The system opens the vodpm.time file.
4. Replace the value in the top line with any number greater than 10 based on how many seconds you want the system to check for VOD data transactions. For example, if you want the system to perform this check every 5 minutes, you would type **300**.

   **Note:** Any value of 10 or less de-activates VOD performance monitoring.

5. Type **:wq** and press **Enter**. The system saves your change and closes the vodpm.time file. A prompt appears.
6. Type **exit** and press **Enter**. The xterm window closes.

## De-Activating VOD Performance Monitoring

Complete these steps to de-activate VOD performance monitoring.

**Note:** UNIX commands are case-sensitive.

1. Open an xterm window on the DNCS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **vi vodpm.time** and press **Enter**. The system opens the vodpm.time file.
4. Replace the value in the top line with any number that equals 10 or less.
5. Type **:wq** and press **Enter**. The system saves your change and closes the vodpm.time file. A prompt appears.
6. Type **exit** and press **Enter**. The xterm window closes.

## Reading VOD Performance Report Files

When you turn on the VOD performance monitoring feature, the system records the number of certain types of data transactions in the following files:

- drmperfmon.csv
- dsmperfmon.csv
- qammgrperfmon.csv

The fields in these files are separated by commas, hence the "csv" (comma-separated values) designation. Separating the fields by commas allows you to view this information in Microsoft Excel, if you prefer.

Each line in these files begins with a date/time stamp, which indicates when the information was gathered. The first line is a header that describes the content of the columns in the lines that appear below the header.

For example, the drmperfmon.csv file shows reported information in the following format:

```
04-30-2007 11:01:20,allocate resource request,allocate resource success,release resources requests,release resources successes

04-30-2007 11:01:50,80,49,10,10
```

The first line of the preceding example shows that VOD performance monitoring was activated on 4-30-2007 at 11:01:20. The data being reported includes the following:

- allocate resource requests
- allocate resource success
- release resources requests
- release resources successes

The second line shows that 30 seconds later, at 11:01:50, there were 80 allocate resource requests, 49 allocate resource successes, 10 release resources requests, and 10 release resources successes during this reporting interval. While this data alone may not be a clear indication of trouble, data gathered and compared over time may help to assist in troubleshooting.

## Monitored VOD Data Transactions

The VOD performance monitoring feature reports on the following data transactions for the drm, dsm, and qamManager processes.

| Process | Monitored Transactions |
|---|---|
| hctmConfig | ▪Number of "allocate resources" requests and successes<br>▪Number of "release resources" requests and successes |
| hctmMac | ▪Number of "session setup" requests and confirmations<br>▪Number of "add resource" requests and confirmations<br>▪Number of "release resource" requests and confirmations<br>▪Number of "session release" requests and confirmations |
| hctmProvision | ▪Number of "create session" requests and responses<br>▪Number of "delete session" requests and responses |

This information is reported in the drmperfmon.csv, dsmperfmon.csv, and qammgrperfmon.csv files, respectively.

# GUI Servers

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers**

The UI Server Managers window provides an at-a-glance status of the Managers that monitor UI Servers. UI Server Managers monitor groups of UI Servers. If a UI Server stops unexpectedly, its Manager automatically restarts the UI Server. From this window, you can also modify the Managers listed in it so that you can more easily manage the UI Servers of your system.

**Note:** UI servers provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console.

## What do you want to do?

- Check the status of a UI server managers
- Manage UI servers
- Close the window by clicking **Exit**

## Check the Status of GUI Server Managers

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers**

### Checking the Status of GUI Server Managers

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **GUI Servers**. The Configure DNCS User Interface Web Applications window opens and lists the UI Server Managers..
4. The **Manager Status** column on the far right provides an at-a-glance status of each Manager. The following lists each possible status for a manager:
    - Green along with the message "**active**" indicates that the Manager process is running. The time indicates the time that Manager started. The number of requests indicates the number of service requests the Manager has processed since it was started.
    - Red along with the message "**inactive**" indicates that the Manager process is not running.
    - Red and the message "**unknown**" indicate that the status of the Manager process is unknown.
5. To close this window, click **Exit**.

## Check the Status of GUI Server Managers

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers**

### Checking the Status of GUI Server Managers

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **GUI Servers**. The Configure DNCS User Interface Web Applications window opens and lists the UI Server Managers..
4. The **Manager Status** column on the far right provides an at-a-glance status of each Manager. The following lists each possible status for a manager:
    - Green along with the message "**active**" indicates that the Manager process is running. The time indicates the time that Manager started. The number of requests indicates the number of service requests the Manager has processed since it was started.
    - Red along with the message "**inactive**" indicates that the Manager process is not running.
    - Red and the message "**unknown**" indicate that the status of the Manager process is unknown.
5. To close this window, click **Exit**.

# Manage UI Servers

### GUI Server Status

### Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > Configure UI Servers

From this window, you can obtain an at-a-glance status of each application (UI Server) in your system. UI servers provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console. Modifying some of the settings for a UI server allows system administrators to customize the behavior of a server and better manage your system. This window also allows you to add new UI servers and to modify, delete, or restart existing UI servers.

## What do you want to do?

From this window, you can perform any of the following tasks:

- View the status of applications (UI servers) that belong to a Manager
- Stop a UI Server
- Start a UI Server

# Manage UI Servers

### GUI Server Status

### Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > Configure UI Servers

From this window, you can obtain an at-a-glance status of each application (UI Server) in your system. UI servers provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console. Modifying some of the settings for a UI server allows system administrators to customize the behavior of a server and better manage your system. This window also allows you to add new UI servers and to modify, delete, or restart existing UI servers.

## What do you want to do?

From this window, you can perform any of the following tasks:

- View the status of applications (UI servers) that belong to a Manager
- Stop a UI Server
- Start a UI Server

## Check Status of UI Servers

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > Configure UI Servers**

### Checking Status of UI Servers

**Note:** Applications (UI servers) provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Configure DNCS User Interface Web Applications opens and lists the UI Server Managers.
4. Click **Configure UI Servers**. The Configure UI Servers window opens and lists the applications (UI Servers) belonging to the Manager you selected.
5. To determine the status of each application (UI server), find the **Status** column on the far right and use it to view the status of each application (UI server). The following list describes each possible status for an application (UI server):
   - Green along with the message "**active**" indicates that the Manager process is running. The time indicates the time that server started up. The number of requests indicates the number of service requests the server has processed since it was started.
   - Red along with the message "**inactive**" indicates that the Manager process is not running.
   - Red and the message "**unknown**" indicate that the status of the Manager process is unknown.
6. To close this window, click **Exit**.

## Check Status of UI Servers

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > Configure UI Servers**

### Checking Status of UI Servers

**Note:** Applications (UI servers) provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Configure DNCS User Interface Web Applications opens and lists the UI Server Managers.
4. Click **Configure UI Servers**. The Configure UI Servers window opens and lists the applications (UI Servers) belonging to the Manager you selected.
5. To determine the status of each application (UI server), find the **Status** column on the far right and use it to view the status of each application (UI server). The following list describes each possible status for an application (UI server):
   - Green along with the message "**active**" indicates that the Manager process is running. The time indicates the time that server started up. The number of requests indicates the number of service requests the server has processed since it was started.
   - Red along with the message "**inactive**" indicates that the Manager process is not running.
   - Red and the message "**unknown**" indicate that the status of the Manager process is unknown.
6. To close this window, click **Exit**.

### Stop a GUI Server

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > [Select UI Server] > Stop selected UI Server**

Sometimes you may need to stop and restart a UI server. For example, if the database is brought down and restarted, you will need to stop and restart the database UI server.

### Stopping a GUI Server

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. In the far left column, click the **Please select a server manager** button next to the Manager whose UI Server you want to stop.
5. Click **Select Server Manager**. The UI Servers window appears and lists the UI servers belonging to the Manager you selected.
6. Click the **Select** button next to the UI Server you want to stop.
7. Click **Stop selected UI Server**. The UI Server stops.
8. You can now start the UI Server you have stopped, or close this page by clicking **Close configuration page**.

### Stop a GUI Server

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > [Select UI Server] > Stop selected UI Server**

Sometimes you may need to stop and restart a UI server. For example, if the database is brought down and restarted, you will need to stop and restart the database UI server.

### Stopping a GUI Server

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. In the far left column, click the **Please select a server manager** button next to the Manager whose UI Server you want to stop.
5. Click **Select Server Manager**. The UI Servers window appears and lists the UI servers belonging to the Manager you selected.
6. Click the **Select** button next to the UI Server you want to stop.
7. Click **Stop selected UI Server**. The UI Server stops.
8. You can now start the UI Server you have stopped, or close this page by clicking **Close configuration page**.

### Start a GUI Server

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > [Select UI Server] > Start selected UI Server**

Sometimes you may need to stop and restart a UI server. For example, if the database is brought down and restarted, you will need to stop and restart the database UI server.

#### Starting a GUI Server

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. In the far left column, click the **Please select a server manager** button next to the Manager whose UI Server you want to start.
5. Click **Select Server Manager**. The UI Servers window appears and lists the UI Servers belonging to the Manager you selected.
6. Click the **Select** button next to the UI Server you want to start.
7. Click **Start selected UI Server**. The UI Server starts.
8. To close this page, click **Close configuration page**.

### Start a GUI Server

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > [Select UI Server] > Start selected UI Server**

Sometimes you may need to stop and restart a UI server. For example, if the database is brought down and restarted, you will need to stop and restart the database UI server.

#### Starting a GUI Server

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. In the far left column, click the **Please select a server manager** button next to the Manager whose UI Server you want to start.
5. Click **Select Server Manager**. The UI Servers window appears and lists the UI Servers belonging to the Manager you selected.
6. Click the **Select** button next to the UI Server you want to start.
7. Click **Start selected UI Server**. The UI Server starts.
8. To close this page, click **Close configuration page**.

# Performance Monitoring

The Performance Monitoring tool allows you to display data collected from DNCS processes in a graphical format, such as a line chart. DHCT and VOD performance data is gathered from DNCS processes in comma separated value (CSV) files and is displayed in a graphical format to help you in maintaining and troubleshooting your system should the need arise.

## What do you want to do?

- Review the types of data that you can monitor with this tool
- Learn how to display performance data in a graphical format
- Configure the Performance Monitoring tool

## Performance Monitoring Reports

The Performance Monitoring tool allows you to display data from the following reports in a graphical format, such as a line chart. For each Report, you can display the results of a single transaction or a combination of transactions as summarized in the following table.

| Report Name | Process Monitored | Transactions Displayed in Graphical Format |
|---|---|---|
| Digital Resources Performance Flow | drm | ▪Number of "allocate resources" requests and successes<br>▪Number of "release resources" requests and successes |
| QAM Manager Performance Flow | qamManager | ▪Number of "session setup" requests and confirmations<br>▪Number of "add resource" requests and confirmations<br>▪Number of "release resource" requests and confirmations<br>▪Number of "session release" requests and confirmations<br>▪Number of session setup timeouts<br>▪Number of session setup failures due to an invalid client ID<br>▪Number of session setup failures due to an invalid session ID<br>▪Number of session setup failures due to the server not accepting the call<br>▪Number of session setup failures due to unavailable resources<br>▪Number of session setup failures due to server with unavailable resources<br>▪Number of session setup failures due to a timeout of the dsm process<br>▪Number of session setup failures due to a reason other than those listed above<br>▪Percentage of sessions successfully set up |
| Digital Sessions Performance Flow | dsm | ▪Number of "create session" requests and responses<br>▪Number of "delete session" requests and responses |
| DHCT Signon Performance Flow | hctmMac | ▪Number of DAVIC connections made<br>▪Number of DAVIC connections lost<br>▪Number of "verify request" received<br>▪Number of "verify response sent"<br>▪Number of "verify response sent" errors<br>▪Number of "verify request received sent to provisioning"<br>▪Number of times hctmMac input queue was detected as full |

| | | |
|---|---|---|
| DHCT UNCONFIG Performance Flow | hctmConfig | ▪Number of "UNConfig receive" requests<br>▪Number of "UNConfig request" confirms<br>▪Number of times the config input queue was detected as full |
| New DHCT Provisioning Performance Flow | hctmProvision | ▪Number of "verify request received by provisioning"<br>▪Number of "verify response sent"<br>▪Number of "verify response sent" errors |

**Related Topics**

- Configure the Performance Monitoring Tool
- Display Performance Data

## Configure the Performance Monitoring Tool

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

The Configuration window allows you to control how frequently the Performance Monitor feature collects performance data.

Follow these instructions to change the data collection interval for the Performance Monitoring feature.

1. Click the **Data Collection Interval (seconds)** field and change the interval to the interval you desire.
2. Click **Save**. The Status area of the window displays "Configuration Saved Successfully."
3. To close the Configuration window, click **Exit**.

**Related Topics**

- Display Performance Data

## Display Performance Data

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

To see transactions for any of the available reports in a graphical format, you must display the performance data. When the report displays, follow the on-screen instructions to set or change how the data is displayed.

### Displaying Performance Data

1. From the DNCS Administrative Console, click the **DNCS tab**.
2. Click the **Utilities tab**.
3. Click **Performance Monitoring**. The main Digital Network Performance Monitoring window opens.
4. Make a selection from each of the following areas to set parameters for the data you would like to display.
    - Type of Graph
    - Start Date
    - End Date
    - Available Reports
5. Click **Select**. The Performance Flow window opens for the report you selected. Follow the on-screen instructions to set or change how you would like to view the data.
6. When you have finished viewing the data, click **Home**. The main Digital Network Performance Monitoring window opens.
7. To close the main window, click **Exit**.

**Note:** To update the list of reports, select **Refresh List**.

## Display Performance Data

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

To see transactions for any of the available reports in a graphical format, you must display the performance data. When the report displays, follow the on-screen instructions to set or change how the data is displayed.

### Displaying Performance Data

1. From the DNCS Administrative Console, click the **DNCS tab**.
2. Click the **Utilities tab**.
3. Click **Performance Monitoring**. The main Digital Network Performance Monitoring window opens.
4. Make a selection from each of the following areas to set parameters for the data you would like to display.
   - Type of Graph
   - Start Date
   - End Date
   - Available Reports
5. Click **Select**. The Performance Flow window opens for the report you selected. Follow the on-screen instructions to set or change how you would like to view the data.
6. When you have finished viewing the data, click **Home**. The main Digital Network Performance Monitoring window opens.
7. To close the main window, click **Exit**.

**Note:** To update the list of reports, select **Refresh List**.

# Reports

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Reports**

The Report Writer software enables you to generate reports that collect data from the DNCS database, poll set-tops for information, and collect system information.

The reports are created in a Hypertext Markup Language (HTML) format, so you can view them online or through a Web browser and you can print them.

This section only contains information on running reports. For troubleshooting reports, see Reports Troubleshooting. For information on installing and configuring Report Writer, refer to Report Writer Version 4.3 for DNCS and ISDS User Guide (part number 4021181).

## What do you want to do?

- Learn how to Add Report Writer Users
- Learn how to Display Reports
- Learn how to Customize Reports
- Learn about Generating Reports
- Learn about Reports Troubleshooting

## Add Report Writer Users

Access to Report Writer requires that the user ID and password are different and unrelated to the system user ID and passwords.

Report Writer is shipped with the user name sareports and the password report. When adding users or changing passwords, follow these guidelines:

- The user name sareports should be the first entry after the group name.
- Each user name is separated by a space.
- In the following example, only the "normal" group has access to the reports.

**Example:** normal: sareports [username] [username]

**Note:** To remove a user, remove the user's name from the groups file.

### Adding New Users or Changing Passwords

1. Log in as **root** on the DNCS.
2. Type **cd /usr/local/apache2/bin** and press **Enter**.
3. Type **./htpasswd /usr/local/apache2/conf/users [username]** and press **Enter**. Replace [username] with the user you are adding or the user whose password you are changing. Do not type the brackets **[ ]** in the command.
4. Type and confirm the **password**.
5. Add the user to the groups file. Use a text editor to open the **/usr/local/apache2/conf/groups** file and append the user name to the line that begins with the word "normal."

### Related Topics

- Display Reports
- Customize Reports
- Generating Reports

### Adding New Users or Changing Passwords

1. Log in as **root** on the DNCS.
2. Type **cd /usr/local/apache2/bin** and press **Enter**.
3. Type **./htpasswd /usr/local/apache2/conf/users [username]** and press **Enter**. Replace [username] with the user you are adding or the user whose password you are changing. Do not type the brackets **[ ]** in the command.
4. Type and confirm the **password**.
5. Add the user to the groups file. Use a text editor to open the **/usr/local/apache2/conf/groups** file and append the user name to the line that begins with the word "normal."

## Display Reports

**Quick Path: DNCS Administrative Console >DNCS tab > Utilities tab > Reports > [Select Report]**

**CAUTION:**

**Before opening Report Writer to display reports, exit all instances of your web browser associated with your UNIX user ID. When you try to open Report Writer with more than one instance of the browser associated with your UNIX user ID, a message appears on the screen stating that your browser has detected a locked file. Do not continue. If you attempt to continue, Report Writer may exhibit unpredictable behavior.**

1. From the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Reports**. A browser opens and displays the web server Welcome page.
4. Click **Report Manager**. A prompt for the user ID and password appears for the server where Report Writer software is located.
5. Type your **User ID** and **Password** and click **OK**.

**Note:** The default user name is **sareports** and the default password is **report**. The browser displays the Reports page. Notice the hyperlinks to the specific reports and a brief description of each report. For more information about reports and how to access them, refer to Generating Reports.

### Related Topics

- Customize Reports
- Generating Reports
- Add Report Writer Users

# Customize Reports

### Insert Your Company Logo

You can customize reports by inserting your company's logo, in GIF format, at the top of each Report Writer page. To do this, exit your browser, name your logo file **top.gif**, and place it in the **/dvs/RepWriter/current/webspace/images** directory.

### Sort the Generated Reports

You can display report data in a different order by sorting any column field. To sort a generated report, click the underlined column heading. After you click the column heading, it is no longer underlined. This indicates that the report was sorted by the selected column.

**Note:** Sorting a report does not regenerate the report data; it only displays the report data in a different order.

### Related Topics

- Generating Reports
- Add Report Writer Users
- Display Reports

### Insert Your Company Logo

You can customize reports by inserting your company's logo, in GIF format, at the top of each Report Writer page. To do this, exit your browser, name your logo file **top.gif**, and place it in the **/dvs/RepWriter/current/webspace/images** directory.

### Sort the Generated Reports

You can display report data in a different order by sorting any column field. To sort a generated report, click the underlined column heading. After you click the column heading, it is no longer underlined. This indicates that the report was sorted by the selected column.

**Note:** Sorting a report does not regenerate the report data; it only displays the report data in a different order.

## Generating Reports

This section describes the different report categories and provides instructions for generating the reports. Also included in this chapter are detailed descriptions of the reports within each category.

### You Need to Know

Before You Begin

Before you read about each type of report and its description, you need to understand that some of the reports refer to the DHCT (set-top) administrative status.

Each DHCT stored in the DNCS database has an associated administrative status, assigned through the Business Operations Support System (BOSS) Application Programming Interface (API). The administrative status can be set by the billing systems or through the DNCSAdministrative Console.

The four possible administrative states of the DHCT are as follows:

- Out of Service
- Deployment
- In Service-One Way
- In Service-Two Way

**Note:** A DHCT whose upstream plant is not two-way mode capable will not function in two-way mode, even though its administrative status has been set to In Service-Two Way.

### Related Topics

- Generating Database Reports
- Generating SNMP Poll Reports
- Generating System Reports

## Generating Database Reports

1. From the DNCS Reports page, click the hyperlink for one of the DNCS Database reports. Did the selected report appear?
    - If yes, the report generation is completed, the report name, the resulting data, and the message **Data Refreshed on MM/DD/YYYY @HH:MM** appears, along with a **Run Report** button. (The HH:MM portion of the date/time stamp is in 24-hour time.)
    - If no, continue with step 2.
2. Click **Run Report**. While the report is being generated, you may see the following message: **Running [report name]. Please wait.** A message appears stating that the report is completed and the number of records processed.

**Note:** If there is not any qualifying data for the report, only the report name, date/time stamp, and the Run Report button appear on the screen.

## Related Topics

- Description of the Database Report
- Generating SNMP Poll Reports
- Generating System Reports

### Descriptions

The following table provides a description of each of the reports that collect data only from the DNCS database. These reports are listed in the order in which you will see them when you open Report Writer.

### Notes:

- Not all of the following reports are applicable to the DNCS. Available reports are based on the implementation of your DNCS. If a report is not supported by the implementation, it will not appear in your options.
- Not all of the reports will contain data, depending on the unique implementation of the DNCS.

| Report Title | Description |
|---|---|
| **PPV Events** | **Data listed:** All pending pay-per-view (PPV) events.<br>**Data sorted by**: Service description and then by start date and time. |
| **Zero Credit** | **Data listed:** All In Service-Two Way DHCTs that have impulse pay-per-view (IPPV) events enabled and a credit limit of 0 (zero).<br>**Data sorted by:** IP address<br>**Normal condition:** Report should not show any data.<br>**Troubleshooting:** DHCTs listed may have been incorrectly staged using the BOSS API. Restage and then re-run the report. |
| **CableCARD Report** | **Data listed:** All CableCARD™ modules that are bound to the system.<br>**Data sorted by:** CableCARD MAC Address |
| **CableCARD-DHCT Combo Device Report** | **Data listed:** All CableCARD-DHCT combo devices that are bound to the system.<br>**Data sorted by:** CableCARD MAC Address |
| **Channels, Sources and Sessions Report** | **Data listed**: Each display channel in the system, including all information about "carriage" of that channel. This includes SDV (if applicable). Updated columns include Bandwidth, Headend Name, Hub Name, QAM Name, and QAM MAC.<br>**Data sorted by:** Channel number |
| **DHCT Report** | **Data listed:** All DHCTs (set-tops) in the DNCS database and some DHCT configuration information.<br>**Normal conditions:** This report can be extensive and not viewable on a workstation that has little free memory. It may take several minutes to generate/display this report.<br>This report is most useful if you have a small number of DHCTs in your system. A DHCT listed in the database will not appear on this report if it is associated with a DHCT type that is not in the DNCS database.* |
| **DHCT Packages Report** | **Data listed:** All DHCTs and their associated packages with package details.<br>**Note:** This report can be generated using the DHCT MAC Address or Package Name filtering options. |

| | |
|---|---|
| **DNCS Packages Report** | **Data listed:** All packages and their associated sources on the DNCS. Includes details of the sources which are assigned to a package. Reports can be run based on the package name or the source name.<br><br>**Note:** The data in this report can be filtered by the name of the package or the name of the source. |
| **Service Group Report** | **Data listed:** All service groups and their associated names, parent IDs, QAM ports, and child IDs. Those sections that are not applicable are listed either as zeros (0) or N/A.<br><br>**Normal condition:** It may take several minutes to generate/display this report, based on the number of service groups you have in your system. |
| **QAMs Report** | **Data listed:** All of the Cisco and legacy SA QAMs that are in the database and information about their configuration.<br><br>**Normal condition:** A QAM listed in the database will not appear on the report if it does not have valid RF ports in the database.* |
| **Netcrypt Report** | **Data listed:** All Netcrypt devices in the system (if any).<br><br>**Data sorted by:** Netcrypt name |
| **PCG Report** | **Data listed:** All PowerKEY® Conditional Access Gateways in the system and their status.<br><br>**Note:** This report only appears if PCG is enabled on the DNCS. |
| **PCG Session Report** | **Data listed:** Details of the sources and sessions that are built on the PCGs in an ISDS 55-1 system.<br><br>**Note:** The data can be filtered by Frequency, MPEG Program Number, PCG IP Address, PCG Name, Source ID, or Access Criteria. This report only appears if RF+IP and 55-1 features are enabled. |
| **Netcrypt Report** | **Data listed:** All Netcrypt™ servers in the DNCS database and their status.<br><br>**Note:** This report only appears if Netcrypt is enabled on the DNCS. |
| **SDV Servers Report** | **Data listed:** All switched digital broadcast servers in the DNCS database and their settings.<br><br>**Note:** This report only appears if SDV is enabled on the DNCS. |
| **Service Group Report** | **Data listed:** The service groups created on the DNCS.<br><br>**Note:** No filtering options are provided for this report. |
| **QPSK Modems** | **Data listed:** All QPSK Modulators in the database and information about their configuration.<br><br>**Normal condition:** A QPSK Modulator listed in the database will not appear on the report if it is associated with a hub that is not in the DNCS database.* |
| **QPSK Demods** | **Data listed**: All QPSK Demodulators in the database.<br><br>**Normal condition:** A QPSK Demodulator listed in the database will not appear in the report if it is associated with a QPSK Modulator, hub, or node set that is not in the DNCS database.* |

| | |
|---|---|
| **In Service One-Way** | **Data listed:** DHCTs with an administrative status of In Service-One Way.<br><br>**Normal condition:** Report Writer queries the DNCS database to identify DHCTs that have been configured for one-way service. |
| **Non-Responding DHCTs N ever Connected** | **Data listed:** DHCTs with an administrative status of In Service-Two Way or Deployment that do not have an IP address.<br><br>**Normal condition:** Queries the DNCS database to identify DHCTs configured for two-way service that have never established a two-way connection in a DNCS or IP-only ISDS system. These DHCTs should have an IP address, but they do not. In and ISDS RF+IP 55-1 environment, these DHCTs have an Operational status of Unknown. |
| **Non-Responding DHCTs Lost Connection** | **Data listed:** DHCTs with an administrative status of In Service-Two Way which have an IP address, but whose operational status is "Unknown," "MAC initialization failed," or "DSMCC boot failed."<br><br>**Normal condition:** Queries the DNCS database to identify DHCTs configured for two-way service that have lost a previous two-way connection. |
| **TSID List** | **Data listed:** Lists transport stream IDs (TSIDs) used by QAMs from Cisco and other vendors.<br><br>**Normal condition:** Queries the database to identify all TSIDs that have been used in the system. |

*This situation should occur infrequently, if at all, and could indicate that some sort of DNCS database corruption has occurred. Try to open the applicable DNCS Administrative Console GUIs to ensure that the data is intact for a particular device.

### Related Topics

- Generating Database Reports
- Generating SNMP Poll Reports
- Generating System Reports
- Reports Troubleshooting

## Generating SNMP Poll Reports

1. From the DNCS Reports page, click **SNMP Poll Reports**.
2. Click the hyperlink of one of the SNMP Poll Reports.
3. Does the report appear on the screen:
   - If **yes**, the data is from the last time the SNMP Poll Report was run. Click **Back** to return to the SNMP Poll Reports page; then click **Run Report** to refresh the report data.
   - If **no**, go to step 4.
4. Does the following message appear on the screen?
   **This report has not yet been generated on your system. Please press the back button on your browser to return to the SNMP page**.
   - If **yes**, click **Back** to return to the SNMP Poll Reports page.
   - If **no**, click **Run Report** to generate all of the SNMP Poll Reports.

**Important:** The SNMP Poll Reports can take a significant amount of time to complete, depending on the number of DHCTs (set-tops) in your system. While the SNMP Poll Reports are being generated, do not exit your browser. Exiting the browser while the reports are being generated can cause errors in the Report Writer software that will require some manual clean-up steps (see Reports Troubleshooting). We recommend that you do not click anywhere in your browser until the SNMP Poll Reports are completely generated.

**Notes:**

- While the reports are being generated, the following message appears:
  **Running [report name]. Please wait**.
- Concurrently, a table appears on the screen, and as each SNMP Poll report is generated, its status is updated from "working" to "complete."

5. When all the SNMP Poll reports are generated, click the browser **Back** button.
6. Click the hyperlink for a specific SNMP Poll Report.
7. Does the report appear on the screen?
   - If **yes**, you have completed this procedure and all of the SNMP Poll Reports have been generated.
   - If **no**, repeat this procedure.

## Related Topics

- Description of the SNMP Poll Reports
- Generating System Reports
- Generating Database Reports

### Descriptions

The SNMP Poll Reports collect data by issuing up to three SNMP poll requests to each candidate DHCT (set-top).

The term candidate DHCTs refers to DHCTs in the DNCS database that have an associated MAC address, IP address, QPSK Modulator, and QPSK Demodulator, along with an administrative status of In Service-Two Way. If a DHCT listed in the DNCS database does not meet all of these criteria, it will be excluded from the SNMP Poll Report. The SNMP poll request determines the current two-way communication ability of each DHCT.

When the SNMP Poll Report is run, each candidate DHCT is polled (this is also called an SNMP "get" request). This SNMP poll collects all of the data necessary for generating the four SNMP Poll reports. The SNMP Poll reports are different views into the data collected.

If a DHCT does not respond to the initial SNMP poll, it is polled up to two more times (for a maximum of three attempts). If the SNMP poll is unsuccessful after three attempts, the DHCT is considered to be a non-responder and will appear only on the Non-Responding DHCTs-SNMP Poll Report. However, if at least one of the three SNMP poll attempts succeeds, then the DHCT will appear in the OS/App Version, Memory, and DHCT Uptime Reports.

**Note:** You can view the list of candidate DHCTs from the last SNMP Poll Report that was run by examining the **/dvs/RepWriter/current/bin/maclist** file.

The following table provides a description of each of the SNMP Poll Reports. These reports are listed in the order in which you will see them when you open Report Writer.

**Note:** Not all of the following reports are applicable to the DNCS.

| Report Title | Description |
|---|---|
| **Non-Responding DHCTs-SNMP Poll** | **Data listed:** All DHCTs that did not respond to one of three SNMP "get" requests. |
| **OS/App Version*** | **Data listed:** The PowerTV® Operating System and Resident Application versions installed in each DHCT.<br>**Notes:**<br>▪SARA is a Cisco resident application that is run on the DHCT that provides all basic functionality for the DHCT, including navigation, changing channels, volume control, etc.<br>▪Set-tops manufactured by other vendors have a different resident application installed to handle this functionality. |
| **Memory Report*** | **Data listed:** The total memory in each DHCT, and the amount of memory currently free. |
| **DHCT Uptime*** | **Data listed:** The amount of time since each DHCT last rebooted. |

*The OS/App Version, Memory, and DHCT Uptime reports display data collected from both the SNMP "get" request and from the DNCS database.

**Related Topics**

- Generating SNMP Poll Reports
- Reports Troubleshooting
- Generating System Reports
- Generating Database Reports

## Generating System Reports

1. From the DNCS Reports page, click **System Reports**.
2. The data for all the following reports are on this page. Click the hyperlink for a specific report to generate that report.

## Related Topics

- Description of the System Reports
- Generating Database Reports
- Generating SNMP Poll Reports

## Descriptions

The following table provides a description of each of the reports that collect and display information to provide a quick overview of the health of the DNCS system. These reports are listed in the order in which you will see them when you open Report Writer.

**Note:** Not all of the following reports are applicable to the DNCS.

| Report Title | Description |
|---|---|
| **General System Information** | **Data listed:** DNCS system information (CPU, memory, and processes currently running). |
| **File System Information** | **Data listed:** Total and available disk space for the DNCS system. |
| **Network Information** | **Data listed:** Network interfaces and the routing table. |
| **Database Information** | **Data listed:** Information about the INFORMIX database on the DNCS.<br>**Note:** This is the database used by the DNCS. |

## Related Topics

- Generating System Reports
- Reports Troubleshooting
- Generating Database Reports
- Generating SNMP Poll Reports

# DNCS Security

## Introduction

This section describes the enhanced security features included with the DNCS.

- User Accounts
- Password Management

# User Accounts

This section describes how to create and delete user accounts.

## What do you want to do?

- Create a user account
- Delete a user account
- Find out information about a user account

## Creating a User Account

**Note:** The user will be required to change their password during their first successful login session.

1. Open an xterm window on the DNCS.
2. Log into the DNCS as root.
3. Type **useradd -u [user ID] -g [user group] -c "[comment about this user]" -d [user home directory] -s [user shell] -m -k [user skeleton directory]; passwd [user ID]** at the prompt.

   **Notes:**

   - The user ID must be between 6 and 8 alphanumeric characters.
   - The user ID cannot contain special characters.
   - Do not type the brackets **[ ]** in the command.

4. Type the new password for the user account and press **Enter**. A prompt to re-enter the password appears.
5. Type the password again and press **Enter**.
6. Type **cd /export/home/[username]** and press **Enter**. The user's home directory becomes the active directory.
7. Open the user's **.profile** file in a UNIX text editor.
8. Add the following lines to the .profile file:

   **export PS1="$LOGNAME@'hostname':$PWD>"**

   **set -o vi**

9. Save and close the user's .profile file.

**Related Topics**

- Deleting a User Account
- Who Am I?

## Deleting a User Account

Use this procedure to delete user accounts.

1. Log into the DNCS as root.
2. Review the user files in the user's home directory and move any files that should be retained to another directory, outside the user's home directory.
3. In an xterm window, type **userdel -r [username]** and press **Enter**. The system deletes the user's home directory.

   **Note:** Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

4. Type **projdel user.[username]** and press **Enter**. The system removes the user from the /etc/project file.

   **Note:** Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

5. Is the user you are deleting a Regular User?
   - If **yes**, type **groupdel [username]** and press **Enter**. The system deletes the group associated with that user.

     **Note:** Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

   - If **no**, you are finished with this procedure.

**Related Topics**

- Creating a User Account
- Who Am I?

## Who Am I?

To determine your current ID or your session role, you can type one of the following from the DNCS command line and press **Enter**:

- **id**
- **/usr/ucb/whoami**

  The system returns the user ID of the your current session or the session role of your current session.

**Note:** If you add /usr/ucb to your default path, you only need to type **whoami** and press **Enter**.

### Related Topics

- Creating a User Account
- Deleting a User Account

# Password Management

Regardless of password management rules enforced by a system, users must still be encouraged to choose difficult to guess passwords. Proper system management of passwords is important but the primary responsibility for strong passwords ultimately rests with the user.

## What do you want to do?

- Learn about password guidelines
- Change your password

## Password Guidelines

**Note:** These guidelines apply to all systems in your network.

Users must select a very strong, complex password. Strong passwords have the following general characteristics:

- Contain 8 or more characters
- Contain characters from at least three of the following:
  - Lower-case letters
  - Upper-case letters
  - Digits
  - Special characters
- Do **not** consist of only one character type (**aaaaaaa** or **11111111**)
- Do **not** contain any aspects of a date
- Are **not** proper names or words you would find in the dictionary
- Are **not** the same as previous passwords with an added capitalization
- Are **not** telephone numbers or similar numeric groups
- Are **not** user IDs, user names, group IDs, or other system identifiers
- Do **not** contain more than two (2) consecutive occurrences of the same character
- Are **not** consecutive keyboard patterns (for example, **qwerty**)

**Related Topics**

- Changing Your Own Password

## Changing Your Own Password

**Note:** This topic applies to all systems.

1. Open an xterm window on the system.
2. At the login prompt, type **passwdSAM Service** and press **Enter**. The system will prompt you for your existing password.
3. Enter your **existing password** and press **Enter**. The system will prompt you for your new password.
4. Enter your **new password** and press **Enter**. The system prompts you to re-enter your new password.
5. Type your **new password** again and press **Enter**. The system compares your two password entries. If they match, the **password successfully changed** message appears. If they do not match, you must re-enter the new password.
6. Type **exit** and press **Enter** to close the xterm window.
7. Log out of the system.
8. Log into the system with your new password.

**Related Topics**

- Password Guidelines

# Troubleshoot the Network

## Introduction

This section describes troubleshooting techniques for your DBDS.

Troubleshoot a DBDS

# Troubleshoot a DBDS

**Important:** We recommend that you run the Doctor Report every morning and every evening. However, you should always run the Doctor Report anytime you suspect or experience problems.

For further information about the Doctor Report, refer to DBDS Utilities Version 6.3 Installation Instructions and User Guide (part number 4031374). To obtain a copy of this publication, see Printed Resources.

**Note:** To troubleshoot an RCS, follow these suggestions as well as those specific to an RCS.

Click on the symptom that best describes the trouble you are having.

- DHCTs are being classified as non-responding units in large quantities
- DNCS process is not running
- Programs are experiencing interference (for example, snow or static)

## DHCTs Classified as Non-Responding

These errors can occur if you have configured two or more QPSK demodulators at the same frequency on the same node set.

Complete these steps to resolve this problem.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. On the Network Element Provisioning tab, click **QPSK**. The QPSK List appears.
4. On the QPSK List, click **File > Modem Summary**. The QPSK Modem Summary window appears showing all of your QPSK modulators with their associated demodulators, node sets, and frequencies.
5. Make a note of the QPSK demodulators that are assigned to the same node set with the same frequency.
6. Modify these demodulators using the following guidelines:
   - If you are NOT using a backup service channel, you can assign only one QPSK demodulator to a node set. Then, you can assign the same frequency to other QPSK demodulators.
   - If you are using a backup service channel, you can assign more than one QPSK demodulator to the same node set. However, you must assign a unique frequency to each demodulator on that node set.

## DNCS Process Not Running

After the DNCS is up and running, all of the DNCS processes should have a green working state on the DNCS Control window. However, if a process remains in a **red** or **yellow** working state, this indicates that the process is not functioning properly. If this occurs, perform the following corrective steps.

**Important:** If you are unsure of how to perform any of these steps, contact Cisco Services.

1. Save the log files in the **/dvs/dncs/tmp** directory. The log files associated with the process have the format of <process name>.xxx, where xxx is a three-digit number.
2. Save the dncsLog files in the **/var/log** directory. The log files have the format dncsLog.x, where x is a single-digit number.
3. Save any corefiles in the **/dvs/dncs/tmp/corefiles/<processName>** directory. Corefiles will have

the format core.xxxxx, where xxxxx is a five- digit number.

4. Is the current working state of the process in question **red** or **yellow**?
   - If it is **red**, go to step 5.
   - If it is **yellow**, stop here and contact Cisco Services.
5. Try to restart the process as follows:
   - In the DNCS Control window, click once on the process name.
   - Click **Process > Start Process**.
6. Did the process change to a **green** working state?
   - If **yes**, the process is now running. No further action is necessary.
   - If **no**, contact Cisco Services.

## Program Interference

If DHCTs are experiencing program interference (for example, snow or static), try changing the appropriate QAM frequencies by 250 kHz from their current settings. Click for a table of recommended QAM frequencies.

## DHCTs Classified as Non-Responding

These errors can occur if you have configured two or more QPSK demodulators at the same frequency on the same node set.

Complete these steps to resolve this problem.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **Network Element Provisioning** tab.
3. On the Network Element Provisioning tab, click **QPSK**. The QPSK List appears.
4. On the QPSK List, click **File > Modem Summary**. The QPSK Modem Summary window appears showing all of your QPSK modulators with their associated demodulators, node sets, and frequencies.
5. Make a note of the QPSK demodulators that are assigned to the same node set with the same frequency.
6. Modify these demodulators using the following guidelines:
    - If you are NOT using a backup service channel, you can assign only one QPSK demodulator to a node set. Then, you can assign the same frequency to other QPSK demodulators.
    - If you are using a backup service channel, you can assign more than one QPSK demodulator to the same node set. However, you must assign a unique frequency to each demodulator on that node set.

## DNCS Process Not Running

After the DNCS is up and running, all of the DNCS processes should have a green working state on the DNCS Control window. However, if a process remains in a **red** or **yellow** working state, this indicates that the process is not functioning properly. If this occurs, perform the following corrective steps.

**Important:** If you are unsure of how to perform any of these steps, contact Cisco Services.

1. Save the log files in the **/dvs/dncs/tmp** directory. The log files associated with the process have the format of <process name>.xxx, where xxx is a three-digit number.
1. Save the dncsLog files in the **/var/log** directory. The log files have the format dncsLog.x, where x is a single-digit number.
1. Save any corefiles in the **/dvs/dncs/tmp/corefiles/<processName>** directory. Corefiles will have the format core.xxxxx, where xxxxx is a five- digit number.
1. Is the current working state of the process in question **red** or **yellow**?
    - If it is **red**, go to step 5.
    - If it is **yellow**, stop here and contact Cisco Services.
1. Try to restart the process as follows:
    - In the DNCS Control window, click once on the process name.
    - Click **Process > Start Process**.
1. Did the process change to a **green** working state?
    - If **yes**, the process is now running. No further action is necessary.
    - If **no**, contact Cisco Services.

# Troubleshoot a DBDS

**Important:** We recommend that you run the Doctor Report every morning and every evening. However, you should always run the Doctor Report anytime you suspect or experience problems.

For further information about the Doctor Report, refer to DBDS Utilities Version 6.3 Installation Instructions and User Guide (part number 4031374). To obtain a copy of this publication, see Printed Resources.

**Note:** To troubleshoot an RCS, follow these suggestions as well as those specific to an RCS.

Click on the symptom that best describes the trouble you are having.

- DHCTs are being classified as non-responding units in large quantities
- DNCS process is not running
- Programs are experiencing interference (for example, snow or static)

## DHCTs Classified as Non-Responding

These errors can occur if you have configured two or more QPSK demodulators at the same frequency on the same node set.

Complete these steps to resolve this problem.

1. On the DNCS Administrative Console, click the **DNCS** tab.
1. On the DNCS tab, click the **Network Element Provisioning** tab.
1. On the Network Element Provisioning tab, click **QPSK**. The QPSK List appears.
1. On the QPSK List, click **File > Modem Summary**. The QPSK Modem Summary window appears showing all of your QPSK modulators with their associated demodulators, node sets, and frequencies.
1. Make a note of the QPSK demodulators that are assigned to the same node set with the same frequency.
1. Modify these demodulators using the following guidelines:
    - If you are NOT using a backup service channel, you can assign only one QPSK demodulator to a node set. Then, you can assign the same frequency to other QPSK demodulators.
    - If you are using a backup service channel, you can assign more than one QPSK demodulator to the same node set. However, you must assign a unique frequency to each demodulator on that node set.

## DNCS Process Not Running

After the DNCS is up and running, all of the DNCS processes should have a green working state on the DNCS Control window. However, if a process remains in a **red** or **yellow** working state, this indicates that the process is not functioning properly. If this occurs, perform the following corrective steps.

**Important:** If you are unsure of how to perform any of these steps, contact Cisco Services.

1. Save the log files in the **/dvs/dncs/tmp** directory. The log files associated with the process have the format of <process name>.xxx, where xxx is a three-digit number.
1. Save the dncsLog files in the **/var/log** directory. The log files have the format dncsLog.x, where x is a single-digit number.
1. Save any corefiles in the **/dvs/dncs/tmp/corefiles/<processName>** directory. Corefiles will

have the format core.xxxxx, where xxxxx is a five- digit number.

1. Is the current working state of the process in question **red** or **yellow**?
   - If it is **red**, go to step 5.
   - If it is **yellow**, stop here and contact Cisco Services.
1. Try to restart the process as follows:
   - In the DNCS Control window, click once on the process name.
   - Click **Process > Start Process**.
1. Did the process change to a **green** working state?
   - If **yes**, the process is now running. No further action is necessary.
   - If **no**, contact Cisco Services.

## Program Interference

If DHCTs are experiencing program interference (for example, snow or static), try changing the appropriate QAM frequencies by 250 kHz from their current settings. Click for a table of recommended QAM frequencies.

# Unlisted, Active Sessions

This topic shows you how to correct unlisted, active sessions by tearing down the session and then restarting it from the Set Up Digital Source Definition window. Restarting a session from the Set Up Digital Source Definition window automatically opens the Define Session window with predefined values for most settings based on the data you used to set up the session. This method allows you to easily identify and change any incorrect information as you use the Define Session window to restart the session with correct parameters.

Follow this process to correct unlisted, active sessions:

1. Tear down the session.
2. Restart the session from the Set Up Digital Source Definition window.

**In This Section**

Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators
Restart a Session

## Tear Down Sessions on Content QAM, MQAM, or GQAM Modulators

1. If you have not already done so, display the appropriate sessions. For assistance, refer to Use the Filter to Display Sessions.

2. When the list of sessions displays, use one of the following methods to select the sessions you would like to tear down:

   - To tear down specific sessions, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete.
   - To tear down all sessions, click **Select All Displayed Sessions**.

**Note:** If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.

3. Click **Tear Down**. The system tears down the sessions you selected and updates the status of all sessions.

4. Click **File > Close** to close the Session Data window.

5. Depending on your reason for tearing down the session, you may decide to complete one of the following tasks:

   - If you tore down the session in order to delete a QAM modulator, you can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind. For assistance, see Delete a Content QAM Modulator.
   - If you deleted the session in order to correct an unlisted, active session, restart the session. For assistance, see Restart a Session.

## Restart a Session

**Quick Path: DNCS Administrative Console > System Provisioning tab > Source > [Select Source for Session] > File > Source Definition > [Select Source Definition] > Start Session > [Follow Set Up Digital Source Definition Window Prompts]**

After you tear down a session, follow this procedure to restart it from the Set Up Digital Source Definition window. Tearing down and restarting a session is helpful in correcting unlisted, active sessions.

**Note:** Restarting a session from the Set Up Digital Source Definition window automatically opens the Define Session window with predefined values for most settings based on the data you used to set up the session. This method allows you to easily identify and change any incorrect information as you use the Define Session window to restart the session with correct parameters.

1. On the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **Source**. The Source List window opens.
3. Select the source for the session, click **File > Source Definition**. The Source Definition List opens for the source you selected.

   **Note:** You can find the source for a session by looking through the Source ID column to find the ID that corresponds to the session ID.

4. Select the source definition with the status of Tear Down and click **File > Open**. The Set Up Digital Source Definition window opens for the source definition you selected.
5. Click **Start Session**. The Define Session window opens.
6. If necessary, select the correct source type, and then click **Next**. The Session Setup window opens.
7. If necessary, select the correct input device, and then click **Next**. The Select Outputs window opens.
8. Select the modulator that will receive content from this source and click **Next**. The Wrap-Up window opens and displays settings and values for the device.

   **Note:** To select more than one modulator, hold down the **Ctrl** key on your keyboard as you click on each modulator.

9. Verify that the values shown are correct and click **Next**. The Save Source Definition window opens.

   **Note:** If any values are incorrect, change them.

10. Click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

# Troubleshooting an RCS

Even with regular maintenance, you may encounter problems with your RCS. If problems do occur, the following tasks can help you troubleshoot your RCS.

## What do you want to do?

- Adjust the logging level for key RCS processes
- Adjust the logging level for key RCS libraries
- Troubleshoot common DBDS problems

# Reports Troubleshooting

This section describes the most common situations that may cause errors with the Report Writer software and provides troubleshooting guidelines and possible solutions. Refer to the following table to review symptoms and possible remedies.

| Symptom | Possible Solutions |
|---|---|
| Cannot find the error files | ▪Determining if Error Files Exist<br>▪Error Files |
| Cannot find the web browser toolbar | ▪Displaying the Web Browser Toolbar |
| Cannot access Report Writer | ▪Report Writer Not Installed Properly<br>▪Web Server Not Running<br>▪Cannot Access Report Writer URL |
| No data in report | ▪No Data or Old Data in the Report<br>▪Web Browser Unable to Display Data |
| Old data in report | ▪No Data or Old Data in the Report |
| Browser displays runtime errors when you try to generate a report | ▪Runtime Errors |
| Web browser does not display data | ▪No Data or Old Data in the Report<br>▪Web Browser Unable to Display Data |
| SNMP Poll reports do not regenerate data | ▪SNMP Poll Reports Do Not Regenerate Data |

**In This Section**


General Reports Troubleshooting
Report Writer Not Installed Properly
Web Server Not Running
Cannot Access the Report Writer URL
No Data or Old Data in the Report
Runtime Errors
Web Browser Unable to Display Data
SNMP Poll Reports Do Not Regenerate Data

## General Reports Troubleshooting

If errors occur while Report Writer is generating a report, those errors are logged into one or more files, depending on the report type. By examining the contents of these files, it may be possible to determine why Report Writer is not providing the results you expect.

### Related Topics

- Error Files
- Determining if Error Files Exist
- Displaying the Web Browser Toolbar

### Error Files

The Digital Network Control System creates one or more of the following files if errors occur while Digital Network Control System is generating a report. Examine the contents of these files to determine why Digital Network Control System is not providing the results you expect.

| Report | File |
|---|---|
| All Reports | /tmp/PPVEvents.err |
| | /tmp/ZeroCredit.err |
| | /tmp/CableCard.err |
| | /tmp/CSSReport.err |
| | /tmp/Converters.err |
| | /tmp/DhctPkg.err |
| | /tmp/DNCSPkg.err |
| | /tmp/Qams.err |
| | /tmp/NetCrypt.err |
| | /tmp/Pcg.err |
| | /tmp/SDVServers.err |
| | /tmp/QPSKMods.err |
| | /tmp/QPSKDemods.err |
| | /tmp/InServOneWay.err |
| | /tmp/NRNeverConn.err |
| | /tmp/NRLostConn.err |
| | /tmp/SvcGroup.err |
| | /tmp/DhctsignOnFailed.err |
| | tmp/PcgSession.err |
| SNMP Poll Reports | /tmp/NRSNMPPoll.err |
| | /tmp/ResAppVersion.err |
| | /tmp/FreeMem.err |
| | /tmp/Uptime.err |
| | /tmp/asnmp.err |
| | /tmp/getdhcts.err |

### Related Topics

- Determining if Error Files Exist
- Displaying the Web Browser Toolbar
- General Troubleshooting

### Determining if Error Files Exist

When you successfully generate a report, the files listed in the Error Files table are either non-existent or exist but have been cleared (zero content).

1. To determine if an error file exists, log in to the DNCS server and enter the password.
2. Type **cd /tmp** and press **Enter**.
3. Type **ls -l *.err** and press **Enter**.

   **Note:** The "l" in **-l** is a lowercase letter L.

4. Type **cat [filename].err** and press **Enter**. The [filename] represents one of the error file names listed in Error Files. If the file contains errors, its contents will appear on the screen.

### Related Topics

- Displaying the Web Browser Toolbar
- General Troubleshooting
- Error Files

### Displaying the Web Browser Toolbar

If the web browser Navigation Toolbar is not displayed (Back, Forward, etc.), click **View > Toolbars > Navigation Toolbar**. The Navigation Toolbar appears.

### Related Topics

- General Troubleshooting
- Error Files
- Determining if Error Files Exist
- Reports Troubleshooting

## Report Writer Not Installed Properly

If Report Writer is not functioning as expected, verify that the Report Writer software is installed on the DNCS server and that the installation status is "completely installed."

1. Log in to the DNCS as **dncs** user.
2. Open an xterm window on the DNCS.
3. Type **pkginfo -l SAIrptwrt** and press **Enter.** The Report Writer installation status and version number appear on the screen:

```
STATUS: completely installed
VERSION: [product version]
```

4. Does the STATUS field indicate completely installed?
   - If **yes**, the Report Writer software installation is complete.
   - If **no**, you must uninstall then reinstall the Report Writer software. Refer to Report Writer Version 4.3 for DNCS and ISDS User Guide (part number 4021181) for these procedures.

### Related Topics

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Web Server Not Running
- Cannot Access RprtWriter URL
- No Data or Old Data in the Report
- Web Browser Unable to Display Data
- Runtime Errors
- SNMP Poll Reports Do Not Regenerate Data

## Web Server Not Running

To run DNCS, the Apache HTTP Server must be running on the DNCS server.

1. Log in to the DNCS server as **root.**
2. Type **ps -ef | grep httpd** and press **Enter.**
3. Does the information on your screen look similar to the following example:
   **root 458 1 0 08:36:10 ? 0:00 ./httpd**
   - If **yes**, the Apache HTTP Server is running.
   - If **no**, type **/etc/rc2.d/S99http** and press **Enter** to start the Apache HTTP Server.

**Related Topics**

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Report Writer Not Installed Properly
- Cannot Access RprtWriter URL
- No Data or Old Data in the Report
- Web Browser Unable to Display Data
- Runtime Errors
- No Data or Old Data in the Report
- SNMP Poll Reports Do Not Regenerate Data

## Cannot Access the Report Writer URL

If you are unable to access the Digital Network Control System website from your browser, verify that you are typing the correct URL.

1. From the DNCS Admin window select the **DNCS** tab.
2. From the **Utilities** tab, click **Reports.**
3. Select **Report Manager**. A prompt for the user ID and password appears on the screen.
4. Does the Prompt window open?
   - If **yes**, your browser successfully accessed Report Writer.
   - If **no**, type **http://[ip_address]:8045** and press **Enter**. In this command, [ip_address] represents the DNCS server IP address.
5. Did you successfully access the website?
   - If **yes**, click **Report Manager**.
   - If **no**, repeat this procedure.
6. Does the Prompt window open?
   - If **yes**, your browser successfully accessed Report Writer.
   - If **no**, see Report Writer Not Installed Properly to verify that the correct version of the Report Writer software is installed on your DNCS.

**Related Topics**

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Report Writer Not Installed Properly
- Web Server Not Running
- No Data or Old Data in the Report
- Web Browser Unable to Display Data
- No Data or Old Data in the Report
- Runtime Errors
- SNMP Poll Reports Do Not Regenerate Data

# No Data or Old Data in the Report

## No Data in Report

Occasionally, after you run a report, the resulting web page displays only the name of the report, a timestamp, and the Run Report button. If you believe that the report should contain data, use the following procedure to determine if DNCS is connecting to the DNCS database.

1. Log in to the DNCS server and enter the password.
2. Open an xterm window on the DNCS.
3. Type **cd /tmp** and press **Enter.**
4. Type **ls *.err** and press **Enter**.

   **Note:** The "l" in **ls** is a lowercase letter L.

5. Type **cat [report_name].err** and press **Enter**. Replace [report_name] with the name of the report you are requesting. Do not type the brackets **[ ]** in the command.
6. Locate the **[report_name] / open Db( ) error: + an error msg.Exiting** line in the list. The [report_name] represents the name of the requested report.
7. Does the **ERROR: failed to connect!** message appear on your screen?
   - If **yes**, Report Writer could not connect to the DNCS database; this is the reason that the reports do not contain data.
   - If **no**, Report Writer is connected to the DNCS database, and there is no data to report or some other error has occurred.

## Old Data in Report

If a report contains old data, click **Run Report** to refresh the report with current data.

## Related Topics

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Report Writer Not Installed Properly
- Web Server Not Running
- Cannot Access RprtWriter URL
- Web Browser Unable to Display Data
- Runtime Errors
- No Data or Old Data in the Report
- SNMP Poll Reports Do Not Regenerate Data

### No Data in Report

Occasionally, after you run a report, the resulting web page displays only the name of the report, a timestamp, and the Run Report button. If you believe that the report should contain data, use the following procedure to determine if DNCS is connecting to the DNCS database.

1. Log in to the DNCS server and enter the password.
2. Open an xterm window on the DNCS.
3. Type **cd /tmp** and press **Enter.**
4. Type **ls *.err** and press **Enter**.

   **Note:** The "l" in **ls** is a lowercase letter L.

5. Type **cat [report_name].err** and press **Enter**. Replace [report_name] with the name of the report you are requesting. Do not type the brackets **[ ]** in the command.
6. Locate the **[report_name] / open Db( ) error: + an error msg.Exiting** line in the list. The [report_name] represents the name of the requested report.
7. Does the **ERROR: failed to connect!** message appear on your screen?
   - If **yes**, Report Writer could not connect to the DNCS database; this is the reason that the reports do not contain data.
   - If **no**, Report Writer is connected to the DNCS database, and there is no data to report or some other error has occurred.

### Old Data in Report

If a report contains old data, click **Run Report** to refresh the report with current data.

## Runtime Errors

Runtime errors generated by Digital Network Control System are displayed in the browser. The display includes the name of the file that contains the errors, along with the error messages.

To exit the error display, click the browser **Back** button.

**Important**: We recommend that you get assistance from your system administrator to resolve runtime errors.

### Related Topics

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Report Writer Not Installed Properly
- Web Server Not Running
- Cannot Access RprtWriter URL
- No Data or Old Data in the Report
- Web Browser Unable to Display Data
- SNMP Poll Reports Do Not Regenerate Data

## Web Browser Unable to Display Data

Some reports generate a large amount of data. Due to its limitations, your browser may not be able to display very large reports.

To view the data files of reports that have large amounts of data, use a text editor. You can find the data files for each report generated by Report Writer in the **/dvs/RepWriter/current/webspace/reports** directory.

### Data Files

The following tables list the data files generated for each type of report.

| Database Reports | | File Generated |
|---|---|---|
| PPV Events | | PPVEvents.html.dat |
| Zero Credit | | ZeroCredit.html.dat |
| CableCARD Report | | CableCard.html.dat |
| Channels, Sources and Sessions Report | | CSSReport.html.dat |
| DHCT Report | | Converters.html.dat |
| DHCT Packages Report | | DhctPkg.html.dat |
| DNCS Packages Report | | DNCSPkg.html.dat |
| Service Group Report | | SvcGroup.html.dat |
| QAMS Report | | Qams.html.dat |
| PCG Report | | Pcg.html.dat |
| NetCrypt Report | | NetCrypt.html.dat |
| SDV Servers Report | | SDV Servers.html.dat |
| QPSK Modems | | QPSKMods.html.dat |
| QPSK Demods | | QPSKDemods.html.dat |
| In Service One-Way | | InServOneWay.html.dat |
| Non-Responding DHCTs | Never Connected | NRNeverConn.html.dat |
| Non-Responding DHCTs | Lost Connection | NRLostConn.html.dat |
| DHCT Sign-on Failed Report | | DhctSignOnFailed.html.dat |
| PCG Sessions Report | | PcgSession.html.dat |
| **SNMP Poll Reports** | | **File Generated** |
| Non Responding DHCTs | SNMP Poll | NRSNMPPoll.html.dat |
| OS/App Version | | ResAppVersion.html.dat |
| Memory | | FreeMem.html.dat |
| DHCT Uptime | | Uptime.html.dat |
| **System Reports** | | **File Generated** |

No file generated

### Related Topics

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Report Writer Not Installed Properly
- Web Server Not Running
- Cannot Access RprtWriter URL
- No Data or Old Data in the Report
- Runtime Errors
- SNMP Poll Reports Do Not Regenerate Data

### Data Files

The following tables list the data files generated for each type of report.

| Database Reports | | File Generated |
|---|---|---|
| PPV Events | | PPVEvents.html.dat |
| Zero Credit | | ZeroCredit.html.dat |
| CableCARD Report | | CableCard.html.dat |
| Channels, Sources and Sessions Report | | CSSReport.html.dat |
| DHCT Report | | Converters.html.dat |
| DHCT Packages Report | | DhctPkg.html.dat |
| DNCS Packages Report | | DNCSPkg.html.dat |
| Service Group Report | | SvcGroup.html.dat |
| QAMS Report | | Qams.html.dat |
| PCG Report | | Pcg.html.dat |
| NetCrypt Report | | NetCrypt.html.dat |
| SDV Servers Report | | SDV Servers.html.dat |
| QPSK Modems | | QPSKMods.html.dat |
| QPSK Demods | | QPSKDemods.html.dat |
| In Service One-Way | | InServOneWay.html.dat |
| Non-Responding DHCTs | Never Connected | NRNeverConn.html.dat |
| Non-Responding DHCTs | Lost Connection | NRLostConn.html.dat |
| DHCT Sign-on Failed Report | | DhctSignOnFailed.html.dat |
| PCG Sessions Report | | PcgSession.html.dat |
| **SNMP Poll Reports** | | **File Generated** |
| Non Responding DHCTs | SNMP Poll | NRSNMPPoll.html.dat |
| OS/App Version | | ResAppVersion.html.dat |
| Memory | | FreeMem.html.dat |
| DHCT Uptime | | Uptime.html.dat |
| **System Reports** | | **File Generated** |

No file generated

## SNMP Poll Reports Do Not Regenerate Data

Occasionally, the Digital Network Control System software assumes that the SNMP Poll Reports are in the process of running, when in fact they are not. This situation can occur if you exit your browser while the SNMP Poll Reports are running.

**Important:** The SNMP Poll Reports can take a significant amount of time to complete, depending on the number of set-tops in the system. While the SNMP Poll Reports are being generated, do not exit your browser. Exiting the web browser while the reports are being generated can cause errors in the Digital Network Control System software that will require some manual clean-up steps. We also recommend that you do not click any buttons on your browser until the SNMP Poll Reports are completely generated.

**Notes:**

- While the reports are being generated, the following message appears on the screen: **Running [report name]. Please wait**. In this message, [report name] represents the name of the SNMP Poll report being generated.
- Concurrently, a table appears on the screen, and as each SNMP Poll report is generated its status is updated from working to complete.

**Regenerating SNMP Poll Report Data**

If the SNMP Poll Reports do not appear to be regenerating data, complete the following steps to correct the situation.

1. Exit your web browser.
2. From an xterm window on the DNCS, type **su root** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Type **cd /dvs/RepWriter/current/webspace/gen** and press **Enter**.
5. Type **ls** and press **Enter**.
   **Note:** The "l" in **ls** is a lowercase letter L.
6. Does the file **snmprunning** appear on the screen?
   - If **yes**, type **rm snmprunning** and press **Enter** to delete the file.
   - If **no**, then the failure of SNMP Poll Reports to regenerate is not the problem. Review other sections in this chapter and try another resolution.
7. Type **cp snmp.html.refresh snmp.html** and press **Enter**.
8. Type **exit** and press **Enter**.

**CAUTION:**

**Before running Report Writer, exit all instances of your web browser associated with your UNIX user ID. When you try to run Report Writer with more than one instance of your web browser associated with your UNIX user ID, a message appears on the screen stating that your browser has detected a lock file. Do not continue. If you attempt to continue, Report Writer may exhibit unpredictable behavior.**

9. Launch your web browser, and run the SNMP Poll Reports.

**Important:** Do not attempt to use the web browser until the SNMP Poll Reports are complete.

**Related Topics**

- Determining if Error Files Exist
- Error Files
- Displaying the Web Browser Toolbar
- Report Writer Not Installed Properly
- Web Server Not Running
- Cannot Access RprtWriter URL
- No Data or Old Data in the Report
- Web Browser Unable to Display Data
- Runtime Errors

### Regenerating SNMP Poll Report Data

If the SNMP Poll Reports do not appear to be regenerating data, complete the following steps to correct the situation.

1. Exit your web browser.
2. From an xterm window on the DNCS, type **su root** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Type **cd /dvs/RepWriter/current/webspace/gen** and press **Enter**.
5. Type **ls** and press **Enter**.
   **Note:** The "l" in **ls** is a lowercase letter L.
6. Does the file **snmprunning** appear on the screen?
   - If **yes**, type **rm snmprunning** and press **Enter** to delete the file.
   - If **no**, then the failure of SNMP Poll Reports to regenerate is not the problem. Review other sections in this chapter and try another resolution.
7. Type **cp snmp.html.refresh snmp.html** and press **Enter**.
8. Type **exit** and press **Enter**.

**CAUTION:**

**Before running Report Writer, exit all instances of your web browser associated with your UNIX user ID. When you try to run Report Writer with more than one instance of your web browser associated with your UNIX user ID, a message appears on the screen stating that your browser has detected a lock file. Do not continue. If you attempt to continue, Report Writer may exhibit unpredictable behavior.**

9. Launch your web browser, and run the SNMP Poll Reports.

**Important:** Do not attempt to use the web browser until the SNMP Poll Reports are complete.

# Logging

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Logging**

From the Logging Summary window, you can select the type of information the DNCS records about critical processes (and their libraries). When the DNCS records this information, it stores the information in the following locations:

Collective information about all processes is stored in dncsLog in **/var/log/dncsLog**.

Information about individual processes is stored in **/dvs/dncs/tmp/[name of process.*].** The file name of the log for an individual process is the name of the process followed by a 3-digit counter. For example, the file name for the qamManager log might be qamManager.000.

The Logging utility is most useful when you are experiencing problems and want to capture information that can help you resolve the problem. After you adjust the logging level for a specific site and process, you can open the DNCS log in /var/log/dncsLog and view the data that the DNCS has recorded. Or open the log for an individual process in /dvs/dncs/tmp/[name of process.*].

If you are using our RCS solution, you can capture logging information about the processes and libraries for each site in your system.

## What do you want to do?

- Learn about logging levels
- Adjust the logging level of a process
- Adjust the logging level of libraries

## Logging Levels

**Quick Path: DNCS Administrative Console > DNCS tab > Utilities tab > Logging**

By selecting a level of logging for a specific site, you can control the type of information that the DNCS will record about processes running at a site. The default level is the Error level, but you can choose any of the following levels of logging for any process shown as well for any of its libraries.

- **Emergency** - At this level, the DNCS records issues that require immediate attention and may result in a major malfunction of DNCS applications.
- **Alert** - At this level, the DNCS records information about problems with the operating system, such as the system is out of memory or a disk partition is full.
- **Critical** - At this level, the DNCS records information about DNCS problems, such as a process core or a database failure.
- **Error Conditions** (the default logging level) - At this level, the DNCS records operational problems, such as hardware is offline or a code error.
- **Warning** - At this level, the DNCS records information about potential problems that operators should know about.
- **Notice** - At this level, the DNCS records information about normal, but significant events.
- **Information** - At this level, the DNCS records informational messages.
- **Debug** - At this level, the DNCS records information that may help in debugging a problem.

## Adjust the Logging Level of Processes

**Quick Path - With RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select a Site] > [Select Levels] > Save**

**Quick Path - Without RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select Levels] > Save**

### Adjusting the Logging Level of Processes

Follow these steps to select logging levels for processes running on the DNCS (or RNCS if you are using our RCS Solution.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Logging**. The Logging Summary for Host window opens and displays the processes of the DNCS host as the default. If you are using our RCS solution and want to display the processes for a site other than the central DNCS site, go to step 4. Otherwise, go to step 5.
4. Click the **Logging Summary for Host** arrow and select the site whose processes you want to log. The system updates the list of processes and displays the processes running at the site you selected.
5. For each process whose logging level you want to change, click in the appropriate **Logging Levels** box and select the level you want the system to apply.
6. Click **Save**. The system displays a message to let you know the save was completed.
7. Click **OK**.
8. Click **Exit** to close the Logging Summary window and view the logging data in /var/log/dncs/log. Or look at data for an individual process in /dvs/dncs/tmp/[name of process.*].

## Adjust the Logging Level of Processes

**Quick Path - With RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select a Site] > [Select Levels] > Save**

**Quick Path - Without RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select Levels] > Save**

### Adjusting the Logging Level of Processes

Follow these steps to select logging levels for processes running on the DNCS (or RNCS if you are using our RCS Solution.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Logging**. The Logging Summary for Host window opens and displays the processes of the DNCS host as the default. If you are using our RCS solution and want to display the processes for a site other than the central DNCS site, go to step 4. Otherwise, go to step 5.
4. Click the **Logging Summary for Host** arrow and select the site whose processes you want to log. The system updates the list of processes and displays the processes running at the site you selected.
5. For each process whose logging level you want to change, click in the appropriate **Logging Levels** box and select the level you want the system to apply.
6. Click **Save**. The system displays a message to let you know the save was completed.
7. Click **OK**.
8. Click **Exit** to close the Logging Summary window and view the logging data in /var/log/dncs/log. Or look at data for an individual process in /dvs/dncs/tmp/[name of process.*].

## Adjust the Logging Level of Libraries

**Quick Path - With RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select a Site] > [Select Process] > Display Libraries**

**Quick Path - Without RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select Process] > Display Libraries**

### Adjusting the Logging Level of Libraries

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Logging**. The Logging Summary for Host window opens and displays the processes of the DNCS host as the default. If you are using our RCS solution and want to display the processes for a site other than the central, DNCS site, go to step 4. Otherwise, go to step 5.
4. Click the **Logging Summary for Host** arrow and select the site whose processes you want to log. The system updates the list of processes and displays the processes running at the site you selected.
5. Click **Select** next to the process whose libraries you want to log.
6. Click **Display Libraries**. The Libraries for the process you selected in the previous step are listed beneath the Logging Summary list.
7. For each library whose logging level you want to change, click in the appropriate **Logging Levels** box and select the level you want the system to apply
8. Click **Save**. The system displays a message to let you know the save was completed.
9. Click **OK**.
10. Click **Exit** to close the Logging Summary window. You can now open an xterm window and view the logging data in /var/log/dncs/log. Or look at data for an individual process in **/dvs/dncs/tmp/[name of process.*]**.

## Adjust the Logging Level of Libraries

**Quick Path - With RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select a Site] > [Select Process] > Display Libraries**

**Quick Path - Without RCS: DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select Process] > Display Libraries**

### Adjusting the Logging Level of Libraries

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Logging**. The Logging Summary for Host window opens and displays the processes of the DNCS host as the default. If you are using our RCS solution and want to display the processes for a site other than the central, DNCS site, go to step 4. Otherwise, go to step 5.
4. Click the **Logging Summary for Host** arrow and select the site whose processes you want to log. The system updates the list of processes and displays the processes running at the site you selected.
5. Click **Select** next to the process whose libraries you want to log.
6. Click **Display Libraries**. The Libraries for the process you selected in the previous step are listed beneath the Logging Summary list.
7. For each library whose logging level you want to change, click in the appropriate **Logging Levels** box and select the level you want the system to apply
8. Click **Save**. The system displays a message to let you know the save was completed.
9. Click **OK**.
10. Click **Exit** to close the Logging Summary window. You can now open an xterm window and view the logging data in /var/log/dncs/log. Or look at data for an individual process in **/dvs/dncs/tmp/[name of process.*]**.

# Troubleshooting DNCS Online Help

Occasionally, you may encounter problems while using DNCS Online Help. Here are some troubleshooting tips you can use that may resolve the problem.

## Graphics Do Not Print

If you try to print a Help page and the graphics do not print, you probably did not wait long enough for the page to load completely before printing. Reload the Help page and make sure all of the graphics have loaded before attempting to print the page.

## Help Page Does Not Display Properly

Occasionally, a Help page may not load completely. To resolve this problem, complete these steps:

1. Click **View > Reload** on your browser toolbar.
2. Did the page reload properly?
   - If **yes**, you are finished with this procedure.
   - If **no**, go to step 3.
3. Close the Help completely, and then re-open the Help from the DNCS.
4. Did the page reload properly?
   - If **yes**, you are finished with this procedure.
   - If **no**, go to step 5.
5. Contact your system administrator.

## Graphics Do Not Print

If you try to print a Help page and the graphics do not print, you probably did not wait long enough for the page to load completely before printing. Reload the Help page and make sure all of the graphics have loaded before attempting to print the page.

# Troubleshooting DNCS Online Help

Occasionally, you may encounter problems while using DNCS Online Help. Here are some troubleshooting tips you can use that may resolve the problem.

## Graphics Do Not Print

If you try to print a Help page and the graphics do not print, you probably did not wait long enough for the page to load completely before printing. Reload the Help page and make sure all of the graphics have loaded before attempting to print the page.

## Help Page Does Not Display Properly

Occasionally, a Help page may not load completely. To resolve this problem, complete these steps:

1. Click **View > Reload** on your browser toolbar.
1. Did the page reload properly?
    - If **yes**, you are finished with this procedure.
    - If **no**, go to step 3.
1. Close the Help completely, and then re-open the Help from the DNCS.
1. Did the page reload properly?
    - If **yes**, you are finished with this procedure.
    - If **no**, go to step 5.
1. Contact your system administrator.

# Glossary of Terms

**10BASE-T**

An IEEE standard (802.3) for operating 10 Mbps Ethernet networks (LANs) using two pairs of twisted-pair cabling: one pair for transmitting data and the other for receiving data.

**access network**

An HFC network consisting of a fiber optic transmission system extending from a hub to the HFC nodes, and a coax bus network extending from the HFC nodes to the DHCTs within the subscriber's homes.

**access point**

An interface between the wireless network and a wired network. Access points combined with Ethernet support the creation of multiple radio cells that enable roaming.

**Advanced DSG**

Advanced DOCSIS Set-top Gateway. Operates with the DCD message. Address assignment is dynamic. The DSG tunnel address is determined by the DSG agent and learned by the DSG client through the DSG address table in the DCD message.

**analog**

A format in which information is transmitted by modulating a continuous transmission signal, such as amplifying the strength of a signal or varying its frequency.

**API**

Application Program Interface. A set of protocols, routines, and tools for building software applications. An interface that enables programs to communicate with each other.

**Application Server**

A computer workstation and server used to execute the application programs, which provide an interface for downloading application data to the DHCTs. The AppServer works in conjunction with the DNCS and the two computers share a common database.

**AppServer**

See Application Server.

**ASI**

Application Services Interface. A DVB standard for the transfer of MPEG transport streams.

**authentication**

A method in which the network requires a user to identify themselves by entering a user name and password.

**authorization**

The process of granting or denying access to specific resources.

**authorized service domain**

In the authorized service domain (ASD), content is secured using the mechanisms available through the operator's

conditional access system.

The authorized service domain (ASD) physically translates into a collection of one or more trusted devices where content may be securely stored and moved within the domain (typically the subscriber's home).

The distinction between the authorized service domain and other forms of copy protection (for example, DTCP) is that the content remains under operator control at all times with ASD. The control points within the domain are the M-Cards supplied by the operator. Consider the authorized service domain as the operator's digital rights management (DRM) system and an extension of the operator's conditional access (CA) system.

**autobinding**

A process that binds a CableCARD module and host when the CableCARD module is inserted into the host. Autobinding is available for two-way hosts only if all of the following conditions are met:

- The DNCS is set up for autobinding.
- The CableCARD module and host are staged in a two-way environment.

  **Note:** To use autobinding, the CableCARD module and host must be staged in a two-way environment. Once staged and bound, they can be used in a one-way environment.

- The host is not on the certificate revocation list (CRL).

**AVFS**

Audio/video file system.

**backbone**

The part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.

**bandwidth**

The maximum data carrying capacity of a transmission link. For networks, bandwidth is usually expressed in bits per second (bps).

**BER**

Bit error rate. Ratio of received bits that contain errors.

**BFS**

Broadcast File System. The primary interface (means of communication) between the AppServer and the DHCTs that are connected to the network.

**BFS BIG**

Broadcast File System Broadband Integrated Gateway. A device that processes the data it receives and sends it to the data QAM modulator.

**BFS QAM**

A QAM that carries BFS (broadcast file system) data to all set-tops in the headend. A BFS QAM can also carry in-band system information (SI) to all set-tops in a headend. However, when a single QAM is used to carry only SI, it is referred to as a distinguished QAM.

**BIG**

Broadband Integrated Gateway. A device that provides a data pipeline from the DNCS to the DHCTs.

**bind**

A DNCS function that matches the CableCARD module's ID to its host's ID to ensure that the host device conforms to the copy-protection rules defined by the Copy Control Information (CCI). You must bind a CableCARD module to its host before the host can receive high-value copy-protected services.

**bit rate**

The number of bits of information that can be transmitted over a channel in a given second (usually express in bits per second [bps]).

**boot**

The loading of the operating system (OS) and application programs into the main memory or random access memory (RAM) of the system.

**Bootloader**

A factory program installed into the DHCTs to ensure reliable upgrades.

**BOSS**

Business Operations Support System. Open Network Computing RPC protocol for sending requests and responses. It is used by the Billing System to interface to the DNCS and is one of the DNCS/ISDS interfaces for communication with SMS hosts. All BOSS requests are processed by the BOSS server and routed to the proper DNCS/ISDS component.

**BOSS Server**

Provides a mechanism for the routing of a BOSS requests to and from the appropriate DNCS/ISDS component and the BOSS client that initiated the request. Also provides a mechanism for the routing of a BASS request to and from the appropriate Application Server and the BASS client that initiated the request.

**bounce**

Stop and restart a network element or process. For example, to bounce the osm process means to stop and restart the process.

**bps**

Bits per second.

**brick mode**

A state in which the DHCT is not authorized to receive services. Provided by a package which stops all functions of the DHCT, including the ability for it to turn on. Also called service disconnect.

**bridge**

Device that connects and passes packets between two network segments that use the same communications protocol.

**broadband**

A characteristic of a network that indicates that a wide band of frequencies is available. A large amount of information can be carried by multiplexing and transmitting on many different frequencies simultaneously.

Sometimes used more narrowly to describe cable modem service or DSL (digital subscriber line) service from a telephone company.

**broadcast address**

A unique address reserved for sending a message to all receiving stations.

**broadcast flag**

A technology that sends a message to copying devices not to allow unauthorized copying or distribution via networking devices such as connected Digital Video Recorders.

**broadcast server**

A server that delivers interactive content and broadcast data feeds. It uses Internet Protocol (IP) to encode and deliver data over networks that support IP Multicast.

**broadcast-only mode**

A state in which a DHCT has not established an interactive communications path, and only receives broadcast and CA traffic. Advanced services (digital broadcast, IPG, PPV) are available to the DHCT in this mode, but IPPV polling and interactive data services do not function.

**bsm**

Broadcast Segment Manager. The Broadcast Segment Manager is responsible for fielding broadcast segment definitions. It also receives notifications from the SI Manager when broadcast sources start, and forwards those notifications to the Conditional Access Subsystem.

**BTSC**

Broadcast Televisions Standard Committee.

**CA**

See Conditional Access.

**CableCARD**

A device that plugs into a digital cable-ready TV or DHCT and allows the receipt of encrypted services.

**CableLabs**

Cable Television Laboratories. A research consortium sponsored by cable television operators.

**CAQAM**

Conditional access quadrature amplitude modulator. See also QAM, GQAM, MQAM.

**carousel**

Transports data modules and application server processes from the BFS server to the DHCT. For each new application server process that registers with the BFS, a new data carousel is created and the ID information is updated in the BFS directory structure. Also known as Data Carousel or Data Pump.

**CCI (Copy Control Information)**

Copy Control Information defines a program's level of copy protection. There are currently three copy protection

levels defined: copy freely, copy once, and copy never (copy once and copy never are known as high-value copy protection). The CCI is set for the program by the program originator.

The DNCS/ISDS sends the CCI information to the DHCT or CableCARD module in an Entitlement Control Message (ECM) that lets the DHCT or CableCARD module know whether the program is high-value or not.

**CF session**

Continuous Feed Session. Defines and allocates resources that the network uses to deliver a particular service to subscribers. A CF Session will remain intact until the DNCS operator manually tears it down.

**Channel Map**

A set of channels that specific subscribers are authorized to receive through their DHCTs.

**Clear Channel**

A service that is delivered to subscribers unscrambled or unencrypted.

**Client, MR-DVR**

A requesting DHCT in a MR-DVR network that can play back DVR-recorded programs saved on the MR-DVR server.

**cluster**

A group of servers and other resources that act like a single system and enable high availability and, in some cases, load balancing and parallel processing.

**CMTS**

Cable Modem Termination System. A device, located at the headend or a distribution hub, that provides complimentary functionality to the cable modems to enable data connectivity over a hybrid fiber coax (HFC) network.

**combo binding**

The binding process that occurs after the CableCARD module in an SSC DHCT/CableCARD module pair downloads EMMs during staging. This process occurs only if the SSC DHCT/CableCARD module pair are in the inventory file on the BFS.

**Note:** Although we recommend that you use a two-way system to stage and bind DHCTs, you can use combo binding with a one-way system.

**component video**

A video connection that splits the video signal into three parts; one for brightness and two for color.

**composite audio/video cable**

A color-coded, 3-pronged A/V cable that carries audio and video. The yellow wire carries video and the red and white wires carry right and left audio, respectively.

**composite video**

A video connection in which the brightness and color portions of the signal are combined into one signal (signal for broadcast TV).

### conditional access

An encryption/decryption process, which provides access to the broadcaster's services and ensures secure purchase transactions for interactive services.

### content QAM

A QAM that carries content

### Copy protection

A system for preventing the unauthorized reproduction of copyrighted media through setting the copy protection levels for a program or service. There are three types of copy protection settings:

- Copy freely
- Copy once (high-value)
- Copy never (high-value)

### Copy-protected content

Video and/or audio content that is coded to prevent it from being copied by recording devices, such as digital video recorders or personal computers.

### CPE

customer premise equipment. Network devices (PCs, set-top boxes) that are located at a customer site and connect to a cable modem (CM) or other access network.

### CPU

Central processing unit.

### CRC

Cyclic redundancy check. Error-checking technique.

### CRL

Certification Revocation List. A list of host devices that are not authorized to duplicate copy-protected content.

### CVT

Code Version Table. A method for staging DHCTs. The CVT is a table that contains information about download channels and information to map client release software versions to specific DHCT types. The Broadcast File Server (BFS) broadcasts this information once per second on every quadrature amplitude modulation (QAM) frequency and on the quadrature phase shift keying (QPSK) frequency. If a DHCT does not have valid client release software installed (such as new DHCTs), the DHCT searches QAM frequencies for software download information. When the DHCT finds this information, it can begin to download valid client release software.

### data bus

The bus (connections between and within the CPU, memory, and peripherals) that is used to carry data to and from a processing unit or storage device.

### data carousel

See carousel.

**data pump**

See carousel.

**data rate**

An amount of information that can be transferred per a unit of time, for example bits per second (bps).

**DAVIC**

Digital Audio Visual Council. DAVIC is becoming the industry standard for end-to-end interoperability of broadcast and interactive digital audio-visual information and of multimedia communication.

**DBDS**

Digital Broadband Delivery System. The entire network architecture of our digital system that ultimately provides signal to and from a subscriber's DHCT. The DBDS consists of five areas: sources, headend, transport network, hub, and access network.

**decoder**

A device that receives a digital signal and converts it back into an analog signal.

**decryption**

The process of decoding encrypted data into its original and understandable language.

**demodulation**

The process of decoding an analog signal into digital data.

**demodulator**

Receives information such as billing and performance monitoring data in a reverse path from the DHCT and returns it to the DNCS for processing.

**DHCT**

Digital Home Communications Terminal. Our digital set-top that is two-way capable for interactive services. See also Explorer.

**DhctInstantHit**

See instant hit.

**distinguished QAM**

A QAM that carries only system information (SI) data in band to all set-tops in a headend.

**DNCS**

Digital Network Control System. A computer server that monitors and controls the DBDS network elements; located at the DBDS headend or at a remote site.

**DOCSIS cable modem (CM)**

DOCSIS cable modem. DOCSIS CMs obtain boot configuration using DHCP, Time, and TFTP client implementations.

**DOCSIS®**

Data over cable service interface specification. This specification defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks. This standard was developed by CableLabs in North America and approved by the International Telecommunication Union (ITU).

**downstream**

The digital transmission path from the server (headend) to the subscriber.

**DTV**

Digital Television. A telecommunication system for broadcasting and receiving video and audio by means of digital signals.

**DVB**

- Short for Digital Video Broadcasting Project (DVB), DVB is an industry-led consortium of more than 260 broadcasters, manufacturers, network operators, and regulatory bodies and others in over 35 countries committed to designing global standards for the global delivery of digital television and data services.

- DVB is also the name used to describe the various European systems for television, radio and data broadcasting in all areas of the world outside of North America.

**DVB common scrambling**

Digital Video Broadcast (DVB) common scrambling. An encryption algorithm developed and supported by the DVB group used primarily in Europe.

**DVI**

Digital video interface. A multi-pin output that provides a high-resolution digital video signal to HD-compatible TVs.

**DVR**

digital video recorder. A device that records television programs without the use of videotape and saves them to a hard drive located inside the recorder. The programs can then be deleted, saved to a tape, or left on the hard drive. A DVR allows you to pause live broadcast for interruption, such as creating your own instant replays. Also known as PVR.

**EA**

Entitlement Agent. Data structures transmitted within messages having cryptographic protection that authorize reception of service to a DHCT.

**EAC**

Emergency Alert Controller. A workstation that receives and formats the Emergency Alert Message (EAM), then sends it by FTP to the Digital Network Control System (DNCS) over an Ethernet connection.

**EAM**

Emergency Alert Message. A message sent by the Federal Communications Commission (FCC), the National Weather Service, or local authorities to cable service providers who broadcast these messages to cable television subscribers. These messages include regular tests of the Emergency Alert System, as well as messages that warn of dangerous conditions such as thunderstorms, floods, tornadoes, hurricanes, and earthquakes.

**EARS**

Emergency Alert Receiver Server. A server that monitors a designated port to receive EAMs. When the EARS receives an EAM, it places the audio portion of the EAM in the /export/home/easftp directory and sends the EAM to the MMMServer.

**EAS**

Emergency Alert System. A warning system that is activated at the headend and broadcasts emergency messages to subscribers.

**EAT**

Emergency Action Termination. An event code that ends transmission of EAMs to subscribers. Used when your system does not use CableCARD modules.

**ECM**

Entitlement Control Message. System-wide information that "unlocks" an encrypted service by transmitting control words. Each ECM is unique for each service. An ECM enables cryptographic partitioning so that different Entitlement Agents (EAs) can selectively grant access to their own services.

**eCM**

Embedded cable modem.

**EMM**

Entitlement Management Message. Contains information for a specific DHCT that enables it to access secure services.

**EMTA**

Embedded MTA. A hardware device that includes both an MTA and a cable modem in the same unit.

**encoder**

A device that converts an analog signal into a digital signal.

**encrypted service**

A service that is encrypted, or scrambled, so that it is protected from being accessed (stolen) by people who have not paid for the service.

**encryption**

The process of converting plain text into a coded signal for security.

**EOM**

End of Message. An event code that ends transmission of EAMs to subscribers. Used when your system uses CableCARD modules.

**ESE**

External secure element.

**EuroDOCSIS**

The EuroDOCSIS standard was derived from the U.S. DOCSIS standard in order to ensure correct and optimal

performance of EuroDOCSIS modems and CMTSs in European networks, in addition to full compliance with the European DVB (Digital Video Broadcasting) standard in the downstream channel.

**EUT**

Entitlement unit table. A table that lists all packages and their associated sources.

**Explorer®**

Our registered trademark name for the Digital Home Communications Terminal (DHCT). Also known as a set-top box.

**FAT Channel**

See BFS.

**FCC**

Federal Communications Commission. An independent United States government agency, charged with regulating interstate and international communications by radio, television, wire, satellite and cable.

**FDC**

Forward Data Channel. Carries digital data (tuning, management, Internet, and at least two days of IPG data) in ATM cells on RF signals from the ATM switch to a router, which then forwards the data to the correct network. Also known as out-of-band data channel.

**Field-return DHCT**

A DHCT that has been removed from the subscriber's home has been returned to the cable service provider for service or repair.

**FIPS**

Federal Information Processing Standards. A series of standards issued by the U.S. National Institute of Standards and Technology (NIST) that address Federal requirements for the interoperability of different systems, for the portability of data and software, and for computer security.

**firewall**

Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network.

**flash memory (ROM)**

Nonvolatile storage that can be electrically erased and reprogrammed so that software images can be stored, booted, and rewritten as necessary.

**flash ROM**

A rewritable ROM that does not lose its information when the power turns off.

**force tuning**

The set-top service is changed without the user's control. Force Tuning may be initiated and suspended by EAS messages.

**forward path**

A physical connection from the hub to a DHCT that may support multiple analog transmission channels, digital transmission channels, and forward data channels.

**FPM**

Forward purchase message.

**frequency**

The number of times an electromagnetic wave repeats an identical unit of time, usually one second. One Hertz (Hz) is equal to one cycle per second.

**FTP**

File Transfer Protocol. A method used to exchange files between computers on a network or the Internet using the TCP/IP protocol.

**gateway**

A network component that acts as an entrance to another network.

**GBAM**

Global broadcast authenticated message. GBAMs provide a mechanism that allows IPPV purchases to be secured. The combination of tokens required to purchase specific events.

**GoQAM**

Gigabit Overlay QAM modulator. A software-modified GQAM modulator that functions on an Overlay system. A GQAM that accepts two pairs of inputs, where each pair consists of an incumbent-encrypted stream and its corresponding clear stream. See also QAM, GQAM, MQAM.

**GQAM**

gigabit quadrature amplitude modulation. A QAM that provides up to sixteen 6 MHz outputs while occupying only one unit of rack space. See also QAM, MQAM.

**HDCP**

High-bandwidth digital content protection. A type of encryption used with high-resolution signals over DVI and HDMI connections to prevent unauthorized duplication of copyrighted material.

**HDMI**

High definition media interface. A multi-pin connection port that used to transfer uncompressed digital video with HDCP copy protection, while also having the capability to transmit multi-channel audio.

**HDTV**

high-definition television. The high-resolution subset of the DTV system.

**headend**

The location of the network elements that processes the signal by receiving and preparing the source signals and making them ready for the transport network. See also network elements.

**HFC**

hybrid fiber coax. Consists of fiber optic transmission systems extending from a hub to HFC nodes, and a coax bus network extending from the HFC nodes to the DHCTs within the subscriber's home.

### high-value copy-protected service

A copy-protected service that has a copy protection setting of either copy once or copy never.

### hub

Physical locations designed to serve a specific number of subscribers, usually 50 to 15,000. May be co-located with the headend or miles away from the headend. Hubs receive, modulate, and boost the signal prior to sending it to the network of HFC nodes for distribution to the subscriber. Hubs usually contain QPSK modulators/demodulators that establish the two-way communications with the DHCTs.

### IEEE

Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.

### IEEE 1394

A high speed digital interface that is used to transmit digital audio/video data. Also known as Firewire.

### IEEE 802.11

A family of IEEE specifications for setting wireless LAN standards. Specified for 1 and 2 Megabits per second (Mbps) wireless Local Area Networks (LANs).

### IEEE-802.11b

An IEEE specification for 5.5 or 11 Megabits per second (Mbps) wireless Local Area Networks (LANs).

### IEE-802.3

An IEEE specification for SCMA/CD based Ethernet networks.

### IEEE-802.x

The set of specifications for local area networks (LAN) from the Institute of Electrical and Electronics Engineers (IEEE).

### inband

Interactive content sent as part of a broadcasted data stream (like MPEG-2).

### instant hit

A transaction from the DNCS or billing system that initiates the transmission of all existing EMMs to the device being staged.

### Internet Protocol

The standard protocol within TCP/IP that defines the basic unit of information passed across an Internet connection by breaking down data messages into packets, routing and transporting the packets over network connections, then reassembling the packets at their destination.

### interstitial

Programming that appears on PPV channels between events, such as general programming or an advertisement.

**IP**

See Internet Protocol.

**IP address**

A 32-bit sequence of numbers used for routing IP data. Each IP address identifies a specific component on a specific network. The address contains a network address identifier and a host identifier.

**IP multicast**

Routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination group address.

**IPG**

Interactive Program Guide. Our name for the on-screen program guide provided by the Explorer DHCT.

**IPPV**

impulse pay-per-view. Service for which cable subscribers can electronically order program events using two-way (or reverse path) methods. Subscribers are charged a user fee for individual program events. See also PPV.

**IRD**

Integrated Receiver Decoder. A satellite receiver that also demodulates and decodes digital signals from a satellite and outputs a "clear" decrypted MPEG-2 data channel.

**IRT**

Integrated Receiver Transcoder. A depopulator and decoder combination that receives a digital signal from a satellite and outputs a "clear" decrypted MPEG-2 data stream.

**ISP**

Internet Service Provider. An organization offering and providing Internet access to the public using computer servers connected directly to the Internet.

**LAN**

Local Area Network. High-speed, low-error data network covering a relatively small geographic area that connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.

**LCD**

Liquid crystal display. An alphanumeric display using liquid crystals sealed between two pieces of glass.

**LED**

light-emitting diode. Semiconductor device that converts electrical energy into light. Status lights on hardware devices are typically LEDs.

**M-Card Module**

Multi-Stream CableCARD Module. The next generation CableCARD module that supports decryption of up to six

programs and also provides two-way network access in both DAVIC and DOCSIS systems.

**MAC address**

Media Access Control address. A unique physical address embedded into a network device. Similar to a serial number.

**manual binding**

Adding the CableCARD module ID and host ID to the DNCS through the CableCARD interface on the DNCS so that the CableCARD module can receive "high-value" copy-protected services (services with copy-protection settings of either copy once or copy never).

**MMM Server**

Multi-Media Message Server. Relays the EAM TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer.

**modem**

A "modulation/demodulation" device that converts digital data, which is the data used by computers, to the analog format of data which is the type of data transmitted over phone lines.

**modulator**

A device that sends control and authorization information from the DNCS to the DHCT.

**MPEG**

Moving Picture Experts Group. An international video compression standards-setting group working under the supervision of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). MPEG's mission is to develop standards for compressed full-motion video, still image, audio and other associated information.

**MPEG-1**

A bit stream standard for compressed video and audio optimized to fit into a bandwidth of 1.5 Mbps.

**MPEG-2**

Intended for higher quality video-on-demand applications and runs at data rates between 4 and 9 Mbps.

**MPEG-4**

A low-bit-rate compression algorithm intended for 64-kbps connections.

**MQAM**

Multiple Quadrature Amplitude Modulation. A QAM that provides up to four 6 MHz outputs while occupying only one unit of rack space. See also QAM, GQAM.

**MSO**

multiple system operator. A cable company that operates more than one cable system.

**MTBF**

mean time between failure.

**multicast**

Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the destination address.

**multicast address**

Single address that refers to multiple network devices.

**multicast group**

Dynamically determined group of IP hosts identified by a single IP multicast address.

**multiplexing**

Scheme that allows multiple logical signals to be transmitted simultaneously across a single physical channel.

**NAT**

Network address translation. The translation of an Internet Protocol (IP) address used within one network to a different IP address known within another network.

**NDS M-Card**

An NDS M-Card is an M-Card that uses NDS-based encryption.

**network elements**

Devices typically located at the headend, which include satellite receivers (IRT, IRD), Real-Time Encoder (RTE), BIG, QAM modulator, DNCS, and the application server. Also known as system components.

**NVM**

non-volatile memory. Memory that holds its content when the device it is associated with is turned off.

**OCAP**

OpenCable Application Platform. The US cable industry's middleware standard specified by CableLabs.

**on-demand session**

A tangible service, such a movies, that the on-demand network delivers to the subscriber. As the on-demand network matures, the on-demand sessions or MPEG programs routed through the network will broaden to offer services such as music, video teleconferencing, Internet information, and time-shifted TV, including HDTV.

**OOB**

Out-Of-Band. See FDC.

**OSM**

Operating System Manager. A method for staging DHCTs. In the OSM method, the DHCT receives System Information (SI) and a type-specific user-to-network configuration (UN-Config) message, which includes a table of contents (TOC) file, from the DNCS. The DHCT reads the contents of the TOC file and compares the checksums of the currently loaded image files against the file information in the TOC file.

**Radio Frequency**

Logical grouping of information that includes a header containing control information and (usually) user data.

**PAL**

Phase alternation line. TV system used in most of Europe in which the color carrier phase definition changes in alternate scan lines. Utilizes an 8 MHz-wide modulated sign.

**PAT**

program association table. A second table in the transport stream which contains a list of all MPEG programs on the transport stream along with their associated program numbers.

**PCR**

program clock reference.

**PID**

packet/program identifier. A number assigned to MPEG transport packets to identify the contents of the data and the information stream to which they belong. The 13-bit PID number is assigned in the MPEG-2 transport packet headers. All packets from the same stream have the same PID number.

**PIN**

personal identification number. A password used for identification.

**PIP**

Picture-in-Picture. Allows you to watch more than one TV program (channel) at the same time on television sets or other devices. With PIP feature of TV, one program will be displayed on the entire TV screen, and another program or programs will be displayed in individual smaller squares on the screen.

**PMT**

program map table.

**POD Module**

Point-of-Deployment module. Approximately the size of a credit card and inserts into a host device (either a DHCT or cable-ready television) to provide conditional access to secure digital content. See also CableCARD, M-CARD.

**POST**

Power on self test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

**PowerKEY® Conditional Access system**

Our registered trademark name for the hardware and software encryption and decryption of digital signal. Uses secret key, public key, and private key data to secure the digital signal.

**PowerTV**

Our registered trademark name for the operating system software and integrated circuits created for high-speed processing and presentation of interactive graphics and audio for the DHCT.

**PPV**

pay-per-view. Service for which subscribers are charged a user fee for individual program events. See also IPPV.

**provision**

The process of preparing a device or service so that the DNCS/ISDS recognizes the device, which allows the device to operate properly.

**PVR**

See DVR.

**QAM modulator**

A device that uses QAM techniques to modulate a digital signal onto an HFC network to deliver voice, video, and data to a DHCT.

**QPSK modulator/demodulator**

The QPSK modulator works with the QPSK demodulator and the DHCT to provide forward signaling and a reverse communications path for interactive video and data services. The QPSK modulator and demodulator convert digital bit streams to RF format and RF signals to digital bits, respectively.

**RAM**

Random access memory. Volatile memory that can be read and written by a microprocessor.

**revoked**

Condition in which a host device cannot be authorized to copy copy-protected services.

**RF**

radio frequency. The range of electromagnetic frequencies above the audio range and below infrared light. Most wireless transmission uses RF, including radio, TV, satellites, portable phones, cellular phones, and wireless networks.

**RJ-45**

Registered jack-45. A serial connector used to hook up computers to local area networks (LANs).

**RMA DHCT**

Return Material Authorization DHCT. A DHCT that the service provider has received back from factory repair.

**RMT**

Required Monthly Test. The FCC requires operators of cable television stations to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

**router**

A device that routes data through a packet-switched network, such as the Internet, from one LAN or WAN to another, or from a LAN to the Internet.

**RWT**

Required Weekly Test. The FCC requires operators of cable television stations to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

**S-CARD**

Single-Stream CableCARD. See also CableCARD, M-CARD, POD Module.

**S-Video**

A video connection that carries the brightness and color portions of a video signal in separate streams for improved color accuracy and reduced distortion.

**SAM**

Service Application Manager. Associates a specific service with an application that defines the medium to be used for that service, such as the World Wide Web. The SAM maintains the application in a specific directory to be used when needed by the DHCTs.

**SAP**

Second audio program. This feature allows cable service providers to offer subscribers a second audio option for their programming. The other option may be a different language or another audio track, such as the weather or a sports event.

**SARA**

SA Resident Application. The set of operating programs that is "permanently" loaded into the DHCT. These programs are immediately available to the subscriber upon activation of the DHCT.

**SCS MQAM Modulator**

Simulcrypt Synchronizer MQAM Modulator

**SDI**

Serial digital interface.

**SDTV**

Standard definition TV. Digital television format that includes 480-line resolution in both interlaced (480i) and progressively scanned (480p) formats.

**SDV**

Switched Digital Video. SDV is a technology that allows cable operators to recover bandwidth from infrequently-viewed channels, by making these channels "on-demand." Instead of sending all channels to the set-tops, lightly viewed channels are put into a switching pool and are only sent to the set-tops when viewers tune to them.

**Service Disconnect feature**

The process of disabling a DHCT so that it cannot be used to view cable services. Also known as Brick mode.

**service gateway**

Front-end gateway for the delivery of service through the DBDS. Provides DSM-CC signaling as required to establish network resource for service delivery.

**service group**

A QAM modulator (or a cluster of QAMs) that is installed for delivering on-demand services to an associated

population of DHCTs. The association of a DHCT to a specific service group is determined by first identifying the QAM modulator (or a cluster of QAMs) that a DHCT can receive.

**sessions**

Logical elements that define and allocate the resources that the network uses to deliver source content.

**shared key authentication**

A type of authentication that assumes each station has received a secret shared key through a secure channel independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of Shared Key authentication requires implementation of the 802.11 Wireless Equivalent Privacy algorithm.

**SI**

system information. A standard set of tables providing the data necessary for a navigation device to discover and access services.

**SMTA**

Standalone MTA. A hardware device that contains an MTA but does not include a DOCSIS modem or other transport. Typically connected to a cable modem through an Ethernet connection.

**SNMP**

Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

**SONET**

Synchronous Optical Network. An optical fiber network capable of transmitting ATM data packets over long distances. This data remains in a digital state and can be repeated indefinitely.

**source**

In the DBDS, a source is the actual program or data that is made available to the DHCT as a service to the subscriber. Sources can include: MPEG-2 digital broadcast services that are non-secure, non-encrypted, audio/video programs; Internet connections from an Internet service provider (ISP); Digital PPVs that are secure, encrypted, digital MPEG-2 programs; Digital music services; Analog programs that are modulated in the traditional format or converted into MPEG-2 format.

**spatial reuse**

Reusing the same frequencies for different fiber nodes or branches on the HFC network. This means that a node or group of distribution nodes use one set of QAM transmitters for a service group, and other nodes or groups of nodes use a different service group, but all use the same set of narrowcast frequencies.

**SR**

System Release. Our software release package for components of the DBDS.

**SSID**

Service Set Identifier. A group name shared by every member of a wireless network in which client PCs with the same SSID are allowed to establish a connection.

**staging**

The process of loading the necessary software and security information into the Explorer DHCT prior to deployment in subscriber's homes.

**subnet mask**

32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.

**subscriber**

A household or business that legally receives and pays for cable and/or pay television service for its own use.

**switched digital video**

See SDV.

**tar**

Short for tape archive, a UNIX utility that combines a group of files into a single file with a .tar extension.

**TCP/IP**

Transmission Control Protocol/Internet Protocol. An Internet working protocol that provides reliable data transport using connection-oriented techniques.

**TOC**

Table of contents. A file that lists the files included in the OSM EMM transfer.

**transport network**

Provides the communication link enabling audio, video, and data to be transported from the headend to the hub. It involves a network of switching and transmission equipment and can include AM fiber and SONET technologies.

**transport stream**

A data communications signal that is formatted in accordance with the protocol defined in the MPEG-2 specification ISO IEC 13818. An MPEG transport stream can carry voice, video, or data information. The MPEG data transmission protocol transports real-time data.

**UN-Config**

User-to-network configuration. A message sent from the DNCS that configures the DHCT.

**unicast**

Message sent to a single network destination.

**unicast address**

Address specifying a single network device.

**UNIX**

An operating system that is less computer/server-specific than other operating systems. UNIX is widely used in the telecommunications industry and by the Internet.

**upstream**

The transmission path from the subscriber to the headend.

**USB**

universal serial bus. A port on a PC or other device that provides connection to peripherals, such as CD-ROM drives, printers, modems, and keyboards.

**VASP**

Value-added service provider.

**VBI**

Vertical blanking interval.

**VCS**

Virtual channel service.

**VOD**

video-on-demand. The ability of a subscriber to select a program event and watch it within moments of selection. VOD allows pausing and rewinding of the event.

**VoIP**

Voice-over-Internet-Protocol. These services are a provision of voice telephony through the use of packet-switched networks running Internet Protocol (IP) networks rather than traditional circuit switching.

**WAN**

Wide Area Network. A network that interconnects geographically distributed computers or local area networks.

**xOD**

anything-On-Demand. Combines two on-demand delivery mechanisms, VOD and SVOD, into one application.

**10BASE-T**

An IEEE standard (802.3) for operating 10 Mbps Ethernet networks (LANs) using two pairs of twisted-pair cabling: one pair for transmitting data and the other for receiving data.

**access network**

An HFC network consisting of a fiber optic transmission system extending from a hub to the HFC nodes, and a coax bus network extending from the HFC nodes to the DHCTs within the subscriber's homes.

**access point**

An interface between the wireless network and a wired network. Access points combined with Ethernet support the creation of multiple radio cells that enable roaming.

### Advanced DSG

Advanced DOCSIS Set-top Gateway. Operates with the DCD message. Address assignment is dynamic. The DSG tunnel address is determined by the DSG agent and learned by the DSG client through the DSG address table in the DCD message.

**analog**

A format in which information is transmitted by modulating a continuous transmission signal, such as amplifying the strength of a signal or varying its frequency.

**API**

Application Program Interface. A set of protocols, routines, and tools for building software applications. An interface that enables programs to communicate with each other.

### Application Server

A computer workstation and server used to execute the application programs, which provide an interface for downloading application data to the DHCTs. The AppServer works in conjunction with the DNCS and the two computers share a common database.

### AppServer

See Application Server.

**ASI**

Application Services Interface. A DVB standard for the transfer of MPEG transport streams.

**authentication**

A method in which the network requires a user to identify themselves by entering a user name and password.

**authorization**

The process of granting or denying access to specific resources.

**authorized service domain**

In the authorized service domain (ASD), content is secured using the mechanisms available through the operator's conditional access system.

The authorized service domain (ASD) physically translates into a collection of one or more trusted devices where content may be securely stored and moved within the domain (typically the subscriber's home).

The distinction between the authorized service domain and other forms of copy protection (for example, DTCP) is that the content remains under operator control at all times with ASD. The control points within the domain are the M-Cards supplied by the operator. Consider the authorized service domain as the operator's digital rights management (DRM) system and an extension of the operator's conditional access (CA) system.

**autobinding**

A process that binds a CableCARD module and host when the CableCARD module is inserted into the host. Autobinding is available for two-way hosts only if all of the following conditions are met:

- The DNCS is set up for autobinding.
- The CableCARD module and host are staged in a two-way environment.

  **Note:** To use autobinding, the CableCARD module and host must be staged in a two-way environment. Once staged and bound, they can be used in a one-way environment.

- The host is not on the certificate revocation list (CRL).

**AVFS**

Audio/video file system.

**backbone**

The part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.

**bandwidth**

The maximum data carrying capacity of a transmission link. For networks, bandwidth is usually expressed in bits per second (bps).

**BER**

Bit error rate. Ratio of received bits that contain errors.

**BFS**

Broadcast File System. The primary interface (means of communication) between the AppServer and the DHCTs that are connected to the network.

**BFS BIG**

Broadcast File System Broadband Integrated Gateway. A device that processes the data it receives and sends it to the data QAM modulator.

**BFS QAM**

A QAM that carries BFS (broadcast file system) data to all set-tops in the headend. A BFS QAM can also carry in-band system information (SI) to all set-tops in a headend. However, when a single QAM is used to carry only SI, it is referred to as a distinguished QAM.

**BIG**

Broadband Integrated Gateway. A device that provides a data pipeline from the DNCS to the DHCTs.

**bind**

A DNCS function that matches the CableCARD module's ID to its host's ID to ensure that the host device conforms to the copy-protection rules defined by the Copy Control Information (CCI). You must bind a CableCARD module to its host before the host can receive high-value copy-protected services.

**bit rate**

The number of bits of information that can be transmitted over a channel in a given second (usually express in bits per second [bps]).

**boot**

The loading of the operating system (OS) and application programs into the main memory or random access memory (RAM) of the system.

**Bootloader**

A factory program installed into the DHCTs to ensure reliable upgrades.

**BOSS**

Business Operations Support System. Open Network Computing RPC protocol for sending requests and responses. It is used by the Billing System to interface to the DNCS and is one of the DNCS/ISDS interfaces for communication with SMS hosts. All BOSS requests are processed by the BOSS server and routed to the proper DNCS/ISDS component.

### BOSS Server

Provides a mechanism for the routing of a BOSS requests to and from the appropriate DNCS/ISDS component and the BOSS client that initiated the request. Also provides a mechanism for the routing of a BASS request to and from the appropriate Application Server and the BASS client that initiated the request.

**bounce**

Stop and restart a network element or process. For example, to bounce the osm process means to stop and restart the process.

**bps**

Bits per second.

**brick mode**

A state in which the DHCT is not authorized to receive services. Provided by a package which stops all functions of the DHCT, including the ability for it to turn on. Also called service disconnect.

**bridge**

Device that connects and passes packets between two network segments that use the same communications protocol.

**broadband**

A characteristic of a network that indicates that a wide band of frequencies is available. A large amount of information can be carried by multiplexing and transmitting on many different frequencies simultaneously. Sometimes used more narrowly to describe cable modem service or DSL (digital subscriber line) service from a telephone company.

**broadcast address**

A unique address reserved for sending a message to all receiving stations.

**broadcast flag**

A technology that sends a message to copying devices not to allow unauthorized copying or distribution via networking devices such as connected Digital Video Recorders.

**broadcast server**

A server that delivers interactive content and broadcast data feeds. It uses Internet Protocol (IP) to encode and deliver data over networks that support IP Multicast.

**broadcast-only mode**

A state in which a DHCT has not established an interactive communications path, and only receives broadcast and CA traffic. Advanced services (digital broadcast, IPG, PPV) are available to the DHCT in this mode, but IPPV polling and interactive data services do not function.

**bsm**

Broadcast Segment Manager. The Broadcast Segment Manager is responsible for fielding broadcast segment definitions. It also receives notifications from the SI Manager when broadcast sources start, and forwards those notifications to the Conditional Access Subsystem.

**BTSC**

Broadcast Televisions Standard Committee.

## CA

See Conditional Access.

**CableCARD**

A device that plugs into a digital cable-ready TV or DHCT and allows the receipt of encrypted services.

**CableLabs**

Cable Television Laboratories. A research consortium sponsored by cable television operators.

## CAQAM

Conditional access quadrature amplitude modulator. See also QAM, GQAM, MQAM.

**carousel**

Transports data modules and application server processes from the BFS server to the DHCT. For each new application server process that registers with the BFS, a new data carousel is created and the ID information is updated in the BFS directory structure. Also known as Data Carousel or Data Pump.

## CCI (Copy Control Information)

Copy Control Information defines a program's level of copy protection. There are currently three copy protection levels defined: copy freely, copy once, and copy never (copy once and copy never are known as high-value copy protection). The CCI is set for the program by the program originator.

The DNCS/ISDS sends the CCI information to the DHCT or CableCARD module in an Entitlement Control Message (ECM) that lets the DHCT or CableCARD module know whether the program is high-value or not.

**CF session**

Continuous Feed Session. Defines and allocates resources that the network uses to deliver a particular service to subscribers. A CF Session will remain intact until the DNCS operator manually tears it down.

**Channel Map**

A set of channels that specific subscribers are authorized to receive through their DHCTs.

**Clear Channel**

A service that is delivered to subscribers unscrambled or unencrypted.

### Client, MR-DVR

A requesting DHCT in a MR-DVR network that can play back DVR-recorded programs saved on the MR-DVR server.

**cluster**

A group of servers and other resources that act like a single system and enable high availability and, in some cases, load balancing and parallel processing.

**CMTS**

Cable Modem Termination System. A device, located at the headend or a distribution hub, that provides complimentary functionality to the cable modems to enable data connectivity over a hybrid fiber coax (HFC) network.

**combo binding**

The binding process that occurs after the CableCARD module in an SSC DHCT/CableCARD module pair downloads EMMs during staging. This process occurs only if the SSC DHCT/CableCARD module pair are in the inventory file on the BFS.

**Note:** Although we recommend that you use a two-way system to stage and bind DHCTs, you can use combo binding with a one-way system.

**component video**

A video connection that splits the video signal into three parts; one for brightness and two for color.

**composite audio/video cable**

A color-coded, 3-pronged A/V cable that carries audio and video. The yellow wire carries video and the red and white wires carry right and left audio, respectively.

**composite video**

A video connection in which the brightness and color portions of the signal are combined into one signal (signal for broadcast TV).

**conditional access**

An encryption/decryption process, which provides access to the broadcaster's services and ensures secure purchase transactions for interactive services.

**content QAM**

A QAM that carries content

## Copy protection

A system for preventing the unauthorized reproduction of copyrighted media through setting the copy protection levels for a program or service. There are three types of copy protection settings:

- Copy freely
- Copy once (high-value)
- Copy never (high-value)

### Copy-protected content

Video and/or audio content that is coded to prevent it from being copied by recording devices, such as digital video recorders or personal computers.

**CPE**

customer premise equipment. Network devices (PCs, set-top boxes) that are located at a customer site and connect to a cable modem (CM) or other access network.

**CPU**

Central processing unit.

**CRC**

Cyclic redundancy check. Error-checking technique.

**CRL**

Certification Revocation List. A list of host devices that are not authorized to duplicate copy-protected content.

## CVT

Code Version Table. A method for staging DHCTs. The CVT is a table that contains information about download channels and information to map client release software versions to specific DHCT types. The Broadcast File Server (BFS) broadcasts this information once per second on every quadrature amplitude modulation (QAM) frequency and on the quadrature phase shift keying (QPSK) frequency. If a DHCT does not have valid client release software installed (such as new DHCTs), the DHCT searches QAM frequencies for software download information. When the DHCT finds this information, it can begin to download valid client release software.

**data bus**

The bus (connections between and within the CPU, memory, and peripherals) that is used to carry data to and from a processing unit or storage device.

**data carousel**

See carousel.

**data pump**

See carousel.

**data rate**

An amount of information that can be transferred per a unit of time, for example bits per second (bps).

**DAVIC**

Digital Audio Visual Council. DAVIC is becoming the industry standard for end-to-end interoperability of broadcast and interactive digital audio-visual information and of multimedia communication.

**DBDS**

Digital Broadband Delivery System. The entire network architecture of our digital system that ultimately provides signal to and from a subscriber's DHCT. The DBDS consists of five areas: sources, headend, transport network, hub, and access network.

**decoder**

A device that receives a digital signal and converts it back into an analog signal.

**decryption**

The process of decoding encrypted data into its original and understandable language.

**demodulation**

The process of decoding an analog signal into digital data.

**demodulator**

Receives information such as billing and performance monitoring data in a reverse path from the DHCT and returns it to the DNCS for processing.

**DHCT**

Digital Home Communications Terminal. Our digital set-top that is two-way capable for interactive services. See also Explorer.

**DhctInstantHit**

See instant hit.

**distinguished QAM**

A QAM that carries only system information (SI) data in band to all set-tops in a headend.

**DNCS**

Digital Network Control System. A computer server that monitors and controls the DBDS network elements; located at the DBDS headend or at a remote site.

**DOCSIS cable modem (CM)**

DOCSIS cable modem. DOCSIS CMs obtain boot configuration using DHCP, Time, and TFTP client implementations.

**DOCSIS®**

Data over cable service interface specification. This specification defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks. This standard was developed by CableLabs in North America and approved by the International Telecommunication Union (ITU).

**downstream**

The digital transmission path from the server (headend) to the subscriber.

**DTV**

Digital Television. A telecommunication system for broadcasting and receiving video and audio by means of digital signals.

## DVB

- Short for Digital Video Broadcasting Project (DVB), DVB is an industry-led consortium of more than 260 broadcasters, manufacturers, network operators, and regulatory bodies and others in over 35 countries committed to designing global standards for the global delivery of digital television and data services.

- DVB is also the name used to describe the various European systems for television, radio and data broadcasting in all areas of the world outside of North America.

### DVB common scrambling

Digital Video Broadcast (DVB) common scrambling. An encryption algorithm developed and supported by the DVB group used primarily in Europe.

**DVI**

Digital video interface. A multi-pin output that provides a high-resolution digital video signal to HD-compatible TVs.

**DVR**

digital video recorder. A device that records television programs without the use of videotape and saves them to a hard drive located inside the recorder. The programs can then be deleted, saved to a tape, or left on the hard drive. A DVR allows you to pause live broadcast for interruption, such as creating your own instant replays. Also known as PVR.

**EA**

Entitlement Agent. Data structures transmitted within messages having cryptographic protection that authorize reception of service to a DHCT.

**EAC**

Emergency Alert Controller. A workstation that receives and formats the Emergency Alert Message (EAM), then sends it by FTP to the Digital Network Control System (DNCS) over an Ethernet connection.

## EAM

Emergency Alert Message. A message sent by the Federal Communications Commission (FCC), the National Weather Service, or local authorities to cable service providers who broadcast these messages to cable television subscribers. These messages include regular tests of the Emergency Alert System, as well as messages that warn of dangerous conditions such as thunderstorms, floods, tornadoes, hurricanes, and earthquakes.

## EARS

Emergency Alert Receiver Server. A server that monitors a designated port to receive EAMs. When the EARS receives an EAM, it places the audio portion of the EAM in the /export/home/easftp directory and sends the EAM to the MMMServer.

**EAS**

Emergency Alert System. A warning system that is activated at the headend and broadcasts emergency messages to subscribers.

## EAT

Emergency Action Termination. An event code that ends transmission of EAMs to subscribers. Used when your system does not use CableCARD modules.

**ECM**

Entitlement Control Message. System-wide information that "unlocks" an encrypted service by transmitting control words. Each ECM is unique for each service. An ECM enables cryptographic partitioning so that different Entitlement Agents (EAs) can selectively grant access to their own services.

**eCM**

Embedded cable modem.

**EMM**

Entitlement Management Message. Contains information for a specific DHCT that enables it to access secure services.

**EMTA**

Embedded MTA. A hardware device that includes both an MTA and a cable modem in the same unit.

**encoder**

A device that converts an analog signal into a digital signal.

**encrypted service**

A service that is encrypted, or scrambled, so that it is protected from being accessed (stolen) by people who have not paid for the service.

**encryption**

The process of converting plain text into a coded signal for security.

**EOM**

End of Message. An event code that ends transmission of EAMs to subscribers. Used when your system uses CableCARD modules.

**ESE**

External secure element.

## EuroDOCSIS

The EuroDOCSIS standard was derived from the U.S. DOCSIS standard in order to ensure correct and optimal performance of EuroDOCSIS modems and CMTSs in European networks, in addition to full compliance with the European DVB (Digital Video Broadcasting) standard in the downstream channel.

## EUT

Entitlement unit table. A table that lists all packages and their associated sources.

**Explorer®**

Our registered trademark name for the Digital Home Communications Terminal (DHCT). Also known as a set-top box.

**FAT Channel**

See BFS.

**FCC**

Federal Communications Commission. An independent United States government agency, charged with regulating interstate and international communications by radio, television, wire, satellite and cable.

**FDC**

Forward Data Channel. Carries digital data (tuning, management, Internet, and at least two days of IPG data) in ATM cells on RF signals from the ATM switch to a router, which then forwards the data to the correct network. Also known as out-of-band data channel.

**Field-return DHCT**

A DHCT that has been removed from the subscriber's home has been returned to the cable service provider for service or repair.

**FIPS**

Federal Information Processing Standards. A series of standards issued by the U.S. National Institute of Standards and Technology (NIST) that address Federal requirements for the interoperability of different systems, for the portability of data and software, and for computer security.

**firewall**

Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network.

**flash memory (ROM)**

Nonvolatile storage that can be electrically erased and reprogrammed so that software images can be stored, booted, and rewritten as necessary.

**flash ROM**

A rewritable ROM that does not lose its information when the power turns off.

**force tuning**

The set-top service is changed without the user's control. Force Tuning may be initiated and suspended by EAS messages.

**forward path**

A physical connection from the hub to a DHCT that may support multiple analog transmission channels, digital transmission channels, and forward data channels.

## FPM

Forward purchase message.

**frequency**

The number of times an electromagnetic wave repeats an identical unit of time, usually one second. One Hertz (Hz) is equal to one cycle per second.

**FTP**

File Transfer Protocol. A method used to exchange files between computers on a network or the Internet using the TCP/IP protocol.

**gateway**

A network component that acts as an entrance to another network.

**GBAM**

Global broadcast authenticated message. GBAMs provide a mechanism that allows IPPV purchases to be secured. The combination of tokens required to purchase specific events.

**GoQAM**

Gigabit Overlay QAM modulator. A software-modified GQAM modulator that functions on an Overlay system. A GQAM that accepts two pairs of inputs, where each pair consists of an incumbent-encrypted stream and its corresponding clear stream. See also QAM, GQAM, MQAM.

**GQAM**

gigabit quadrature amplitude modulation. A QAM that provides up to sixteen 6 MHz outputs while occupying only one unit of rack space. See also QAM, MQAM.

**HDCP**

High-bandwidth digital content protection. A type of encryption used with high-resolution signals over DVI and HDMI connections to prevent unauthorized duplication of copyrighted material.

**HDMI**

High definition media interface. A multi-pin connection port that used to transfer uncompressed digital video with HDCP copy protection, while also having the capability to transmit multi-channel audio.

**HDTV**

high-definition television. The high-resolution subset of the DTV system.

**headend**

The location of the network elements that processes the signal by receiving and preparing the source signals and making them ready for the transport network. See also network elements.

**HFC**

hybrid fiber coax. Consists of fiber optic transmission systems extending from a hub to HFC nodes, and a coax bus network extending from the HFC nodes to the DHCTs within the subscriber's home.

### high-value copy-protected service

A copy-protected service that has a copy protection setting of either copy once or copy never.

**hub**

Physical locations designed to serve a specific number of subscribers, usually 50 to 15,000. May be co-located with the headend or miles away from the headend. Hubs receive, modulate, and boost the signal prior to sending it to the network of HFC nodes for distribution to the subscriber. Hubs usually contain QPSK modulators/demodulators that establish the two-way communications with the DHCTs.

**IEEE**

Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.

**IEEE 1394**

A high speed digital interface that is used to transmit digital audio/video data. Also known as Firewire.

### IEEE 802.11

A family of IEEE specifications for setting wireless LAN standards. Specified for 1 and 2 Megabits per second (Mbps) wireless Local Area Networks (LANs).

### IEEE-802.11b

An IEEE specification for 5.5 or 11 Megabits per second (Mbps) wireless Local Area Networks (LANs).

**IEE-802.3**

An IEEE specification for SCMA/CD based Ethernet networks.

**IEEE-802.x**

The set of specifications for local area networks (LAN) from the Institute of Electrical and Electronics Engineers (IEEE).

**inband**

Interactive content sent as part of a broadcasted data stream (like MPEG-2).

**instant hit**

A transaction from the DNCS or billing system that initiates the transmission of all existing EMMs to the device being staged.

**Internet Protocol**

The standard protocol within TCP/IP that defines the basic unit of information passed across an Internet connection by breaking down data messages into packets, routing and transporting the packets over network connections, then reassembling the packets at their destination.

**interstitial**

Programming that appears on PPV channels between events, such as general programming or an advertisement.

**IP**

See Internet Protocol.

### IP address

A 32-bit sequence of numbers used for routing IP data. Each IP address identifies a specific component on a specific network. The address contains a network address identifier and a host identifier.

### IP multicast

Routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination group address.

**IPG**

Interactive Program Guide. Our name for the on-screen program guide provided by the Explorer DHCT.

**IPPV**

impulse pay-per-view. Service for which cable subscribers can electronically order program events using two-way (or reverse path) methods. Subscribers are charged a user fee for individual program events. See also PPV.

**IRD**

Integrated Receiver Decoder. A satellite receiver that also demodulates and decodes digital signals from a satellite and outputs a "clear" decrypted MPEG-2 data channel.

**IRT**

Integrated Receiver Transcoder. A depopulator and decoder combination that receives a digital signal from a satellite and outputs a "clear" decrypted MPEG-2 data stream.

**ISP**

Internet Service Provider. An organization offering and providing Internet access to the public using computer servers connected directly to the Internet.

## LAN

Local Area Network. High-speed, low-error data network covering a relatively small geographic area that connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.

**LCD**

Liquid crystal display. An alphanumeric display using liquid crystals sealed between two pieces of glass.

**LED**

light-emitting diode. Semiconductor device that converts electrical energy into light. Status lights on hardware devices are typically LEDs.

### M-Card Module

Multi-Stream CableCARD Module. The next generation CableCARD module that supports decryption of up to six programs and also provides two-way network access in both DAVIC and DOCSIS systems.

### MAC address

Media Access Control address. A unique physical address embedded into a network device. Similar to a serial number.

**manual binding**

Adding the CableCARD module ID and host ID to the DNCS through the CableCARD interface on the DNCS so that the CableCARD module can receive "high-value" copy-protected services (services with copy-protection settings of either copy once or copy never).

### MMM Server

Multi-Media Message Server. Relays the EAM TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer.

**modem**

A "modulation/demodulation" device that converts digital data, which is the data used by computers, to the analog format of data which is the type of data transmitted over phone lines.

**modulator**

A device that sends control and authorization information from the DNCS to the DHCT.

**MPEG**

Moving Picture Experts Group. An international video compression standards-setting group working under the supervision of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). MPEG's mission is to develop standards for compressed full-motion video, still image, audio and other associated information.

**MPEG-1**

A bit stream standard for compressed video and audio optimized to fit into a bandwidth of 1.5 Mbps.

**MPEG-2**

Intended for higher quality video-on-demand applications and runs at data rates between 4 and 9 Mbps.

**MPEG-4**

A low-bit-rate compression algorithm intended for 64-kbps connections.

**MQAM**

Multiple Quadrature Amplitude Modulation. A QAM that provides up to four 6 MHz outputs while occupying only one unit of rack space. See also QAM, GQAM.

**MSO**

multiple system operator. A cable company that operates more than one cable system.

**MTBF**

mean time between failure.

**multicast**

Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the destination address.

**multicast address**

Single address that refers to multiple network devices.

**multicast group**

Dynamically determined group of IP hosts identified by a single IP multicast address.

**multiplexing**

Scheme that allows multiple logical signals to be transmitted simultaneously across a single physical channel.

**NAT**

Network address translation. The translation of an Internet Protocol (IP) address used within one network to a different IP address known within another network.

### NDS M-Card

An NDS M-Card is an M-Card that uses NDS-based encryption.

**network elements**

Devices typically located at the headend, which include satellite receivers (IRT, IRD), Real-Time Encoder (RTE), BIG, QAM modulator, DNCS, and the application server. Also known as system components.

**NVM**

non-volatile memory. Memory that holds its content when the device it is associated with is turned off.

**OCAP**

OpenCable Application Platform. The US cable industry's middleware standard specified by CableLabs.

**on-demand session**

A tangible service, such a movies, that the on-demand network delivers to the subscriber. As the on-demand network matures, the on-demand sessions or MPEG programs routed through the network will broaden to offer services such as music, video teleconferencing, Internet information, and time-shifted TV, including HDTV.

**OOB**

Out-Of-Band. See FDC.

**OSM**

Operating System Manager. A method for staging DHCTs. In the OSM method, the DHCT receives System Information (SI) and a type-specific user-to-network configuration (UN-Config) message, which includes a table of contents (TOC) file, from the DNCS. The DHCT reads the contents of the TOC file and compares the checksums of the currently loaded image files against the file information in the TOC file.

**Radio Frequency**

Logical grouping of information that includes a header containing control information and (usually) user data.

## PAL

Phase alternation line. TV system used in most of Europe in which the color carrier phase definition changes in alternate scan lines. Utilizes an 8 MHz-wide modulated sign.

**PAT**

program association table. A second table in the transport stream which contains a list of all MPEG programs on the transport stream along with their associated program numbers.

**PCR**

program clock reference.

**PID**

packet/program identifier. A number assigned to MPEG transport packets to identify the contents of the data and the information stream to which they belong. The 13-bit PID number is assigned in the MPEG-2 transport packet headers. All packets from the same stream have the same PID number.

**PIN**

personal identification number. A password used for identification.

**PIP**

Picture-in-Picture. Allows you to watch more than one TV program (channel) at the same time on television sets or other devices. With PIP feature of TV, one program will be displayed on the entire TV screen, and another program or programs will be displayed in individual smaller squares on the screen.

**PMT**

program map table.

**POD Module**

Point-of-Deployment module. Approximately the size of a credit card and inserts into a host device (either a DHCT or cable-ready television) to provide conditional access to secure digital content. See also CableCARD, M-CARD.

**POST**

Power on self test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

**PowerKEY® Conditional Access system**

Our registered trademark name for the hardware and software encryption and decryption of digital signal. Uses secret key, public key, and private key data to secure the digital signal.

**PowerTV**

Our registered trademark name for the operating system software and integrated circuits created for high-speed processing and presentation of interactive graphics and audio for the DHCT.

**PPV**

pay-per-view. Service for which subscribers are charged a user fee for individual program events. See also IPPV.

**provision**

The process of preparing a device or service so that the DNCS/ISDS recognizes the device, which allows the device to operate properly.

## PVR

See DVR.

### QAM modulator

A device that uses QAM techniques to modulate a digital signal onto an HFC network to deliver voice, video, and data to a DHCT.

### QPSK modulator/demodulator

The QPSK modulator works with the QPSK demodulator and the DHCT to provide forward signaling and a reverse communications path for interactive video and data services. The QPSK modulator and demodulator convert digital bit streams to RF format and RF signals to digital bits, respectively.

**RAM**

Random access memory. Volatile memory that can be read and written by a microprocessor.

**revoked**

Condition in which a host device cannot be authorized to copy copy-protected services.

**RF**

radio frequency. The range of electromagnetic frequencies above the audio range and below infrared light. Most wireless transmission uses RF, including radio, TV, satellites, portable phones, cellular phones, and wireless networks.

## RJ-45

Registered jack-45. A serial connector used to hook up computers to local area networks (LANs).

**RMA DHCT**

Return Material Authorization DHCT. A DHCT that the service provider has received back from factory repair.

**RMT**

Required Monthly Test. The FCC requires operators of cable television stations to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

**router**

A device that routes data through a packet-switched network, such as the Internet, from one LAN or WAN to another, or from a LAN to the Internet.

**RWT**

Required Weekly Test. The FCC requires operators of cable television stations to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

**S-CARD**

Single-Stream CableCARD. See also CableCARD, M-CARD, POD Module.

**S-Video**

A video connection that carries the brightness and color portions of a video signal in separate streams for improved color accuracy and reduced distortion.

**SAM**

Service Application Manager. Associates a specific service with an application that defines the medium to be used for that service, such as the World Wide Web. The SAM maintains the application in a specific directory to be used when needed by the DHCTs.

**SAP**

Second audio program. This feature allows cable service providers to offer subscribers a second audio option for their programming. The other option may be a different language or another audio track, such as the weather or a sports event.

## SARA

SA Resident Application. The set of operating programs that is "permanently" loaded into the DHCT. These programs are immediately available to the subscriber upon activation of the DHCT.

## SCS MQAM Modulator

Simulcrypt Synchronizer MQAM Modulator

**SDI**

Serial digital interface.

**SDTV**

Standard definition TV. Digital television format that includes 480-line resolution in both interlaced (480i) and progressively scanned (480p) formats.

**SDV**

Switched Digital Video. SDV is a technology that allows cable operators to recover bandwidth from infrequently-viewed channels, by making these channels "on-demand." Instead of sending all channels to the set-tops, lightly viewed channels are put into a switching pool and are only sent to the set-tops when viewers tune to them.

### Service Disconnect feature

The process of disabling a DHCT so that it cannot be used to view cable services. Also known as Brick mode.

**service gateway**

Front-end gateway for the delivery of service through the DBDS. Provides DSM-CC signaling as required to establish network resource for service delivery.

**service group**

A QAM modulator (or a cluster of QAMs) that is installed for delivering on-demand services to an associated population of DHCTs. The association of a DHCT to a specific service group is determined by first identifying the QAM modulator (or a cluster of QAMs) that a DHCT can receive.

**sessions**

Logical elements that define and allocate the resources that the network uses to deliver source content.

**shared key authentication**

A type of authentication that assumes each station has received a secret shared key through a secure channel independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of Shared Key authentication requires implementation of the 802.11 Wireless Equivalent Privacy algorithm.

**SI**

system information. A standard set of tables providing the data necessary for a navigation device to discover and access services.

**SMTA**

Standalone MTA. A hardware device that contains an MTA but does not include a DOCSIS modem or other transport. Typically connected to a cable modem through an Ethernet connection.

**SNMP**

Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

**SONET**

Synchronous Optical Network. An optical fiber network capable of transmitting ATM data packets over long distances. This data remains in a digital state and can be repeated indefinitely.

**source**

In the DBDS, a source is the actual program or data that is made available to the DHCT as a service to the subscriber. Sources can include: MPEG-2 digital broadcast services that are non-secure, non-encrypted, audio/video programs; Internet connections from an Internet service provider (ISP); Digital PPVs that are secure, encrypted, digital MPEG-2 programs; Digital music services; Analog programs that are modulated in the traditional format or converted into MPEG-2 format.

**spatial reuse**

Reusing the same frequencies for different fiber nodes or branches on the HFC network. This means that a node or group of distribution nodes use one set of QAM transmitters for a service group, and other nodes or groups of nodes use a different service group, but all use the same set of narrowcast frequencies.

**SR**

System Release. Our software release package for components of the DBDS.

**SSID**

Service Set Identifier. A group name shared by every member of a wireless network in which client PCs with the same SSID are allowed to establish a connection.

**staging**

The process of loading the necessary software and security information into the Explorer DHCT prior to deployment in subscriber's homes.

**subnet mask**

32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.

**subscriber**

A household or business that legally receives and pays for cable and/or pay television service for its own use.

**switched digital video**

See SDV.

**tar**

Short for tape archive, a UNIX utility that combines a group of files into a single file with a .tar extension.

**TCP/IP**

Transmission Control Protocol/Internet Protocol. An Internet working protocol that provides reliable data transport using connection-oriented techniques.

**TOC**

Table of contents. A file that lists the files included in the OSM EMM transfer.

**transport network**

Provides the communication link enabling audio, video, and data to be transported from the headend to the hub. It involves a network of switching and transmission equipment and can include AM fiber and SONET technologies.

**transport stream**

A data communications signal that is formatted in accordance with the protocol defined in the MPEG-2 specification ISO IEC 13818. An MPEG transport stream can carry voice, video, or data information. The MPEG data transmission protocol transports real-time data.

**UN-Config**

User-to-network configuration. A message sent from the DNCS that configures the DHCT.

**unicast**

Message sent to a single network destination.

**unicast address**

Address specifying a single network device.

**UNIX**

An operating system that is less computer/server-specific than other operating systems. UNIX is widely used in the telecommunications industry and by the Internet.

**upstream**

The transmission path from the subscriber to the headend.

**USB**

universal serial bus. A port on a PC or other device that provides connection to peripherals, such as CD-ROM drives, printers, modems, and keyboards.

**VASP**

Value-added service provider.

**VBI**

Vertical blanking interval.

**VCS**

Virtual channel service.

**VOD**

video-on-demand. The ability of a subscriber to select a program event and watch it within moments of selection. VOD allows pausing and rewinding of the event.

**VoIP**

Voice-over-Internet-Protocol. These services are a provision of voice telephony through the use of packet-switched networks running Internet Protocol (IP) networks rather than traditional circuit switching.

## WAN

Wide Area Network. A network that interconnects geographically distributed computers or local area networks.

**xOD**

anything-On-Demand. Combines two on-demand delivery mechanisms, VOD and SVOD, into one application.