Provisioning the DNCS to Support SDV Services User Guide

for System Release 2.7.1/3.7.1/4.2.1

Please Read

Important

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

Notices

Trademark Acknowledgment

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

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

Copyright

Contents

About This Guide

Introduction

The growth in available services to the service provider has far outpaced the increases in access network bandwidth due to upgrades and rebuilds. This same expansion of available services has also created a situation in which, at any given time and in any given service group, most services are not being viewed. Thus, edge device and access network bandwidth are wasted when many of those services are continuously broadcast to subscribers that are not watching them. Switched Digital Video (SDV) is a technique that recaptures such wasted access network bandwidth by delivering selected services only where and when users are actively requesting service. This technique is performed through program switching, which is also known as SDV.

SDV is configured into the SDV manager. Therefore, to provision SDV services on the Digital Network Control System (DNCS), parameters must be configured into the SDV manager on behalf of the SDV server.

Purpose

This document provides instructions for setting up and configuring SDV services on the DNCS.

Scope

The procedures covered in this document only apply to Digital Broadband Delivery System (DBDS) networks with SDV and operating with System Releases (SRs) 2.7.1/3.7.1/4.2.1. These procedures describe how to provision SDV services on the DNCS, as well as how to configure the Service Application Manager (SAM) and other features so that the Digital Home Communications Terminals (DHCTs) can display SDV services.

Important: This document does not describe how to stage SDV servers. For instructions on installing SDV servers, refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide*.

Audience

This document is written for DBDS system operators and engineers, DNCS operators and engineers, field engineers, and Cisco Services engineers.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document.

- *DNCS Online Help, (PC), 4.2.1.2* (part number 4017651)
- *Enhanced Channel Maps User's Guide* (part number 4011413)
- *Gigabit QAM Modulator Model D9479 Hardware Installation and Operation Guide* (part number 745431)
- *Netcrypt Bulk Encryptor Hardware Installation and Operation Guide* (part number 4001444)
- *Netcrypt Bulk Encryptor Software Version 1.1.3 Release Notes and Installation Instructions* (part number 4009746)
- *Provisioning the USRM for SDV on the DNCS* (part number 4015076)
- *SARA Application Server 3.4.1 Release Notes and Installation Instructions* (part number 4012158)
- *SARA Application Server 3.4.1 User's Guide* (part number 4012159)
- *SDV Operator's Guide For System Releases 2.7/3.7 or SR 4.2* (part number 4000308)
- *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584)
- *Switched Digital Video Architecture Guide* (part number 4012490)
- *System Release 2.7 Release Notes* (part number 4012155)
- *System Release 2.7.1 Release Notes* (part number 4001524)
- *System Release 3.7 Release Notes* (part number 4012156)
- *System Release 3.7.1 Release Notes* (part number 4001525)
- *System Release 4.2 Release Notes* (part number 4012157)
- *System Release 4.2.1 Release Notes* (part number 4002179)

Document Version

This is the sixth formal release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

Description	See Topic
Revised the procedure on enabling SDV functionality in the following ways: ■ Added instructions on enabling SDV functionality for tuning adapters. ■ Restructured the procedure to show more clearly how users can enable SDV functionality for **all** set-tops and tuning adapters or for **specific** set-tops and tuning adapters.	■ ***Enable SDV Functionality for All Explorer Set-Tops and/or Tuning Adapters*** (on page 37) ■ ***Enable SDV Functionality for Specific Explorer Set-Tops and/or Tuning Adapters*** (on page 41)

1

Before You Begin

Introduction

Provisioning the SDV server on the DNCS requires preparation. Preceding the provisioning process, you must ensure that your system meets specific requirements along with additional SDV-specific criteria.

In This Chapter

Prerequisites

Overview

This section lists the prerequisites required to provision the DNCS for SDV servers.

Required Prerequisites

To use the SDV service, your system must meet the following prerequisites:

- The DNCS must be operating at System Release (SR) 4.2 or later.
- Headend components (for example, GQAM, Netcrypt device) must include the software versions that are defined in the appropriate documents:
  - *System Release 2.7 Release Notes* (part number 4012155)
  - *System Release 2.7.1 Release Notes* (part number 4001524)
  - *System Release 3.7 Release Notes* (part number 4012156)
  - *System Release 3.7.1 Release Notes* (part number 4001525)
  - *System Release 4.2 Release Notes* (part number 4012157)
  - *System Release 4.2.1 Release Notes* (part number 4002179)
- SARA or a third-party navigator that supports SDV must be installed on your system.
- The following features must be enabled:
  - Switched Digital Video
  - Netcrypt Bulk Encryptor
  - SSP 2.4 Compliant
- All SDV servers should be pre-staged (refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide*).

Required Network Data

Overview

To successfully provision the DNCS for SDV services, you need detailed network data for the SDV server, Netcrypt Bulk Encryptor, edge resource (for example, GQAM), and mini-carousel for each SDV configuration.

This section provides tables to conveniently store the network data to help simplify the provisioning process.

SDV Server

The SDV server provides high-speed channel change services for the SDV system and can be set up to use the following protocols:

- CCP protocol (Channel Change)
- MCP protocol (Mini Carousel)
- HTTP protocol (Web client)
- DSP protocol (Database Sync)
- SNMP Agent protocol

When configuring the SDV server, as well as these protocols, use one of the following three options to define which Ethernet ports are utilized:

- **Option 1**: All SDV protocols are located on one physical interface (eth0).
- **Option 2**: Management is used on a separate interface, HTTP on eth1; all other protocols are configured on eth0.
- **Option 3**: The Mini Carousel is on a separate interface, eth1; all other protocols are configured on eth0.

Note: Refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584) to see procedures for setting up which protocols go out on which ports.

Fill in the values for the fields listed in the following table. These values will be used to provision the DNCS for SDV services.

Field	Your Value
Name of SDV Server	
VASP IP Address **Note:** This IP address is always the address on eth0 interface.	

Netcrypt Bulk Encryptor

The Netcrypt Bulk Encryptor is a device that receives SDV content from the Digital Content Manager (DCM) staging processor. Fill in the values for the fields or interfaces listed in the following table. These values will be used to provision the Netcrypt Bulk Encryptor on the DNCS.

Note: It is recommended that each gigabit Ethernet port be assigned to a different point-to-point subnet using a /30 subnet mask.

Field/Interface		Your Value
Netcrypt Name		
ethA (Management) Interface	MAC Address	
	IP Address	
	Subnet Mask	
	Default Gateway	
Gigabit Ethernet Port 1 (GbE)	MAC Address	
	IP Address	
	Subnet Mask	
	Default Gateway	
Gigabit Ethernet Port 2 (GbE)	MAC Address	
	IP Address	
	Subnet Mask	
	Default Gateway	

Field/Interface		Your Value
Gigabit Ethernet Port 3 (GbE)	MAC Address	
	IP Address	
	Subnet Mask	
	Default Gateway	
Gigabit Ethernet Port 4 (GbE)	MAC Address	
	IP Address	
	Subnet Mask	
	Default Gateway	

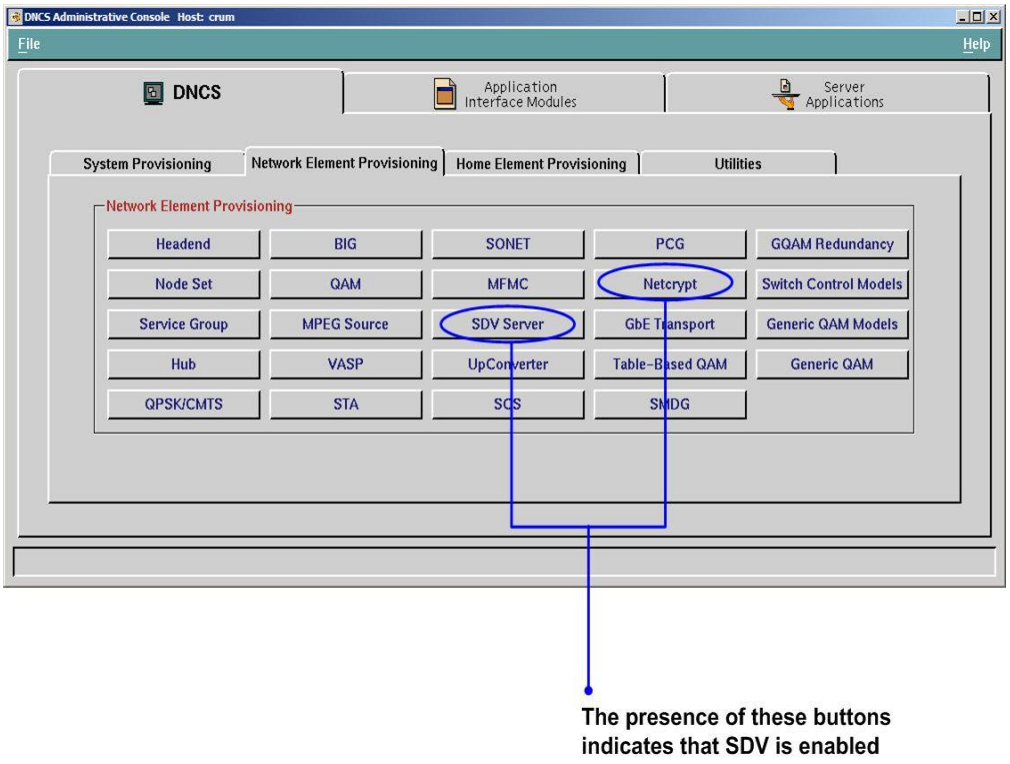
Is the SDV Feature Enabled?

Overview

Before you begin to provision the SDV Server on the DNCS, you must ensure that the SDV feature has been enabled. This section describes how to verify whether or not SDV has been enabled for your system.

Verifying if SDV is Enabled

1 From the DNCS Administrative Console, click the **DNCS** tab and then click the **Network Element Provisioning** tab. The Network Element Provisioning window appears.



2 Are the **SDV Server** and **Netcrypt** buttons visible?

- If **yes**, SDV has been enabled for your system.
- If **no**, call Cisco Services.

  Important: If the SDV server is not enabled, please confirm that the VOD server is SSP 2.3-compliant *before* calling Cisco Services to enable this feature. Enabling the SDV server on the DNCS when the VOD server is not SSP 2.3-compliant will result in a VOD outage.

Confirm the BFS Source for Switched Digital Services

Overview

This section describes how to confirm that the BFS source, SGM-IB, for switched digital services is enabled for SDV services. The SGM IB source is a source that is reserved for switched digital services.

For each SDV-enabled service group *prior* to SR 2.7.1/3.7.1 and 4.2.1, a mini-carousel discovery file is created. Each BFS carousel is limited to 475 individual files; and therefore, in earlier system releases, the number of SDV-enabled service groups available on the DNCS was limited to 475.

Important: The number of 475 SDV-enabled service groups available is based on a block size of 4,000 bytes. Decreasing the block size on your system will decrease the number of available service groups that an inband source can support. We recommend a block size of 4,000 bytes for these sources. This section assumes a block size of 4,000 bytes.

For SR 2.7.1/3.7.1/4.2.1 or later, the DNCS, by default, creates four additional BFS sources to deliver the mini-carousel discovery files. This provides for a default total of five carousels, or up to 2,375 SDV-enabled service groups.

The following table shows the default source IDs and the corresponding names for each source ID.

SRs *prior* to 2.7.1/3.7.1 and 4.2.1

Source ID	Source ID Name	Number of Service Groups
24 (original BFS source)	SGM IB	0–474

SR 2.7.1/3.7.1 and 4.2.1 or later

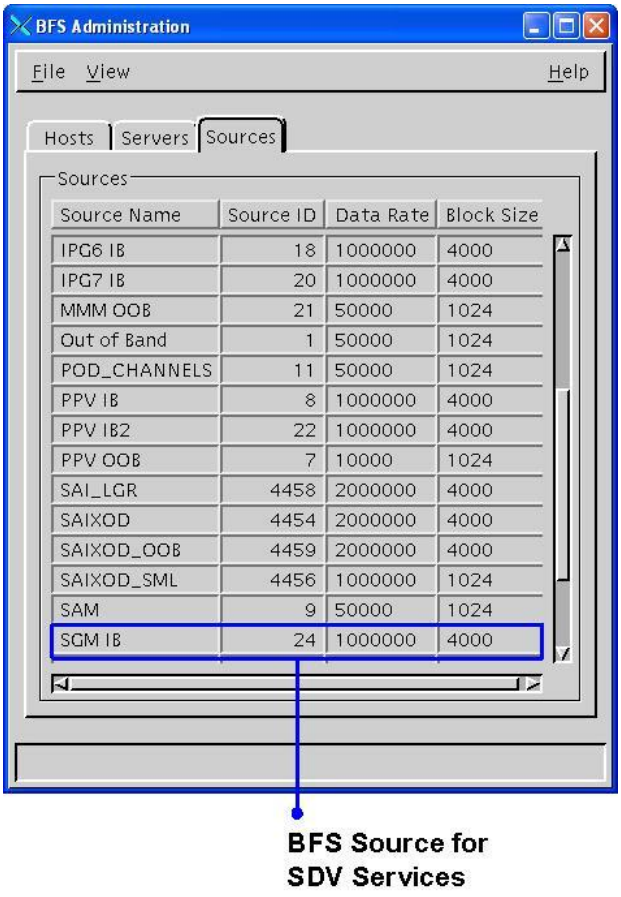
Source ID	Source ID Name	Number of Service Groups
24 (original BFS source)	SGM IB	0–474
26	SGM IB1	475–949
28	SGM IB2	950–1424
30	SGM IB3	1425–1899
32	SGM IB4	1900–2374

Confirming the BFS Source for Switched Digital Services

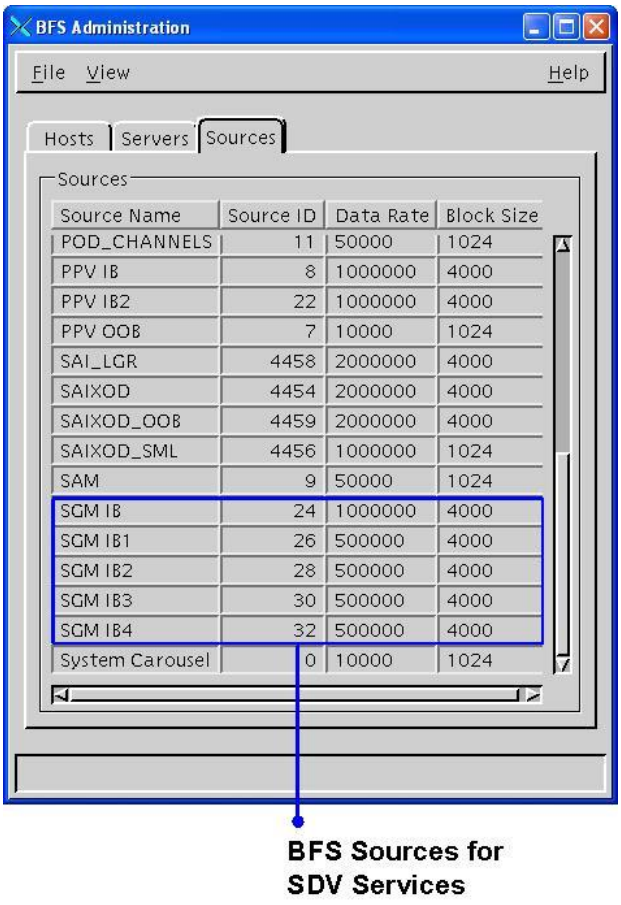
1. Facing the front of the BFS QAM modulator, press the **OPTIONS** button to cycle through the QAM menu screens until you see the **Session Count** screen.
2. Record the number of sessions in the space provided.

   Total Session Count: _____
3. From the DNCS Administrative Console, click the **Application Interface Modules** tab, and then click **BFS Admin**. Depending on your system configuration, one of the following windows opens:
   a. If you are using a typical DBDS with no RCS, the BFS Administration window opens. Go to step 5.
   b. If you are using an RCS configuration, the Please Select a Site window opens. Go to step 4.
4. From the File menu, choose **Select**. The BFS Administration window opens.
5. Click the **Sources** tab. The Sources section of the window appears.

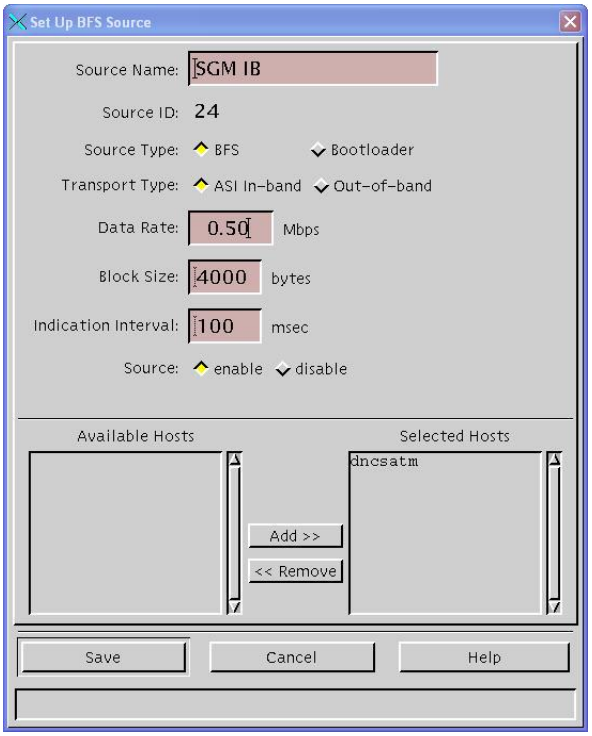
   Systems prior to 2.7.1/3.7.1 and 4.2.1



SR 2.7.1/3.7.1/3.7.1 and 4.2.1 or later



6 From the Source Name column, double-click **SGM IB** to open the Set Up BFS Source window.



7 Is the **Source** field enabled?

- If **yes**, go to step 8.
- If **no**, click **enable** and then go to step 8.

8 Are you running 2.7.1/3.7.1 and 4.2.1 or later?

- If **yes**, repeat step 7 for each source and then go to step 9.
- If **no**, go to step 9.

9 Review the remaining fields in this window. Cisco recommends the following values:

- **Source Type**—BFS
- **Transport Type**—ASI In-band
- **Data Rate**—1.00
- **Block Size**—4000
- **Indication Interval**—100
- **Selected Hosts**—dncsatm

10 Did you make any modifications to this window?

- If **yes**, click **Save** and go to step 11.
- If **no**, click **Cancel**.

11 Repeat steps 1–2 and record the current **Session Count** here: _____

12 Did the session count increase by the number of BFS sources you added?

- If **yes**, you have successfully enabled the SGM IB BFS sources.
- If **no**, call Cisco Services.

2

Provisioning SDV Services on the DNCS

Introduction

This chapter provides the procedures for provisioning the DNCS to support SDV. To provision SDV services on the DNCS, parameters must be configured into the SDV manager on behalf of the SDV server.

Important: These procedures apply for any SDV client application provider, for example, client applications running SARA.

In This Chapter

Set Up the SDV Parameters on the DNCS

Overview

This section describes the parameters that are required to provision switched digital services on the DNCS. These parameters are global parameters that are provisioned for all switched digital service groups and active content.

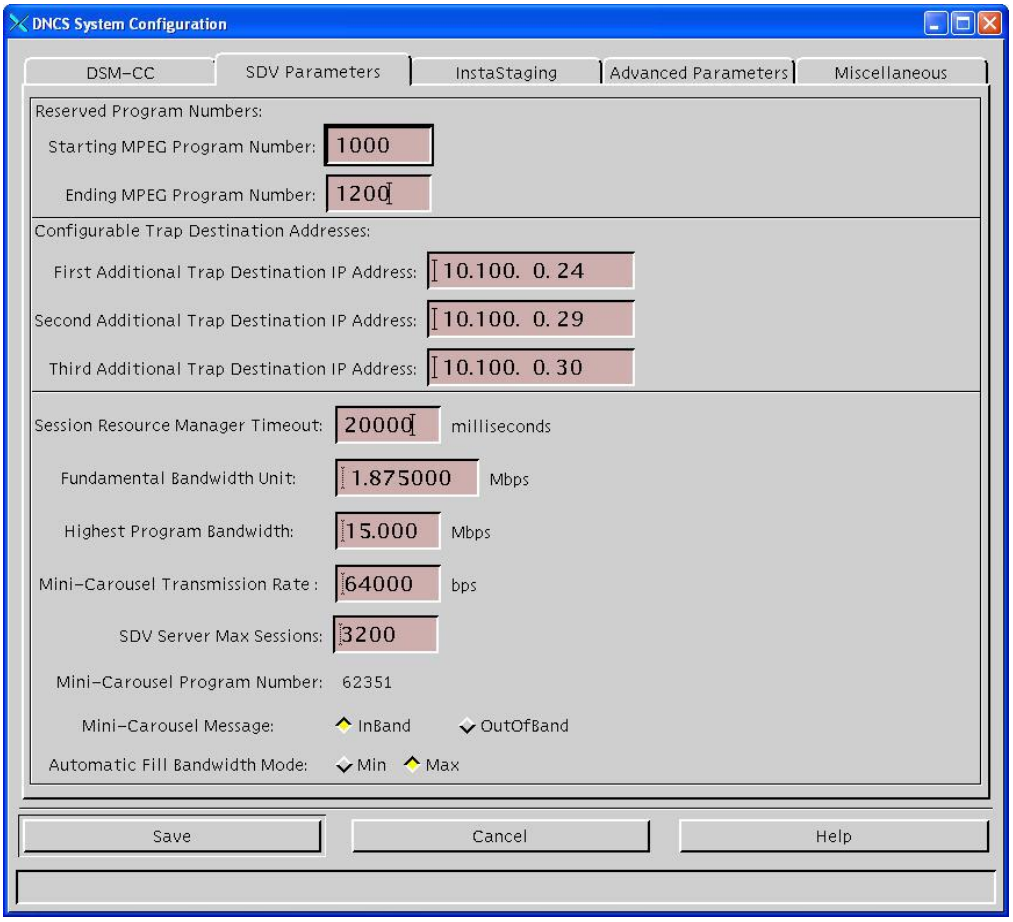
Setting Up the SDV Parameters

Complete the following steps to provision the global parameters for the switched digital service groups.

Note: The SDV parameters shown in these procedures are the most basic requirements that would typically be set up.

1 Click the **DNCS** tab and then click the **System Provisioning** tab.

2 From the System Management section, click **Sys Config** to open the DNCS System Configuration window.



3 Click the **SDV Parameters** tab.

4 From the Reserved Program Numbers area of the window, enter values in the following fields:

- **Starting MPEG Program Number**: The starting number for the range of MPEG program numbers reserved for programs set up for SDV services. The default is 1000
- **Ending MPEG Program Number**: The ending number for the range of MPEG program numbers reserved for programs set up for SDV services. The default is 2000

Note: The program number range is used by the DNCS to limit the program numbers assigned to the GQAM RF output for SDV services.

5 Verify the remaining values that appear by default in the following fields:

- **Configurable Trap Destination Addresses**
  - **First Additional Trap Destination IP Address:** The IP address of the first trap destination device that is registered to receive traps from the SDV server
  - **Second Additional Trap Destination IP Address**: The IP address of the second trap destination device that is registered to receive traps from the SDV server
  - **Third Additional Trap Destination IP Address**: The IP address of the third trap destination device that is registered to receive traps from the SDV server
- **Session Resource Manager Timeout**: The timeout value for a request to the DNCS SRM. The default is 20000 milliseconds

  Note: When the master SRM does not respond within the configured timeout value, the SRM status alarm is asserted
- **Fundamental Bandwidth Unit**: The bandwidth unit in which sessions are requested from the master SRM. The default is 1.875 Mbps; however we recommend that you set this value to 3.75 Mbps.
- **Highest Program Bandwidth**: The highest bandwidth required for a SDV program. The SDV server uses this value to make intelligent decisions when assigning the programs to edge resources in a service group. The default is 15.00 Mbps
- **Mini-Carousel Transmission Rate**: The rate in which the mini-carousel is transmitted by an SDV server to the service group. The rate is defined in bits per second (bps)
- **SDV Server Max Sessions**: A global setting that defines the maximum number of shell sessions allowed for all servers by the SRM
- **Mini-Carousel Program Number**: The program number of the mini-carousel on the inband channel. This value is defined as 62351

- **Mini-Carousel Message**: (InBand/OutOfBand) Select InBand to receive the MC message via an inband stream
- **Automatic Fill Bandwidth Mode**
  - **Max**: When selected, the SDV server will bind programs to edge resources for all available bandwidth regardless of whether subscribers are requesting these programs
  - **Min**: When selected, the SDV server only binds programs when a subscriber has requested the program

  Note: "Max" is the recommended value for this field.

6 Click **Save** and then click **Close**.

Add a VASP Entry for Each SDV Server

Overview

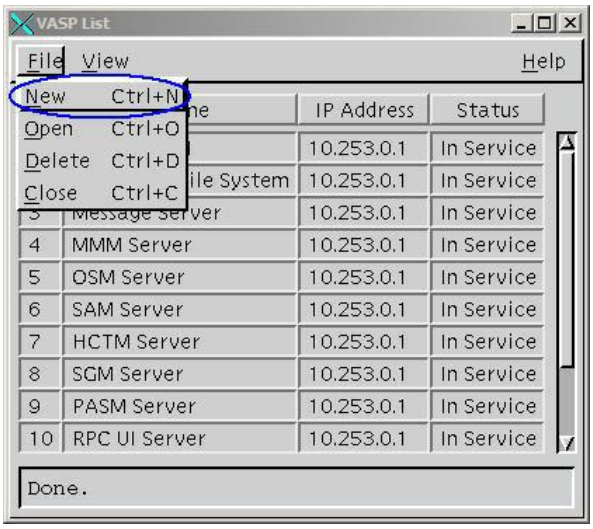
This section describes how to set up a value added service provider (VASP) entry for each SDV server that is installed on your network. A VASP provides an interface for passing application and system data to DHCTs. DHCTs use this data to provide subscribers with services.

Adding VASP Entries on the DNCS

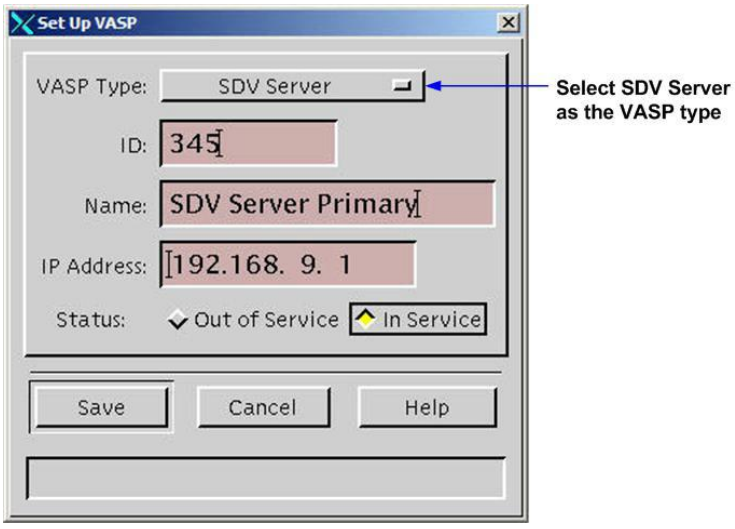
Important: You *must* create a VASP entry for each SDV server set up in your system. Without a VASP entry, the DNCS will not be able to process signals to and from the server.

1 Click the **DNCS** tab and then click the **Network Element Provisioning** tab.

2 Click **VASP** to open the VASP List window.



3 Click **File** and select **New** to open the Set Up VASP window.



4 Select or enter the following values:

- **VASP Type**: Select **SDV Server**.
- **ID**: Enter a unique number that you will use to identify the SDV server (you can use up to 10 numeric characters).
- **Name**: Enter a unique name for the SDV server (for example, enter a name that corresponds to the hub in which it provides services).

  Note: We recommend that you enter the same name that you assigned during setup of the SDV server.
- **IP Address**: Enter the IP address for the SDV server that will be associated with this VASP entry.

  Note: The VASP IP address must match the IP address assigned to the SDV server eth0 interface.
- **Status**: Select **In Service** to indicate that the VASP is in service and operational.

5 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.

6 Repeat steps 2–5 to create a VASP entry for each SDV server that you have set up on your system.

Set Up the SDV Server

Overview

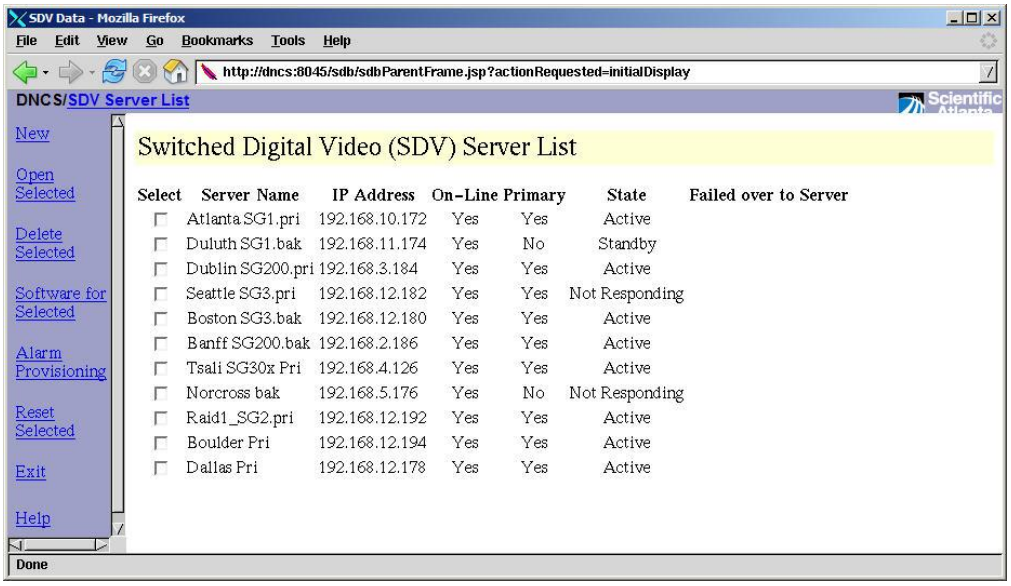
The SDV server provides the "switching control element" for the SDV system. In essence, the switching control element is a process where the SDV server receives channel change requests for switched content from DHCTs. The SDV server then attaches the requested content to a session on the QAM, and assigns the session to real programs. These programs are transmitted to service groups and then delivered to the requesting DHCTs.

Adding a New SDV Server to the DNCS

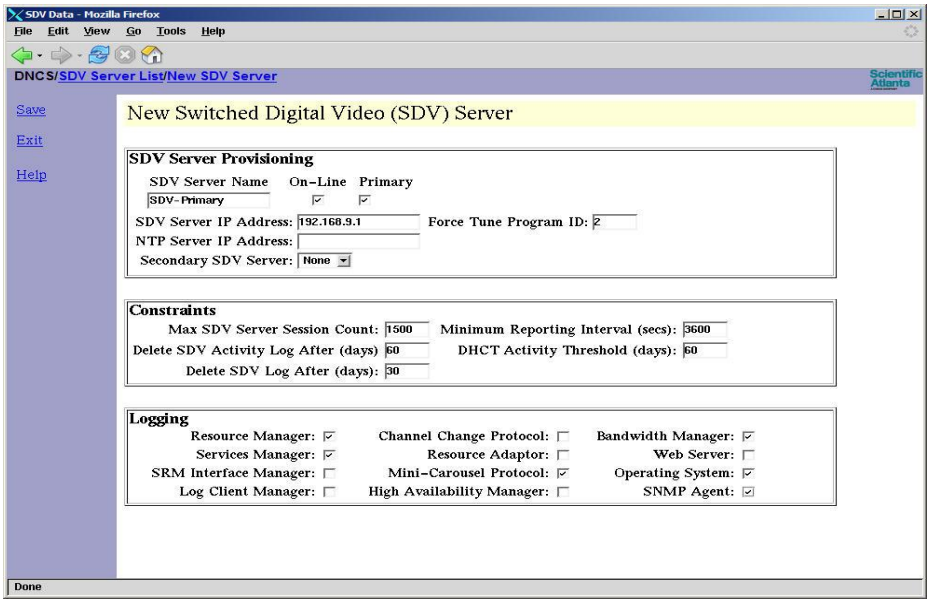
Important: An SDV server must be set up for each VASP entry that you have created.

1 Click the **DNCS** tab and then click the **Network Element Provisioning** tab.

2 Click **SDV Server** to open the Switched Digital Video (SDV) Server List window.



3 Click **New** to open the New Switched Digital Video (SDV) Server window.



4 From the **SDV Server Name** field, type a name that corresponds to the hub to which it is providing service.

Note: Cisco suggests that you enter the same name that you set up for the new VASP entry.

5 Select or enter the following values; however, we recommend that you maintain the default settings for the following fields:

- **SDV Server Provisioning**
  - **On-Line**: Select **On-Line** to indicate that this SDV server is connected within the networked system; do not select **On-Line** if this SDV server is currently not connected to the networked system.
  - **Primary**: Select the **Primary** check box to indicate that this SDV server is the main server in the SDV system; do not select this option if this SDV server is a backup SDV server (backs up a failed primary SDV server).
  - **SDV Server IP Address**: Enter the IP address for the SDV server that you are provisioning.

    Note: This is the same IP address that is defined for VASP entry.
  - **NTP Server IP Address**: Enter the IP address for the NTP (Network Time Protocol) server. The NTP server provides time synchronization services to the SDV server.
  - **Secondary SDV Server**: If you are provisioning a primary SDV server, select a secondary (backup) SDV server to provide a level of redundancy in the event of a primary SDV server outage; if you are provisioning a secondary SDV server, select **None**.
  - **Force Tune Program ID**: Enter the source ID for the program that the DHCT/tuner is forced to tune to if it is removed from an SDV channel.

    Note: This program ID should not be an ID for a switched digital service.

- **Constraints**
  - **Max SDV Server Session Count**: Enter a value (for example, 1500) to set the maximum number of sessions for which the SDV server is allowed.
  - **Delete SDV Activity Log After (days)**: Retain the default value (60); this is the threshold value that dictates when SDV activity logs are automatically deleted.
  - **Delete SDV Log After (days)**: Retain the default value (30); this is the threshold value that dictates when SDV event logs will be automatically deleted from the system.
  - **Minimum Reporting Interval (secs)**: Retain the default value (3600); this is the interval that the SDV client sends user activity information to the SDV server.
  - **DHCT Activity Threshold (days)**: Retain the default value (60); this is the value that, when reached, allows you to delete a DHCT that is not in communication with the system.
- **Logging**: Select any of the following logs that you would like to have monitored on the SDV server

  Note: If you are running SR 4.2.1 or later, you can turn on log monitoring from this DNCS GUI; however, if you are running a SR *prior* to 4.2.1, you can only turn on log monitoring from the SDV Server Web UI (refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide*).
  - **Resource Manager**
  - **Services Manager**
  - **SRM Interface Manager**
  - **Log Client Manager**
  - **Channel Change Protocol**
  - **Resource Adaptor**
  - **Mini-Carousel Protocol**
  - **High Availability Manager**
  - **Bandwidth Manager**
  - **Web Server**
  - **Operating System**
  - **SNMP Agent**

6 Click **Save** to save the values to the new SDV server. You are returned to the Switched Digital Video (SDV) Server List window.

7 Do you need to create an additional SDV server or backup SDV server?

- If **yes**, click the SDV Server List link from the top area of the window and then repeat steps 3 through 6.
- If **no**, click **Exit** to close the Switched Digital Video (SDV) Server List window.

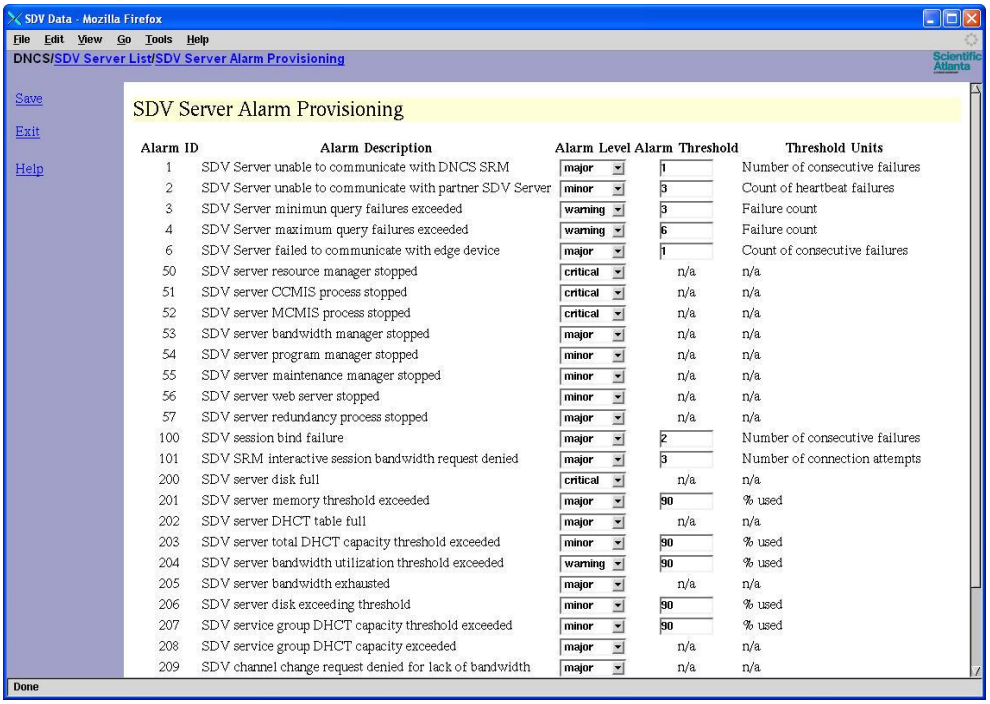
Provisioning Alarms for an SDV Server

Important: You must set the Alarm Threshold for Alarm ID 6 and Alarm ID 100 to 1 as they directly relate to the Resource Fail Threshold and the Resource Alarm Threshold values defined for the SDV Server software. For details about the SDV Server software, refer to the *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584).

When provisioning alarms for an SDV server, you can define the severity of an alarm level (for example, a major alarm or a critical alarm), as well as the maximum number of instances an event can occur until an alarm situation exists. This section describes how to provision specific SDV alarms for an SDV server.

1 From the Switched Digital Video (SDV) Server List window, select a server by clicking the check box in the appropriate **Select** column.

2 Click **Alarm Provisioning**. The SDV Server Alarm Provisioning window opens and describes each alarm type by an ID number and a description.



Alarm ID	Alarm Description	Alarm Level	Alarm Threshold	Threshold Units
1	SDV Server unable to communicate with DNCS SRM	major	1	Number of consecutive failures
2	SDV Server unable to communicate with partner SDV Server	minor	3	Count of heartbeat failures
3	SDV Server minimun query failures exceeded	warning	3	Failure count
4	SDV Server maximum query failures exceeded	warning	6	Failure count
6	SDV Server failed to communicate with edge device	major	1	Count of consecutive failures
50	SDV server resource manager stopped	critical	n/a	n/a
51	SDV server CCMIS process stopped	critical	n/a	n/a
52	SDV server MCMIS process stopped	critical	n/a	n/a
53	SDV server bandwidth manager stopped	major	n/a	n/a
54	SDV server program manager stopped	minor	n/a	n/a
55	SDV server maintenance manager stopped	minor	n/a	n/a
56	SDV server web server stopped	minor	n/a	n/a
57	SDV server redundancy process stopped	major	n/a	n/a
100	SDV session bind failure	major	2	Number of consecutive failures
101	SDV SRM interactive session bandwidth request denied	major	3	Number of connection attempts
200	SDV server disk full	critical	n/a	n/a
201	SDV server memory threshold exceeded	major	90	% used
202	SDV server DHCT table full	major	n/a	n/a
203	SDV server total DHCT capacity threshold exceeded	minor	90	% used
204	SDV server bandwidth utilization threshold exceeded	warning	90	% used
205	SDV server bandwidth exhausted	major	n/a	n/a
206	SDV server disk exceeding threshold	minor	90	% used
207	SDV service group DHCT capacity threshold exceeded	minor	90	% used
208	SDV service group DHCT capacity exceeded	major	n/a	n/a
209	SDV channel change request denied for lack of bandwidth	major	n/a	n/a

3 Click the arrow in the **Alarm Level** field and select one of the following options for defining the severity of the alarm:

- **critical**
- **major**
- **minor**
- **warning**
- **disabled**

4 Enter an integer value (0 to 999) in the **Alarm Threshold** field. This value designates the maximum number of consecutive failures that can occur until the alarm condition occurs.

5 Click **Save**. The DNCS updates the database and the SDV Manager sets these changes to all SDV servers.

6 Go to ***Set Up a Netcrypt Bulk Encryptor*** (on page 24).

Set Up a Netcrypt Bulk Encryptor

Overview

This section provides instructions for completing each of the following tasks that are required to provision a Netcrypt Bulk Encryptor on the DNCS.

1 Add a Netcrypt element to the DNCS, but do not place the element online.

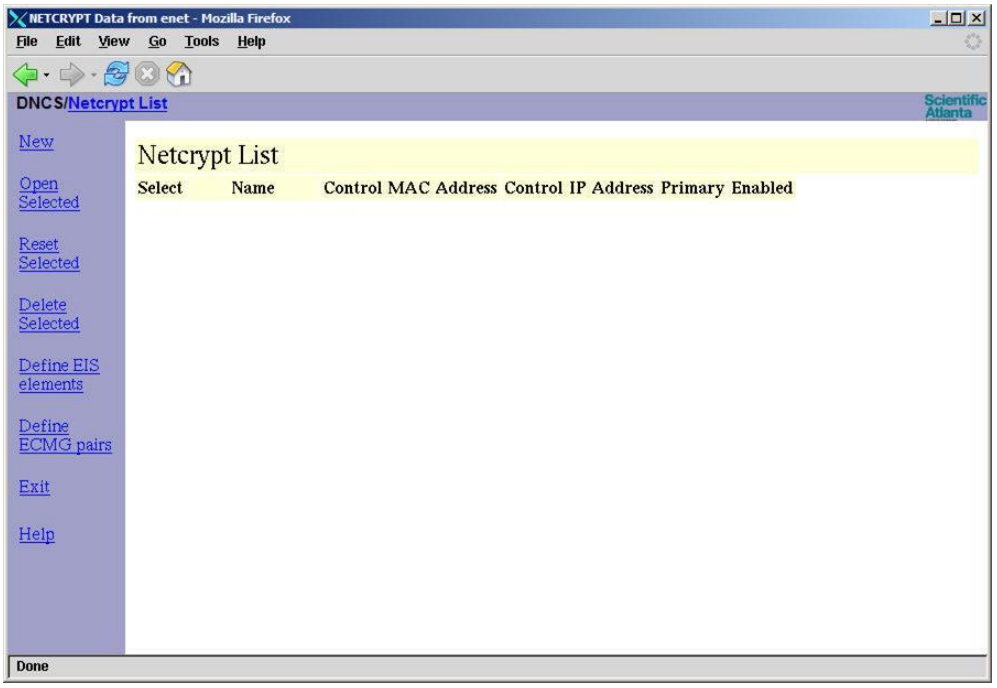
2 Provision the Ethernet ports on the Netcrypt element.

Content is encrypted based on the DNCS control. Provisioning a Netcrypt Bulk Encryptor establishes communication between the DNCS and the Netcrypt Bulk Encryptor. Without DNCS control, the Netcrypt Bulk Encryptor is inoperable.

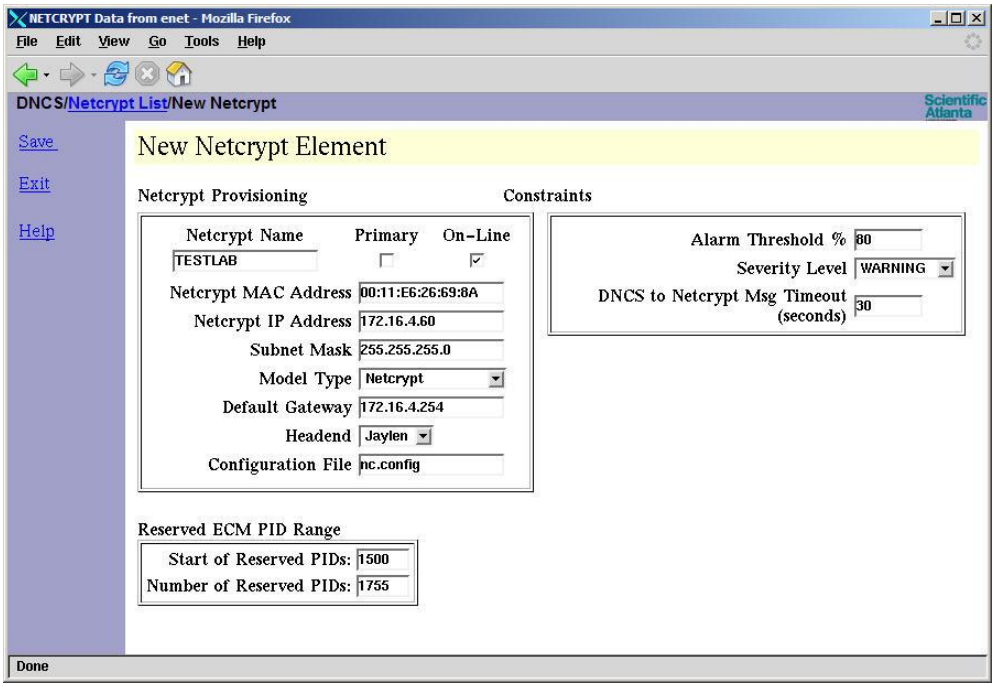
Note: For detailed information about the Netcrypt device, refer to the *Netcrypt Bulk Encryptor Hardware Installation and Operation Guide* (part number 4001444).

Adding a Netcrypt Bulk Encryptor

1 From the Network Element Provisioning tab on the SDV Administrative Console, click **Netcrypt**. The Netcrypt List window opens and shows any Netcrypt elements that have been provisioned on the DNCS.



2 Click **New**. The New Netcrypt Element window opens.



3 Follow these instructions to enter data in the fields of the Netcrypt Provisioning area on the New Netcrypt Element window:

Important: Do not modify the values in the Reserved ECM PID Range or Constraints area of this window.

- **Netcrypt Name**: Enter a name (up to 20 alphanumeric characters) for the unit that is consistent with the naming scheme used on your network map. We recommend that you establish a naming scheme that allows you to easily identify the unit and where it resides. For example, a name of **NBE43hub1** could represent a Netcrypt Bulk Encryptor whose IP address ends in 43 and processes data for Hub 1.
- **Primary**: If this is the main Netcrypt Bulk Encryptor, turn this option on. If this is a backup unit to the primary device, do not select this option.
- **On-Line**: Leave this setting turned off. (Later, when the Netcrypt Bulk Encryptor is completely provisioned and successfully booted, you will need to turn this setting on.)
- **Netcrypt MAC Address**: Enter the MAC Address of the control port (ethA) for the Netcrypt Bulk Encryptor (from the label on the underside of the Netcrypt Bulk Encryptor). Make certain to separate each pair of characters in the 12-character address with a colon, for example 00:00:00:00:00:00.
- **Netcrypt IP Address**: Enter the IP address of the control port (ethA; management IP address) for the Netcrypt Bulk Encryptor. (You can obtain this address from your network map or from your system administrator.)
- **Subnet Mask**: Enter the subnet mask for this subnet.
- **Model Type**: Select **Netcrypt**.

- **Default Gateway**: If your system uses a default gateway, enter the IP address of your default gateway. This is required for a network using routers (layer 3).
- **Headend**: Select the headend where the Netcrypt Bulk Encryptor resides.
- **Configuration File**: Type the name of the Netcrypt configuration file. Typically this file is nc.config; however, you can enter a different configuration file, for example, when testing new Netcrypt software (this configuration file should match the name in the TFTP boot directory).

  Note: When power is applied to the Netcrypt Bulk Encryptor for the first time, or when the unit rebooted, it uses the nc.config file to determine if the correct version of code has been installed on the unit. If the Netcrypt Bulk Encryptor determines that an incorrect version of code has been installed, it requests that the correct code be downloaded.

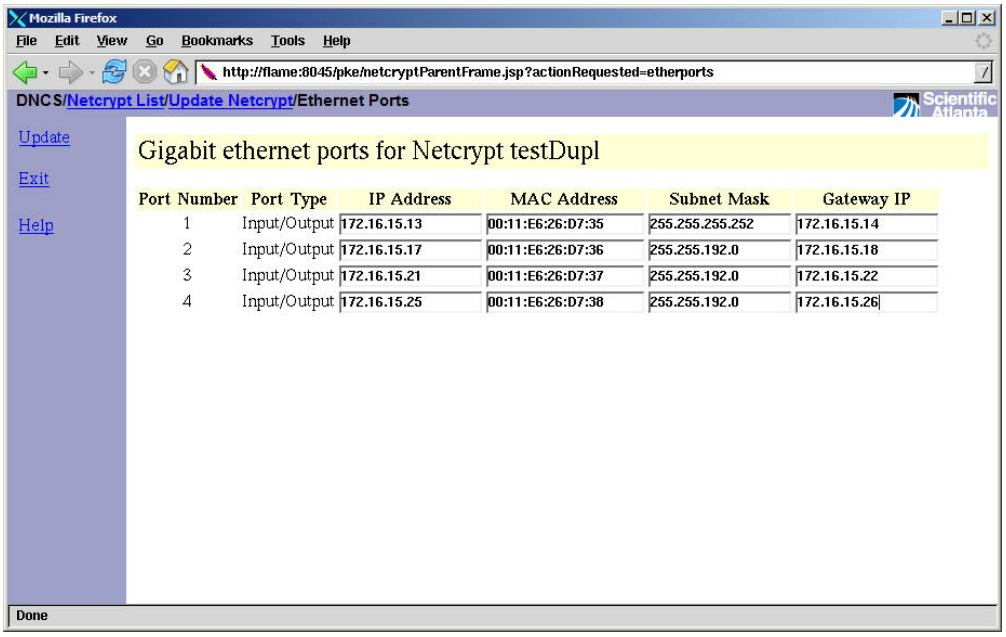
4 Click **Save**. The New Netcrypt Element window closes and the Netcrypt element you saved appears in the list.

Provisioning Gigabit Ethernet Ports for a Netcrypt Bulk Encryptor

After the Netcrypt Bulk Encryptor is listed in the Netcrypt List window, follow these instructions to provision the Gigabit Ethernet ports for the Netcrypt element you added to the New Netcrypt Element window.

1 From the Netcrypt List window, click the **Select** button next to the new Netcrypt Bulk Encryptor whose ports you want to configure, and click **Open Selected.** The Update Netcrypt Element window opens for this Netcrypt device.

2 Click **Ethernet Ports**. The Gigabit Ethernet ports window opens for the Netcrypt element you have added to the DNCS.



3 Follow these instructions to configure the Gigabit Ethernet ports by entering data in the fields that do not already contain data:

- **IP Address**: Enter the IP address assigned to each GbE port that this Netcrypt Bulk Encryptor uses.
- **MAC Address**: Enter the MAC address of each GbE port that this Netcrypt Bulk Encryptor uses. Make certain to separate each pair of characters in the 12-character address with a colon, for example 00:00:00:00:00:00.
- **Subnet Mask**: Enter a subnet mask for the GbE interface.
- **Gateway IP**: If your system uses routers, enter the gateway IP address for each GbE port.

4 Click **Update**. The SDV saves the information you entered and updates the window to display the ports you defined.

5 Click the **Update Netcrypt** link from the top of the Gigabit Ethernet ports window. The Update Netcrypt [Name of Netcrypt] window opens.

6 From the Netcrypt Provisioning area, click **On-Line** and then click **Update**. The DNCS saves the information you entered and the Netcrypt device is placed on-line.

Add the SDV Server to the Desired Service Group

Overview

A service group is a set of modulator channels (Quadrature Amplitude Modulation [QAMs], multiple QAMs [MQAMs], or Gigabit QAMs [GQAMs]) that have been combined to provide services to a unique set of DHCTs. In order to provide SDV services, you must add a service group for each SDV server in your network.

To provide SDV services, GQAMs can only be added to a service group. Service groups enable DHCTs to distinguish which GQAM is providing the SDV service.

Important: The GQAMs you plan to add to a service group must first be installed in your network and configured on the DNCS. If they are not installed and configured, please do so now. If you need assistance, refer to *Gigabit QAM Modulator Model D9479 Hardware Installation and Operation Guide* (part number 745431).

Adding GQAMs to a Service Group for SDV

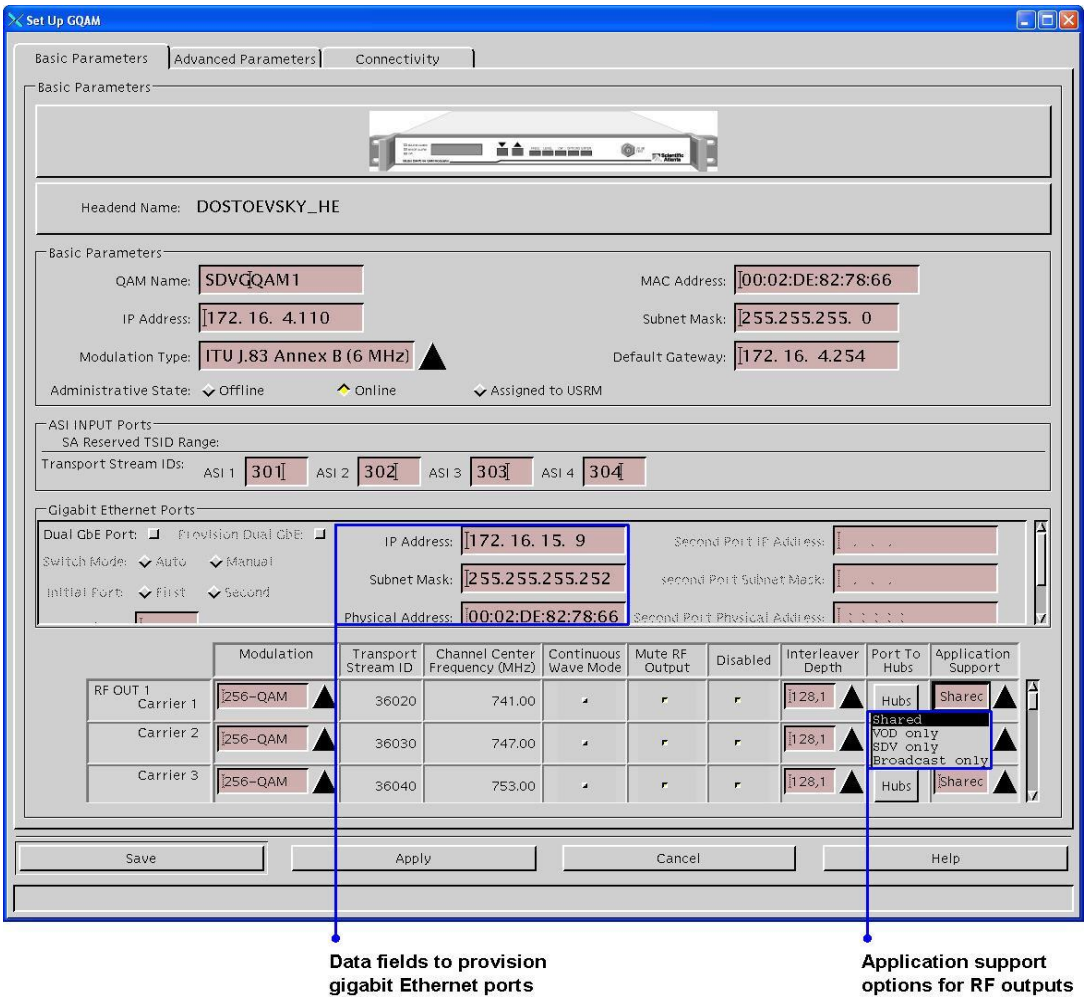
The GQAMs you plan to add to a service group must first be installed in your network and configured on the DNCS. If they are not installed and configured, please do so now. If you need assistance, refer to *Gigabit QAM Modulator Model D9479 Hardware Installation and Operation Guide* (part number 745431).

When configuring the GQAM for SDV services, the GUI on the DNCS should resemble the following output.

Important:

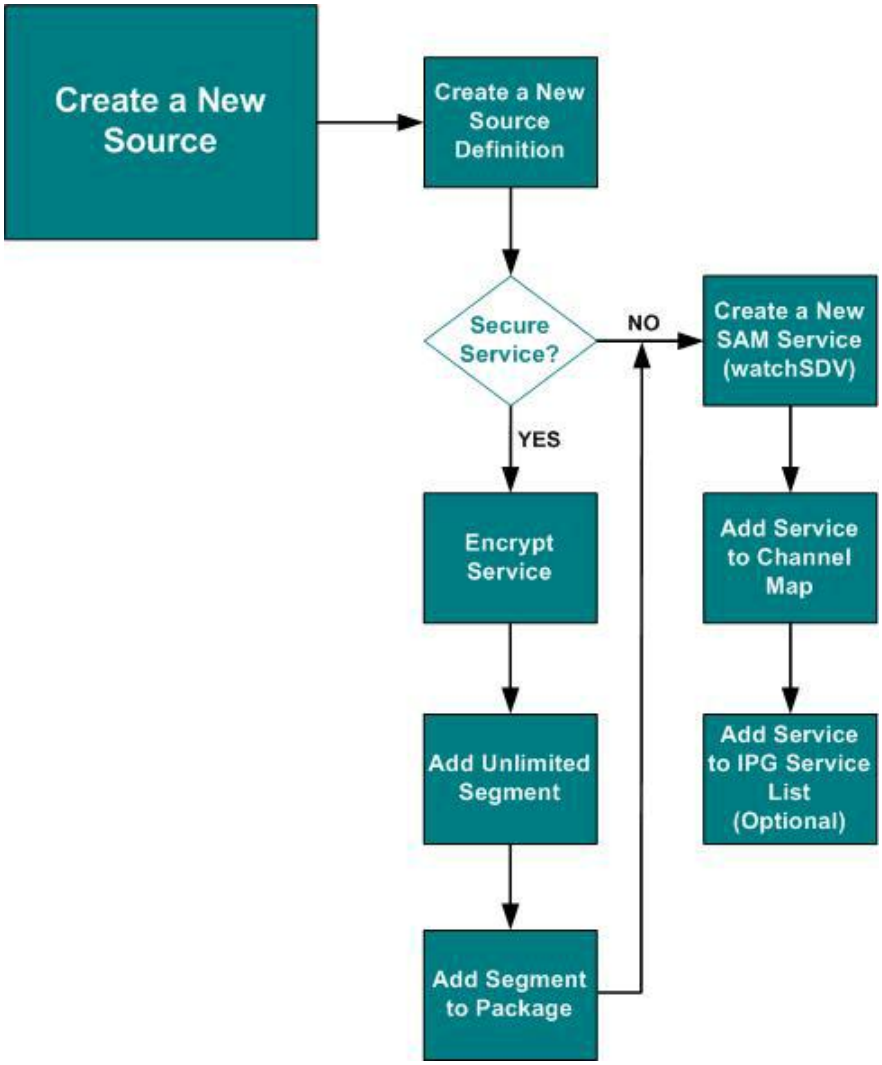
- Please ensure that you have accurately defined the application support for RF outputs planned for SDV service groups. If the carrier is supporting both VOD and SDV, set the application support to **Shared**. If the carrier is supporting SDV only, set the application support to **SDV only**.
- Please ensure that now RF carriers are muted when they are added to a service group.

Note: It is recommended that each Gigabit Ethernet port be assigned to a different point-to-point subnet using a /30 subnet mask.



Creating a New SDV Multicast Source

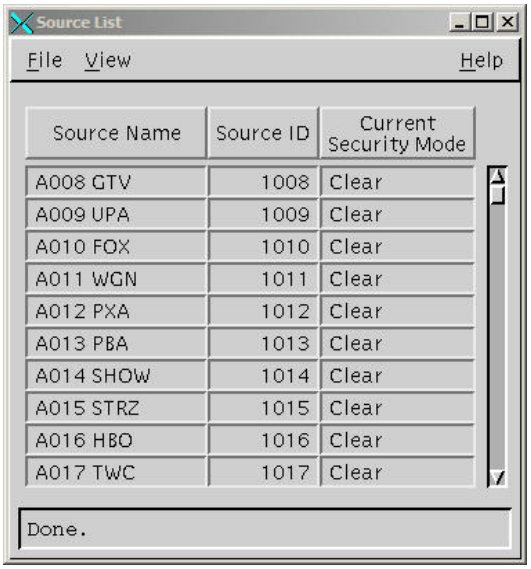
See the following diagram for an overview of the procedures that must be completed to add a new SDV multicast source.



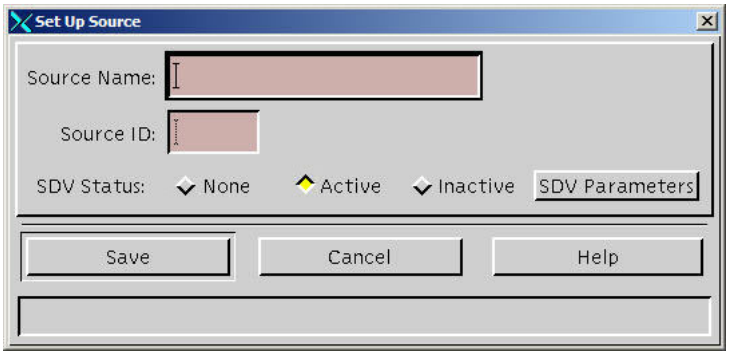
Complete the following steps to set up a new SDV multicast source for SDV services.

1 Click the **DNCS** tab and then click the **System Provisioning** tab.

2 Click **Source** to open the Source List window.



3 Click **File** and select **New** to open the Set Up Source window.



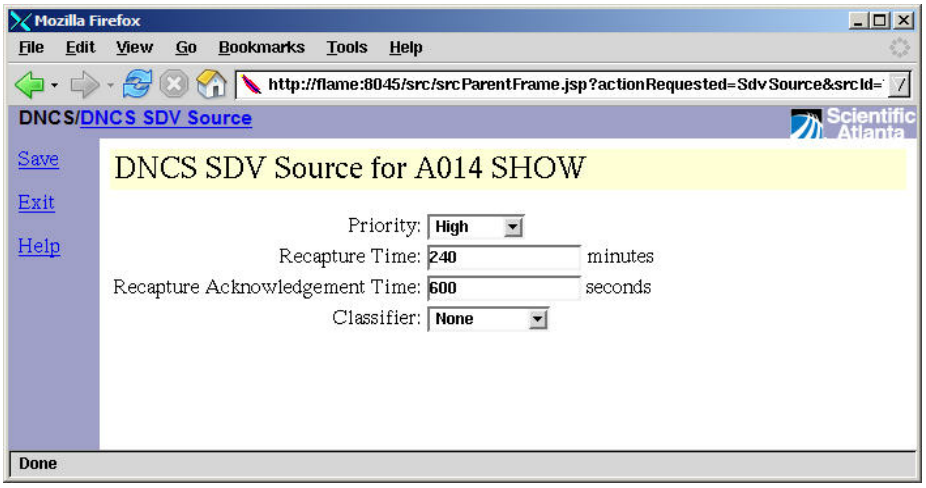
4 Enter a name in the **Source Name** field and the next available ID value in the **Source ID** field.

Important: Spaces are not permitted in the Source Name field.

5 From the SDV Status field, click **Active** to define the source to use SDV services.

Note: Selecting **Inactive** will set up the source for SDV services, but it will remain inactive until it is changed to Active. Selecting **None** will not set up the source for SDV services.

6 Click **SDV Parameters** to set up parameters for the SDV source. The DNCS SDV Source window opens.



7 Maintain the default values or change them to different value specific to your system. The definition for each field is described in the following list:

- **Priority**—This field defines how programs are filled when there are no active users and defines which programs are recaptured if the SDV server reclaims bandwidth from the clients. The default is High
- **Recapture Time**—The amount of time for a program that has no user activity to be considered eligible for recapture. When this time is reached, the SDV server will send a request barker to a client. The request barker prompts the user to acknowledge if they are still watching the program; otherwise, the bandwidth is recaptured and the client is forced tuned to another channel. The default is 240 minutes
- **Recapture Acknowledgement Time**—The time in which a user must acknowledge the request barker on the TV screen to recapture an offered program. The default is 600 seconds
- **Classifier**—A description for the type of program. The default is None

8 Did you make changes to the DNCS SDV Source window?

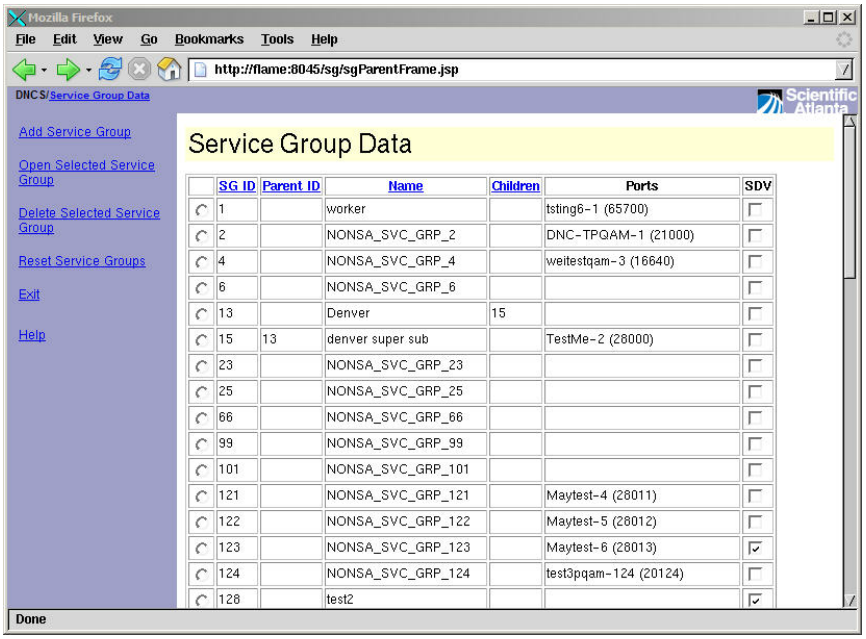
- If **yes**, click **Save** and then click **Exit**.
- If **no**, click **Exit**.

9 From the Set Up Source window, click **Save**. The new source is listed in the Source List window.

Adding the SDV Server to a Service Group

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Service Group** to open the Service Group Data window.

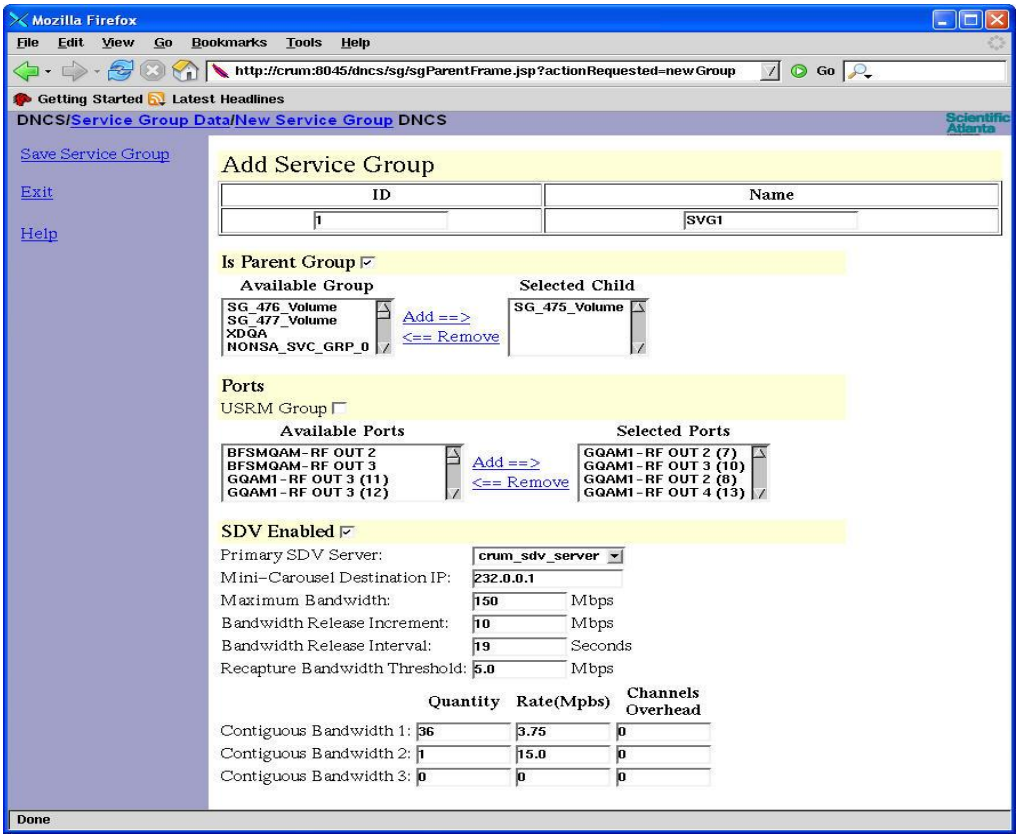


Important: Do not manually select a check box in the SDV column. This field is automatically updated after saving a service group with SDV Enabled.

3 Are you adding or editing a Service Group?

- If **adding a service group**, go to step 4.
- If **editing a service group**, go to step 7.

4 Click **Add Service Group**. The Add Service Group window opens.



5 Click in the **ID** field and type a unique number to identify the service group.

6 Click in the **Name** field, type a name for the service group, and then go to step 8.

Note: The name you enter can include numbers and letters. We recommend that you establish a naming scheme that allows you to easily identify the SDV service, the GQAM modulator(s) providing it, and which hub it serves.

Example: A name of SDV_SG_Hub1_GQ43 could represent an SDV service group associated with a GQAM modulator, whose IP address ends in 43, and that processes SDV data for Hub 1.

7 Select the service group that you want to associate with the SDV server and click **Open Selected Service Group**. The Edit Service Group window opens.

8 Is this service group a parent group (a service group that will contain one or more child service groups)?

- If **yes**, select the check box next to **Is Parent Group**, and then go to step 9.
- If **no**, go to step 11.

9 From the **Available Groups** list, select the child service group that will be included in this parent service group and click **Add**. The child service group moves to the Selected Child list.

10 Do you want to include additional child service groups to the parent group?

- If **yes**, repeat step 9.
- If **no**, go to step 11.

11 If you are using a USRM, select the **USRM Group** check box.

Important: The USRM is a software upgrade to the Model 9500 SDV Server that is available for SR 4.2.1 or later. For details on provisioning the USRM, refer to *Provisioning the USRM for SDV on the DNCS* (part number 4015076).

12 From the Available Ports list, click to select the port for the GQAM modulator that will be providing SDV for this service group or USRM group.

13 Click **Add**. The selected port moves from the Available Ports list into the Selected Ports list.

14 Do you want to add additional ports that will provide SDV for this service group?

- If **yes**, repeat steps 12–13.
- If **no**, go to step 15.

15 Click **SDV Enabled** to enable the service group to support switched digital channels. The lower portion of the window updates to include SDV-related fields.

16 Select or enter the following values:

- **Primary SDV Server**: Select the SDV server that you want to designate as the main server for this service group.
- **Mini-Carousel Destination IP**: Enter the destination multicast IP address for the mini-carousel used by the SDV server assigned to this service group.

  Notes:

  – This IP address is unique for each service group.

  – Any IP address can be assigned as long as it is not already assigned by the Internet Assigned Numbers Authority (IANA).

  – The IANA reserves 232.0.0.0 – 232.255.255.255 for Source Specific Multicast (SSM). Some routers allow this range to be configured; therefore, when using SSM, the 232/8 range is not mandatory.

  – If SSM is not used, we recommend that you use the local administrative multicast range (239/8). If SSM is used (recommended), then we recommend that you use 232/8.

- **Maximum Bandwidth**: The maximum bandwidth that the SDV server will request for all SDV content for each service group.

  Note: To calculate the maximum bandwidth, multiply the number of carriers by 37.5 Mbps. For example, if you have four RF carriers, the maximum bandwidth should not be greater than 150 Mbps.

- **Bandwidth Release Increment**: The Interval that the SDV server uses to determine if excess bandwidth should be returned to the SRM.

- **Bandwidth Release Interval**: Enter the amount of time that will pass, in seconds, before the SDV Manager checks to see if bandwidth is needed.
- **Recapture Bandwidth Threshold**: Defines the bandwidth threshold in which, when reached, the SDV server will attempt to reclaim bandwidth from the set-tops (for example, when a set-top is tuned to a SDV channel yet no one is watching the program). The default value is 30 Mbps.
- **Contiguous Bandwidth 1, Contiguous Bandwidth 2, Contiguous Bandwidth 3**: Defines the following fields for session groups 1, 2, and 3.
  - **Quantity**: Defines the number of preallocated channels.
  - **Rate(Mbps)**: Defines the requesting bandwidth (rate) per channel.

    Important: We recommend that you set the Contiguous Bandwidth 1 rate to 37.5 Mbps. This will reduce the number of session requests from the SDV servers to the DNCS and therefore reduce stress on the system.
  - **Channels Overhead**: Defines the number of overhead channels (extra bandwidth the SDV server maintains in overhead to satisfy channel change requests).

  Notes:
  - Each session group is reserved for a type of program (for example, high definition [HD] programs). Cisco recommends that you define the same program type to each session group for all service groups.
  - The Quantity and Rate fields control the amount of bandwidth the server requests from the SRM when it is initialized.

17 Click **Save Service Group** to save the values to this service group and return to the Service Group Data window, which now lists the service group that you just added.

Note: The SDV check box for this service group is automatically selected.

18 Do you want to set up another Service Group?

- If **yes**, repeat steps 4 through 17.
- If **no**, click **Exit**.

Enable SDV Functionality for All Explorer Set-Tops and/or Tuning Adapters

Overview

This section describes how to enable SDV functionality for all Explorer set-tops and/or tuning adapters that have been deployed in your system by creating an SDV SAM service. Without a SAM SDV service, SDV functionality is disabled on these devices.

Important: If you want to enable SDV functionality for specific set-tops and tuning adapters, skip this section and go to ***Enable SDV Functionality for Specific Explorer Set-Tops and/or Tuning Adapters*** (on page 41).

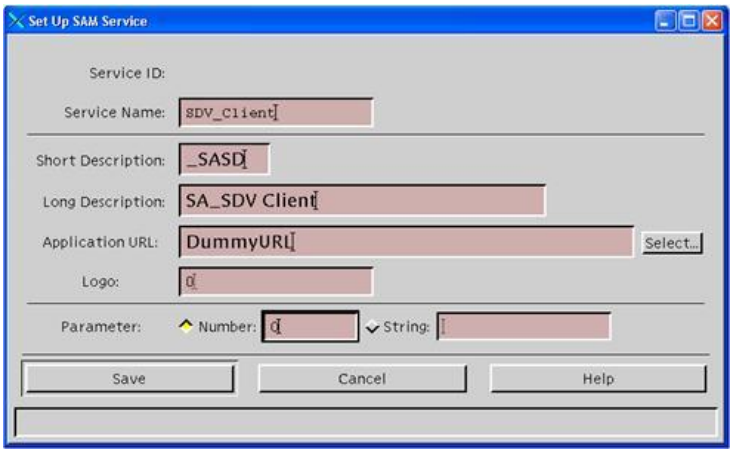
Creating a SAM Service for Switched Digital Services

Creating an SDV SAM service provides SDV functionality for the set-tops and/or tuning adapters that have been deployed in your system. Without an SDV SAM service, SDV functionality is disabled on these devices. This procedure provides instructions for the following methods:

- Enable SDV functionality for all set-tops and tuning adapters
- Enable SDV functionality for all tuning adapters

1 Click the **Application Interface Modules** tab, and then click **SAM Service**. The SAM Service List window opens.

2 Click **File** and select **New**. The Set Up SAM Service window opens.



3 Follow these instructions to enter data in the fields of the Set Up SAM Service window:

- **Service Name**: Enter a name that you want to use to identify the SDV service, such as SDV Client.
- **Short Description**: Enter one of the following depending upon the devices that you want to enable for SDV functionality:
  - **For set-tops and tuning adapters:** Enter **_SASD** as the brief description for the service.

    Important: "_SASD" is the required entry for the Short Description field.
  - **For tuning adapters only:** Enter **_TASD** as the brief description for the service.

    Important: "_TASD" is the required entry for the Short Description field.
- **Long Description**: Enter a detailed description for the SDV service, such as SA_SDV Client. This information is for your use only. Subscribers will not see the text that you enter here.

  Note: You can enter up to 32 alphanumeric characters.
- **Application URL**: Enter **DummyURL**.
- **Logo**: Enter **0** as the number for the logo that is related to the SDV service.
- **Parameter**: Click in the **Number** field and type **0** for the SDV service.

4 Click **Save** to save the service information in the DNCS database and close the Set Up SAM Service window. The SAM Service List window updates to include the new service with its system-assigned service ID and application URL tag.

5 To modify this SDV SAM functionality so that a set-top or tuning adapter acquires its SDV service group ID from the mini carousel and not from SDV service groups that have been manually entered on the DNCS, go to ***Adding a Scan List of SDV Frequencies (Optional)*** (on page 38). Modifying SDV functionality in this way means that operators do not need to enter SDV service groups on the DNCS.

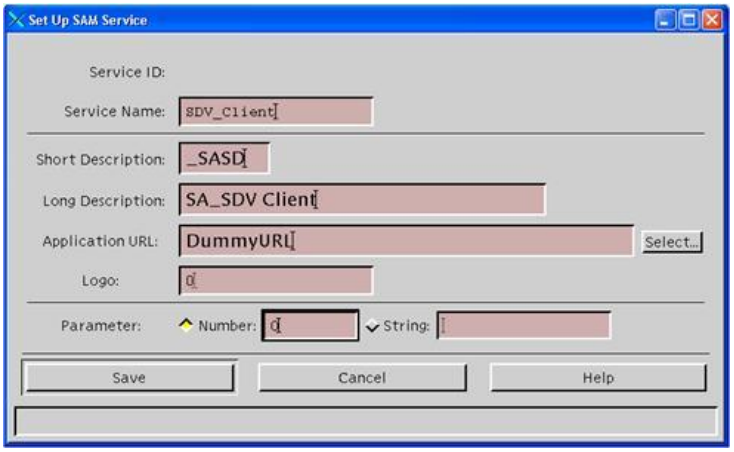
Adding a Scan List of SDV Frequencies (Optional)

Adding a scan list of SDV frequencies to the _SASD or _TASD SAM service URL enables the SDV clients to find a mini carousel and, subsequently, to receive the SDV service group ID from the mini carousel without requiring SDV QAMs or SDV service groups to be entered on the DNCS.

Important: Before provisioning a scan list on the DNCS, please determine the common QAM frequencies used to access SDV across the system.

Complete the following steps to add a scan list of frequencies to your SAM URL.

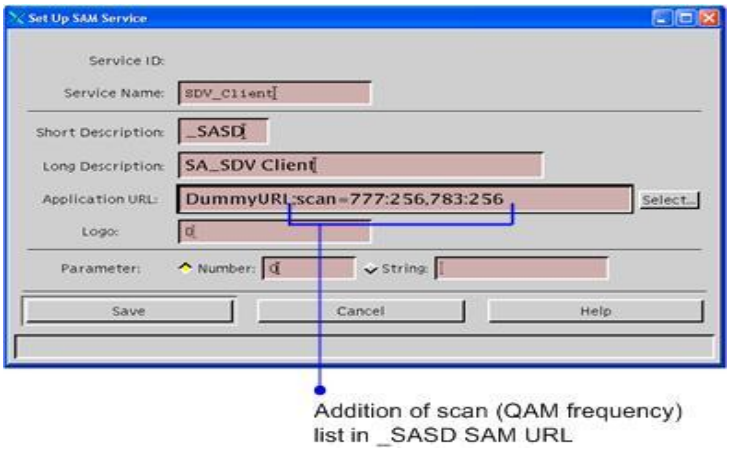
1. Click the **Application Interface Modules** tab, and then click **SAM Service**. The SAM Service List window opens.
2. Double click the _SASD SAM or _TASD SAM service. The Set Up SAM Service window for the SDV SAM service opens, similar to the following example.



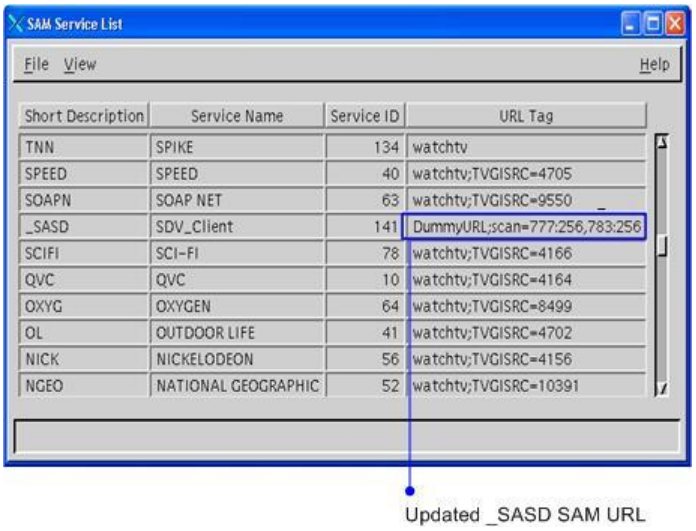
3. Click in the Application URL line and place your cursor at the end of the URL statement.
4. Append the line to include your scan list in the following format: **;scan=<freq>:<mod>,<freq>:<mod>,<freq>:<mod>,...** where frequency is defined in MHz and <mod> is the QAM modulation format.

   Important: You may enter up to 25 frequency:modulation pairs.

   Example: DummyURL;scan=777:256,783:256



5 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.



6 Click **File** and select **Close** to close the SAM Service List.

Enable SDV Functionality for Specific Explorer Set-Tops and/or Tuning Adapters

Overview

This section describes the procedures for enabling the SDV functionality on specific Explorer set-tops and tuning adapters. To enable SDV functionality for certain set-tops and tuning adapters, you must complete the following procedures, which are provided in this section:

- **Create an SDV Package.** By creating a package and then later assigning the package to certain set-tops, you control which set-tops and tuning adapters are enabled for SDV functionality: only set-tops and tuning adapters assigned to the SDV package are enabled for SDV functionality.
- **Create a SAM Service for the SDV Package.** Creating a SAM service for the package allows you to associate the SAM service with the SDV package. Making this association links the package to SDV functionality. If the package is not linked to a SAM service, no functionality is assigned to the package.
- **Authorize Set-Tops and Tuning Adapters for the SDV Package.** Authorizing specific set-tops and tuning adapters for the SDV package enables these set-tops and tuning adapters to receive the SDV SAM service and, in turn, enables them for SDV functionality. Set-tops and tuning adapters that are not authorized for the SDV package are not enabled for SDV functionality and are unable to display SDV services.

Important: If you want to enable SDV functionality globally (for all deployed set-tops and tuning adapters), skip this section and go to ***Enable SDV Functionality for All Explorer Set-Tops and/or Tuning Adapters*** (on page 37).

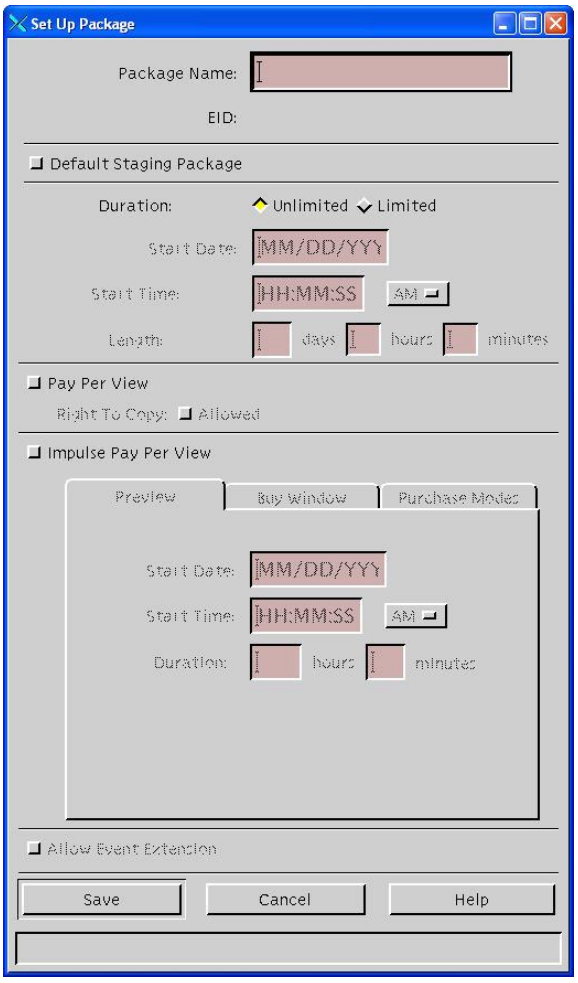
Creating an SDV Package

Packages allow you to deliver secure services to specific set-tops and tuning adapters by controlling the devices allowed to access a service; only set-tops and tuning adapters that receive the SDV package are able to use the SDV service.

1 From the DNCS Administrative Console, click the **DNCS** tab and then select the **System Provisioning** tab.

2 Click **Package** to open the Package List window.

3 From the **File** menu, select **New**. The Set Up Package window opens.



4 Type a name in the **Package Name** field.

Notes:

- Enter the package name that your billing system uses to enable SDV functionality. The name that you enter here must exactly match the package name that your billing system uses.
- If necessary, contact your billing system operator to obtain the correct package name.

5 Click **Save** to save this package in the DNCS database and close the Set Up Package window. The package appears in the Package List window.

6 From the Package List window, select the package you created.

7 Click **File** and select **Open**. The Set Up Package window opens for the package you selected.

8 Record the number shown in the EID field here: _____

Note: The number shown in the EID field is in hexadecimal format.

9 Click **Cancel** to close the Set Up Package window and return to the Package List window.

10 Click **File** and select **Close** to close the Package List window and return to the DNCS Administrative Console.

11 Refer to the hexadecimal conversion table in Appendix E of this document to convert the EID from hexadecimal format to decimal format, and then write the decimal format of the EID here: _____

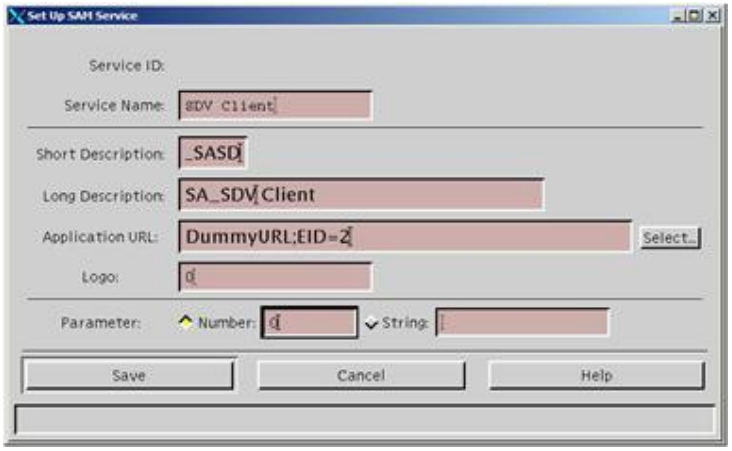
Creating a SAM Service for the SDV Package

Creating an SDV SAM service provides functionality for the SDV package that you just created. Without an SDV SAM service, the package has no functionality. Complete the following procedure to create a SAM service for SDV functionality. This procedure provides instructions for the following methods:

- Enable SDV functionality for specific set-tops and tuning adapters
- Enable SDV functionality for specific tuning adapters

1 Click the **Application Interface Modules** tab, and then click **SAM Service**. The SAM Service List window opens.

2 Click **File** and select **New**. The Set Up SAM Service window opens.



3 Follow these instructions to enter data in the fields of the Set Up SAM Service window:

- **Service Name**: Enter a name that you want to use to identify the SDV service, such as SDV Client.
- **Short Description**: Enter one of the following depending upon the devices that you want to enable for SDV functionality:
  - **For specific set-tops and tuning adapters:** Enter **_SASD** as the brief description for the service.

    Important: "_SASD" is the required entry for the Short Description field.
  - **For specific tuning adapters:** Enter **_TASD** as the brief description for the service.

    Important: "_TASD" is the required entry for the Short Description field.
- **Long Description**: Enter a detailed description for the SDV service, such as SA_SDV Client. This information is for your use only. Subscribers will not see the text that you enter here.

  Note: You can enter up to 32 alphanumeric characters.
- **Application URL**: Enter **DummyURL;EID=#**, replacing the # symbol with the decimal equivalent of the EID belonging to the SDV package.

  Note: To obtain this number, refer to step 11 of ***Creating an SDV Package*** (on page 42).
- **Logo**: Enter **0** as the number for the logo that is related to the SDV service.
- **Parameter**: Click in the **Number** field and type **0** for the SDV service.

4 Click **Save** to save the service information in the DNCS database and close the Set Up SAM Service window. The SAM Service List window updates to include the new service with its system-assigned service ID and application URL tag.

5 To modify this SDV SAM functionality so that a set-top or tuning adapter acquires its SDV service group ID from the mini carousel, and not from SDV service groups that have been manually entered on the DNCS, go to ***Adding a Scan List of SDV Frequencies (Optional)*** (on page 44). Modifying SDV functionality in this way means that operators do not need to enter SDV service groups on the DNCS.

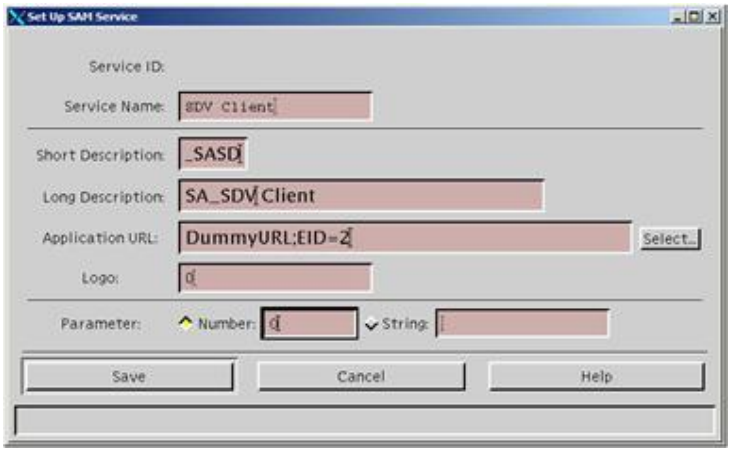
Adding a Scan List of SDV Frequencies (Optional)

Adding a scan list of SDV frequencies to the _SASD or _TASD SAM service URL enables the SDV clients to find a mini carousel and, subsequently, to receive the SDV service group ID from the mini carousel without requiring SDV QAMs or SDV service groups to be entered on the DNCS.

Important: Before provisioning a scan list on the DNCS, please determine the common QAM frequencies used to access SDV across the system.

Complete the following steps to add a scan list of frequencies to your SAM URL.

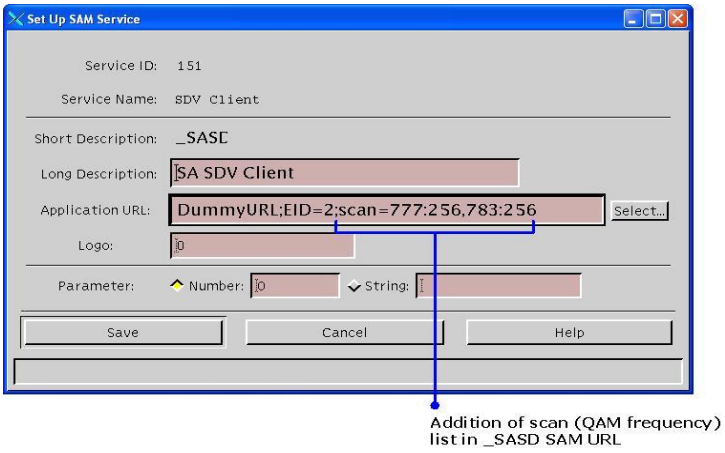
1. Click the **Application Interface Modules** tab, and then click **SAM Service**. The SAM Service List window opens.
2. Double click the _SASD SAM or _TASD SAM service. The Set Up SAM Service window for the SDV SAM service opens, similar to the following example.



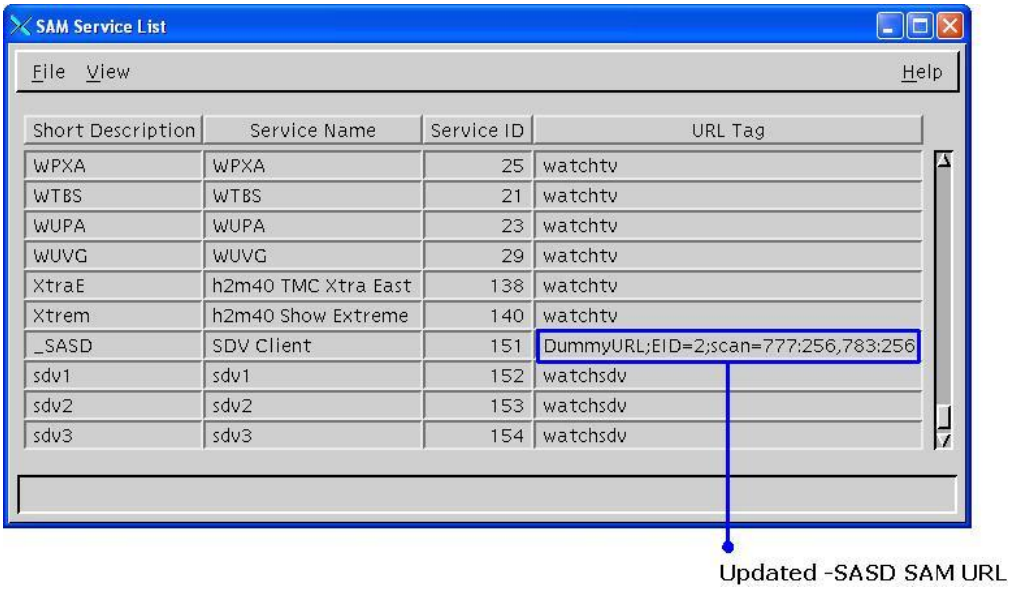
3. Click in the Application URL line and place your cursor at the end of the URL statement.
4. Append the line to include your scan list in the following format: **;scan=<freq>:<mod>,<freq>:<mod>,<freq>:<mod>,...** where frequency is defined in MHz and <mod> is the QAM modulation format.

   Important: You may enter up to 25 frequency:modulation pairs.

   Example: DummyURL;EID=2;scan=777:256,783:256



5 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.



6 Click **File** and select **Close** to close the SAM Service List.

Authorizing DHCTs for a Package

Authorizing specific set-tops and tuning adapters for the SDV package enables these set-tops and tuning adapters to receive the SDV SAM service and, in turn, enables them for SDV functionality. Set-tops and tuning adapters that are not authorized for the SDV package are not enabled for SDV functionality and are unable to display SDV services. Complete the following instructions to authorize a set-top or tuning adapter for the SDV service.

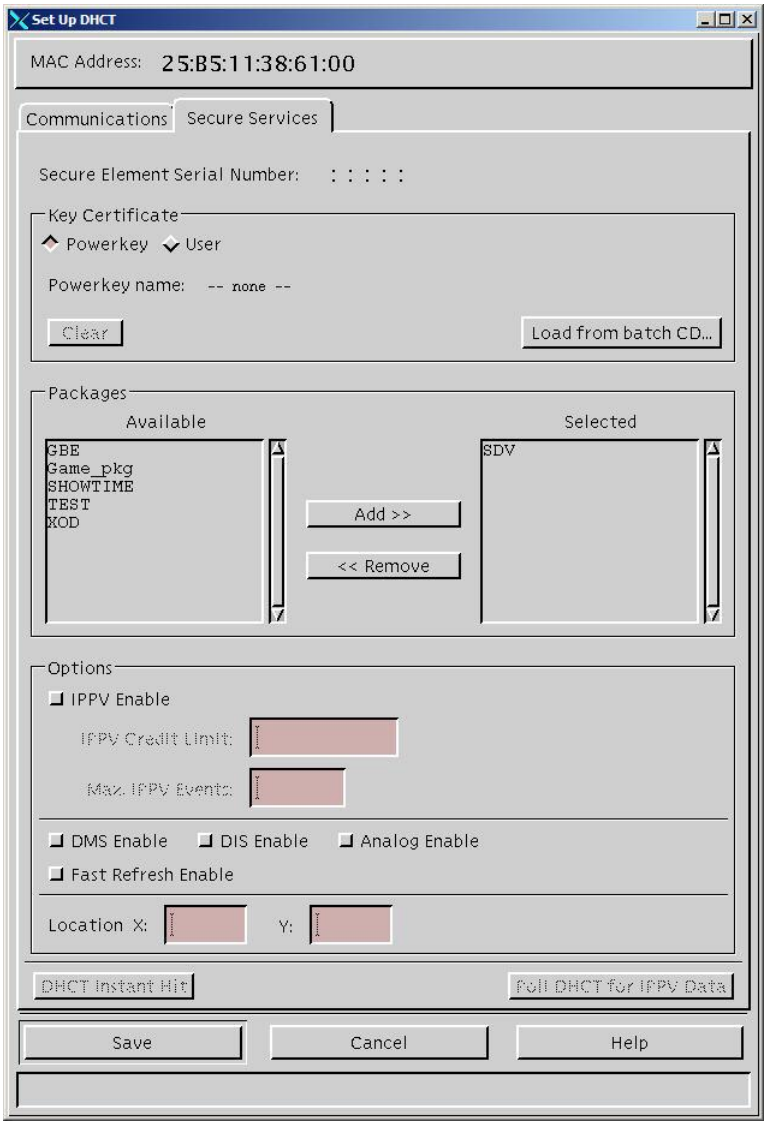
1 Click the **Home Element Provisioning** tab and then click **DHCT**. The DHCT Provisioning window opens.

2 Click **Open** and select one of the following options:

- **By MAC Address**: Enter the MAC address for the set-top.
- **By IP Address**: Enter the IP address for the set-top.
- **By Serial Number**: Enter the serial number for the set-top.

3 Click **Continue**. The Set Up DHCT window opens for the test DHCT.

4 Click the **Secure Services** tab.



5 Scroll through the **Available** field in the Packages area of the window and click to select the SDV package that you want the DHCT to be able to access.

6 Click **Add**. The package name you selected moves into the Selected field.

7 Click **Save**.

8 Click **DHCT Instant Hit** to update the entitlement identification (EID) value.

9 Was the DHCT Instant Hit successful?

- If **yes**, you have completed these procedures.
- If **no**, call Cisco Services.

10 Repeat steps 2–9 for all DHCTs that are using this package.

Set Up a Single or Redundant SDV Multicast Source

Overview

This section describes how to set up a single or a redundant SDV multicast source for SDV services. An SDV multicast source allows the DBDS to successfully deliver the SDV service to subscribers. A redundant SDV multicast source allows the DBDS to have a backup option in the event that SDV services cannot be delivered using the primary SDV multicast source.

Depending on your system needs, refer to one of the following sections to set up an SDV multicast source:

- ***Using an Existing Source for SDV Services*** (on page 48)
- ***Creating a New SDV Multicast Source*** (on page 30)

Notes:

- Before proceeding with this section, Cisco recommends that you update the SDV Server software, if needed.
- You must have video successfully streaming before continuing in this section.

Using an Existing Source for SDV Services

Because you are using an existing source, we assume that you are familiar with the procedures for editing a source; therefore, we have provided an overview of the process, as well as a flowchart, within this section. For detailed instructions about procedures for a process, refer to the *DNCS Online Help (UNIX) 4.2.0.3* (part number 4012122). For details about SDV-specific fields, refer to ***Creating a New SDV Multicast Source*** (on page 30) and ***Creating a Source Definition for a New Source*** (on page 51).

- **Teardown the existing source definition and create a new one for the source**
  - **a** Teardown the source definition
  - **b** Create a new source definition
  - **c** Set up the source definition for the new session for **Multicast through a netcrypt**
  - **d** Edit the SAM service for SDV services and replace the Application URL with **watchsdv**
  - **e** No change is needed for the Channel Map
  - **f** No change is needed for the Interactive Program Guide (IPG) service

- **Create an additional source definition for the source**

  Note: This option is used when the operator wants both the watchtv and watchsdv source definitions, as well as the SAM services available. Typically this option will be used in an Enhanced Channel Map environment. For details about Enhanced Channel Maps, refer to the *Enhanced Channel Maps User's Guide* (part number 4011413).

  a Create a new source definition

  b Create an additional SAM service for the new source and select watchsdv for the Application URL

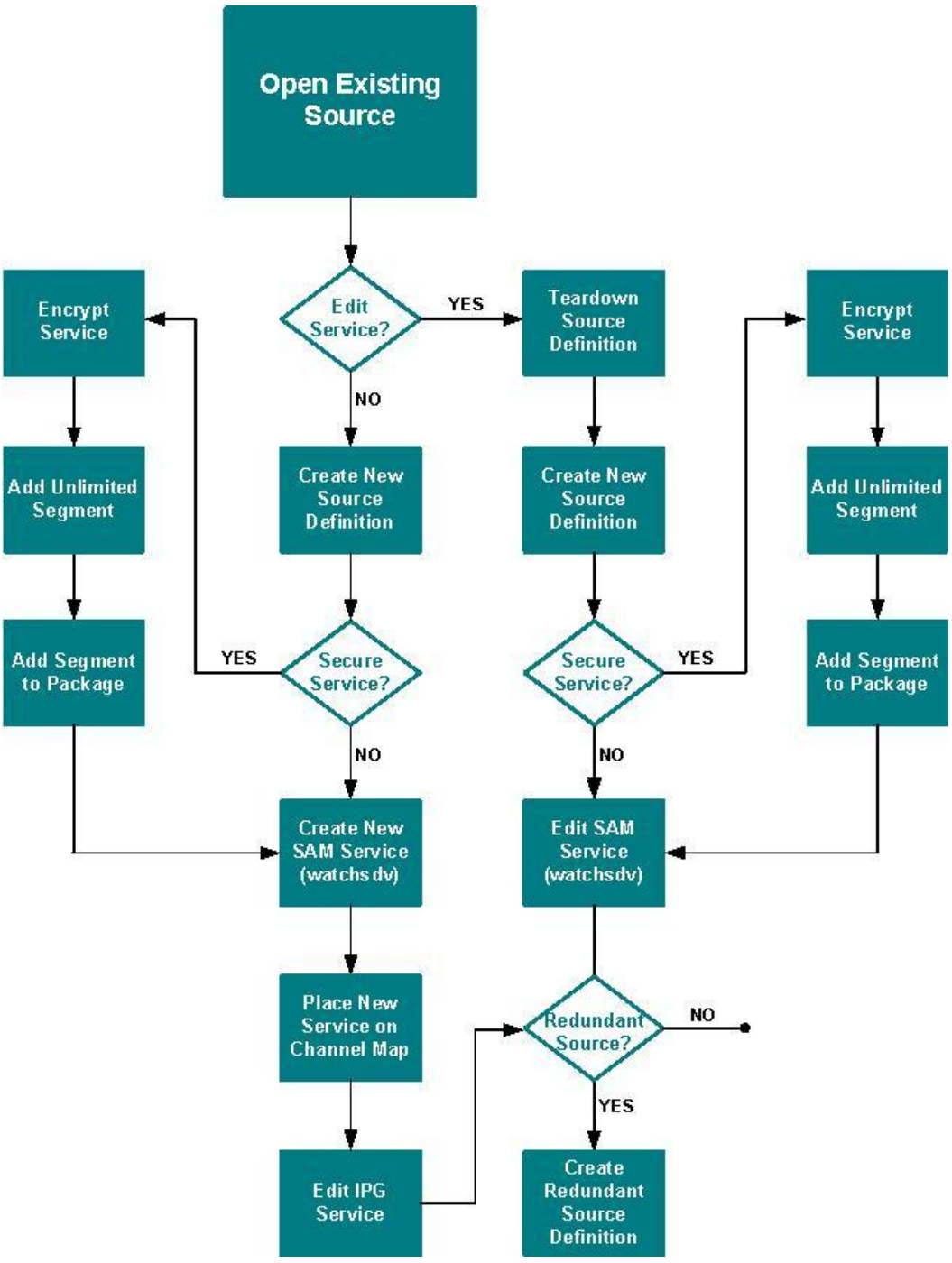
  c Place the new service on the Channel Map

  d Create an IPG service

- **Create a redundant source definition for the existing source**

  Note: It is assumed that you have already set up your SDV source and the primary source definition.

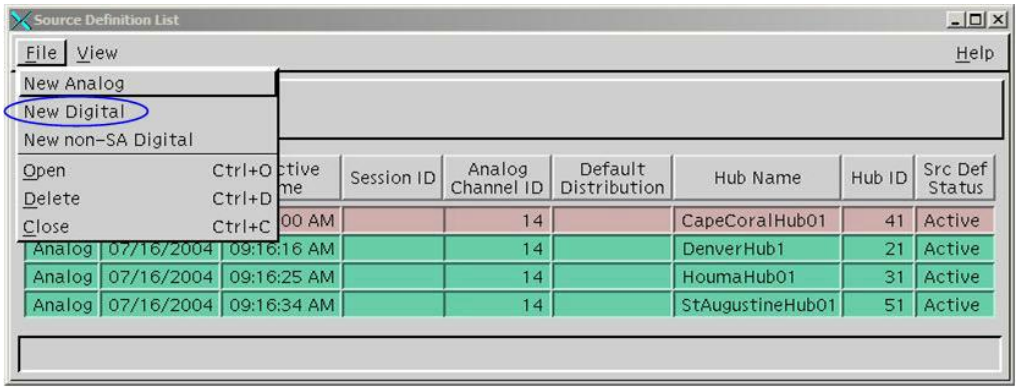
To use an existing source for setting up SDV services, refer to the following diagram.



Creating a Source Definition for a New Source

Complete the following steps to define a source definition (session) for the new source. Sessions define and allocate the resources that the network uses to deliver sources.

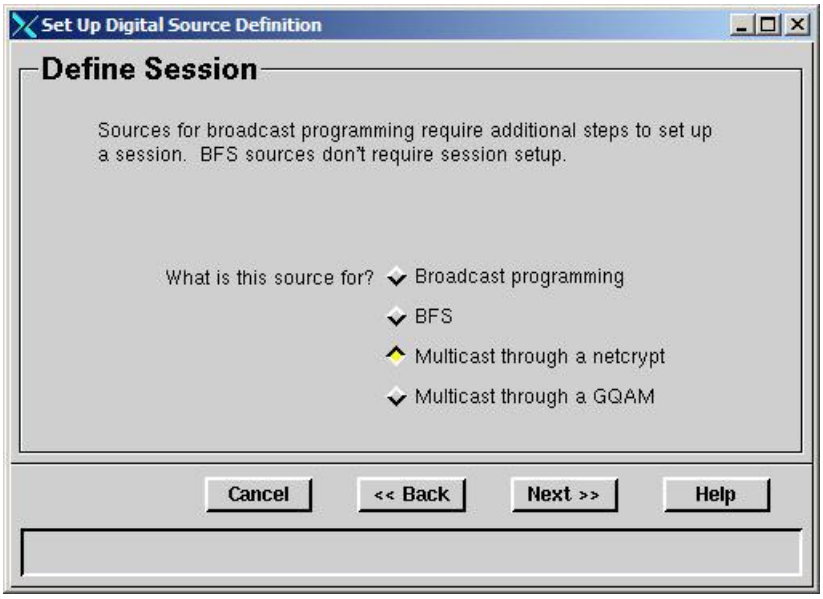
1 From the Source List window, select the new SDV source, click **File**, and then select **Source Definitions**. The Source Definitions window opens.



2 From the File menu, select **New Digital**. The Digital Source Set Up window opens.

3 For the **Session ID** field, type the following: **00:00:00:00:01 nnnn**, where "nnnn" is the source ID that you entered when you added the source to the Source List.

4 Click **Next**. The Define Sessions window opens.

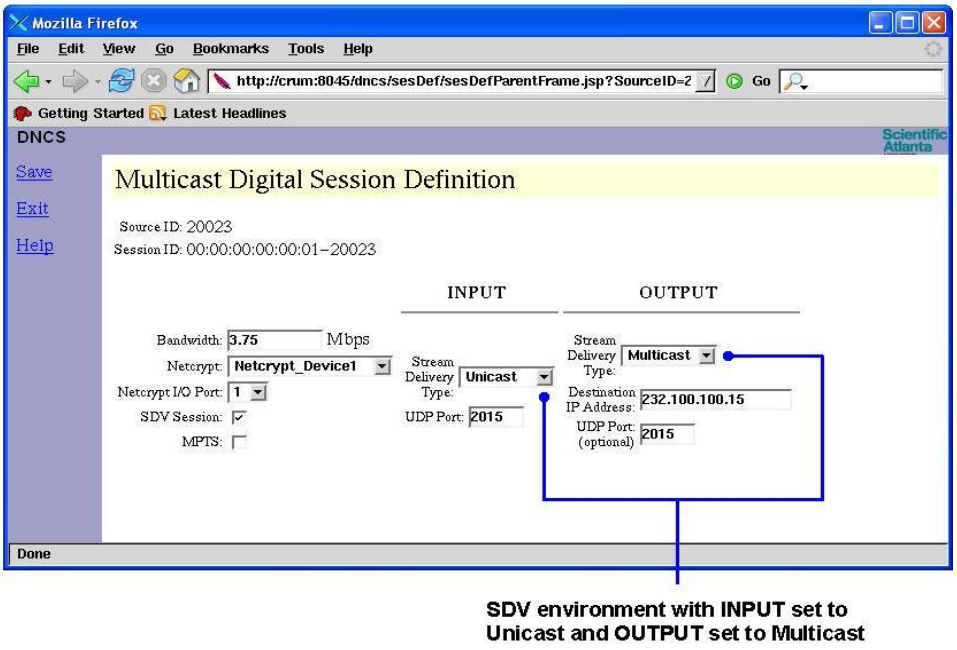


5 Click **Multicast through a netcrypt** and then click **Next**. The Multicast Digital Session Definition window opens.

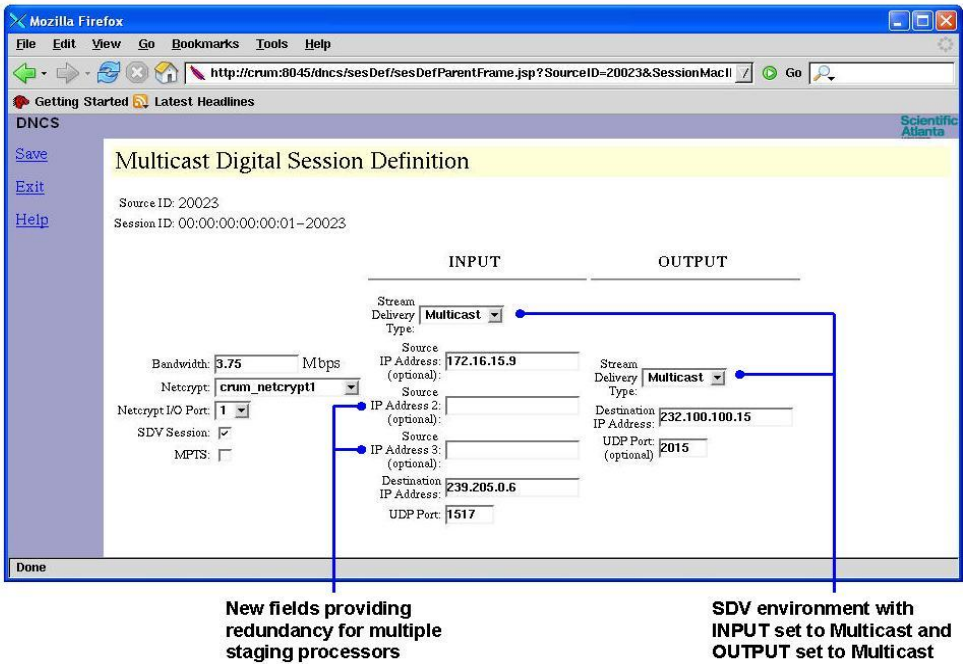
Examples:

Important: Example B is the typical setup in an SDV environment.

A.



B.



6 Enter the appropriate values in the following fields:

- **Bandwidth**: Enter the bandwidth rate for the SDV service.
- **Netcrypt**: Select the Netcrypt device that will be multicasting the content for this service group.
- **Netcrypt I/O Port**: Select the Netcrypt GbE port that will multicasting the content (the same port that is receiving the content from the staging processor or other source).
- **SDV Session**: Click to enable the SDV session.
- **MPTS**: The incoming stream to the Netcrypt is Multi Program Transport Stream (MPTS).

  Important: In an SDV environment, SPTS should be the standard; therefore, MPTS should never be select.
- **Program Field** (only appears when MPTS is selected): Enter the program number from the incoming stream for this session.
- **Stream Delivery Type**: Select **Multicast** or **Unicast** to define how the content is received by the Netcrypt for both INPUT and OUTPUT, and then go to step 7.

  Important: In an SDV environment, sources are typically set up as: Multicast INPUT and Multicast OUTPUT.

7 Select or enter the following values for the appropriate stream delivery type you selected in step 6:

INPUT

- **Multicast**
  - **Source IP Address**: The IP address of the staging processor (for example, DCM, Mentor, BMR, or Terayon device) interface that is sourcing the video.
  - **Source IP Address 2 (optional)**: The IP address of an additional staging processor interface that is sourcing the video. An additional staging processor provides redundancy, if needed.
  - **Source IP Address 3 (optional)**: The IP address of an additional staging processor interface that is sourcing the video. An additional staging processor provides redundancy, if needed.
  - **Destination IP Address**: The destination IP address of the multicast stream incoming to the Netcrypt device.
  - **UDP Port**: The destination UDP port number for the incoming content.
- **Unicast**
  - **UDP Port**: The destination UDP port number for the incoming content.

OUTPUT

- **Multicast**
  - **Destination Multicast IP Address**: The multicast IP address for the destination output source that the Netcrypt device is sending video to.
  - **UDP Port** (optional): The destination UDP port that the Netcrypt device will use when sending the content to the network.

  Notes:
  - If the INPUT Stream Delivery Type is Unicast, Multicast is automatically selected for the OUTPUT Stream Delivery Type.
  - When a multicast IP address is used, the UDP port has no operational value; however, it is beneficial to assign the same UDP port number for all SDV services to ease network troubleshooting.

8 Click **Save**.

9 Are you provisioning a secure service?

- If **yes**, refer to ***Provision a Secure Service*** (on page 58).
- If **no**, go to step 10.

10 Is your client application running SARA?

- If **yes**, go to ***Set Up a New SAM Service for an SDV Multicast Source*** (on page 59).
- If **no**, you have completed the procedures for provisioning the DNCS for SDV. To complete any further procedures, refer to the documentation that accompanies your SDV client application.

Creating a Redundant Source Definition For an Existing Source

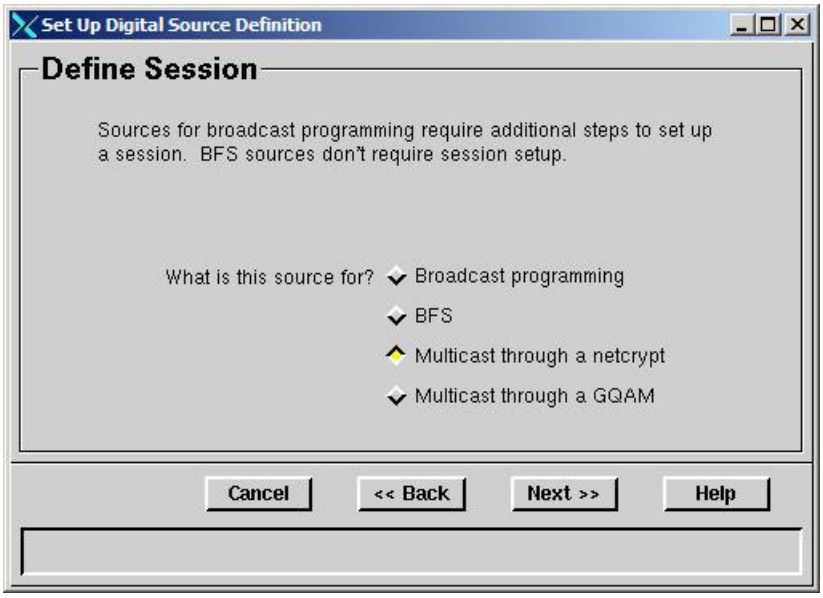
Complete the following steps to define a redundant source definition (session) for an existing SDV source.

1 From the Source List window, select the SDV source, click **File**, and then select **Source Definitions**. The Source Definitions window opens.

2 From the File menu, select **New Digital**. The Digital Source Set Up window opens.

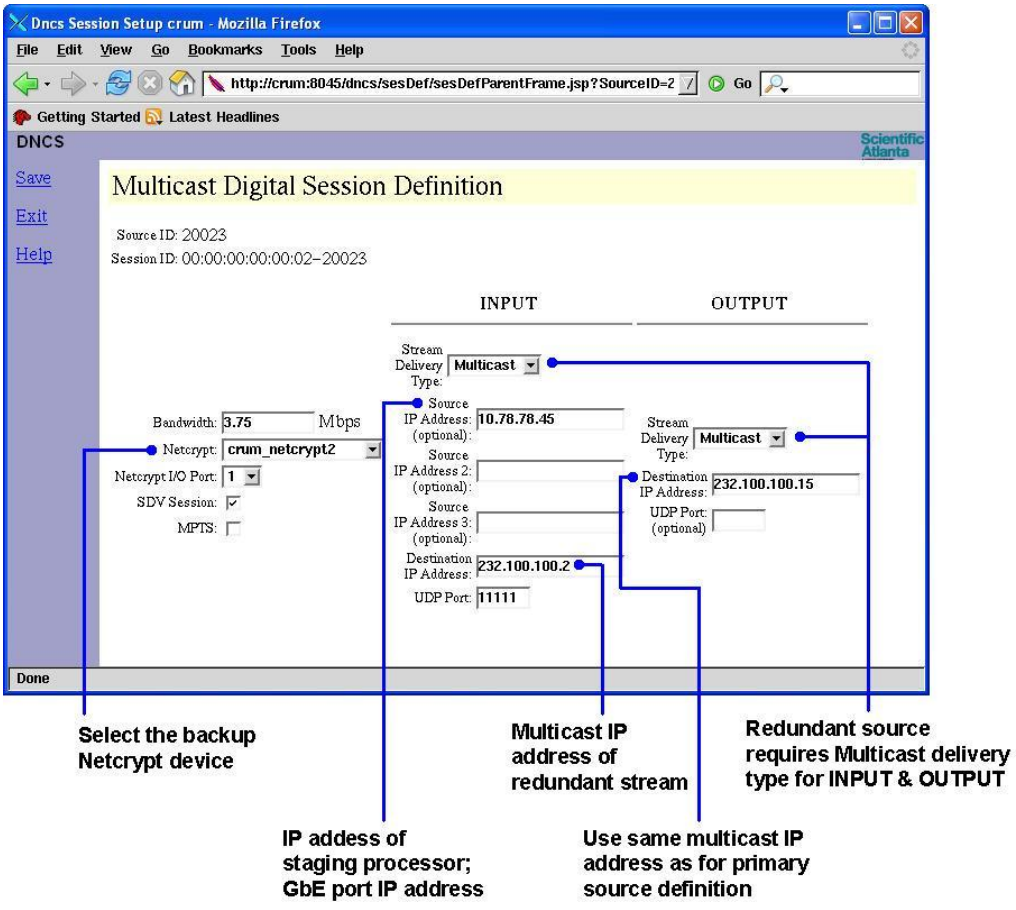
3 For the **Session ID** field, type the following: **00:00:00:00:02 nnnn**, where "nnnn" is the source ID that you entered when you added the source to the Source List.

4 Click **Next**. The Define Session window opens.



5 Click **Multicast through a netcrypt** and then click **Next**. The Multicast Digital Session Definition window opens.

Example:



6 Enter the appropriate values in the following fields:

- **Bandwidth**: Enter the bandwidth rate for the SDV service.
- **Netcrypt**: Select the backup Netcrypt device that will be multicasting the content for this service group.
- **Netcrypt I/O Port**: Select the backup Netcrypt GbE port that will multicasting the content (the same port that is receiving the content from the staging processor or other source).
- **SDV Session**: Click to enable the SDV session.
- **MPTS**: The incoming stream to the Netcrypt is Multi Program Transport Stream (MPTS).

  Important: In an SDV environment, SPTS should be the standard; therefore, MPTS should never be selected.
- **Program Field**: (only appears when MPTS is selected): Enter the program number from the incoming stream for this session.

  Note: Because MPTS must be selected to see this field and SPTS is the standard, you should never see this field.
- **Stream Delivery Type**: Select **Multicast** to define how the content is received by the backup Netcrypt for both INPUT and OUTPUT, and then go to step 7.

  Important: In an SDV environment, backup sources are set up as: Multicast INPUT and Multicast OUTPUT.

7 Select or enter the following values for the appropriate stream delivery type you selected in step 6:

INPUT

- **Multicast**
  - **Source IP Address**: The IP address of the backup staging processor (for example, DCM, Mentor, BMR, or Terayon device) interface that is sourcing the video.
  - **Source IP Address 2 (optional)**: The IP address of an additional backup staging processor interface that is sourcing the video. An additional staging processor provides redundancy, if needed.
  - **Source IP Address 3 (optional)**: The IP address of an additional backup staging processor interface that is sourcing the video. An additional staging processor provides redundancy, if needed.
  - **Destination IP Address**: The destination IP address of the multicast stream incoming to the backup Netcrypt device.
  - **UDP Port**: The destination UDP port number for the incoming content.

OUTPUT

- **Multicast**
  - **Destination Multicast IP Address**: The multicast IP address for the destination output source that the backup Netcrypt device is sending video to.

    Important: This IP address must match the Destination IP Address (INPUT) entered for the primary SDV multicast source definition.
  - **UDP Port** (optional): The destination UDP port that the backup Netcrypt device will use when sending the content to the network.

8 Click **Save**.

Note: For a redundant source definition, you do not need to set up a new SAM service or place the service on the IPG Service List.

Provision a Secure Service

Overview

Secure services can be viewed by only those subscribers who are properly authorized. Subscribers who have purchased the service can then tune to the appropriate channel that is mapped to the service.

Provisioning a Secure Service

1. Refer to the DNCS Online Help for your system release for specific steps to perform the following tasks:
   a. Encrypting the source
   b. Creating an unlimited segment for the source
   c. Assigning the segment to a package
2. Is your client application running SARA?
   - If **yes**, go to ***Set Up a New SAM Service for an SDV Multicast Source*** (on page 59).
   - If **no**, you have completed the procedures for provisioning the DNCS for SDV. To complete any further procedures, refer to the documentation that accompanies your SDV client application.

Set Up a New SAM Service for an SDV Multicast Source

Overview

For each SDV service that you plan to offer to subscribers who are authorized to use an SDV-enabled DHCT, you must set up a SAM service. These SAM services must include the new watchsdv application URL (bfs://resapp/watchsdv). This URL allows DHCTs to use the watchsdv application when displaying an SDV channel.

Setting Up a New SAM Service for an SDV Multicast Source

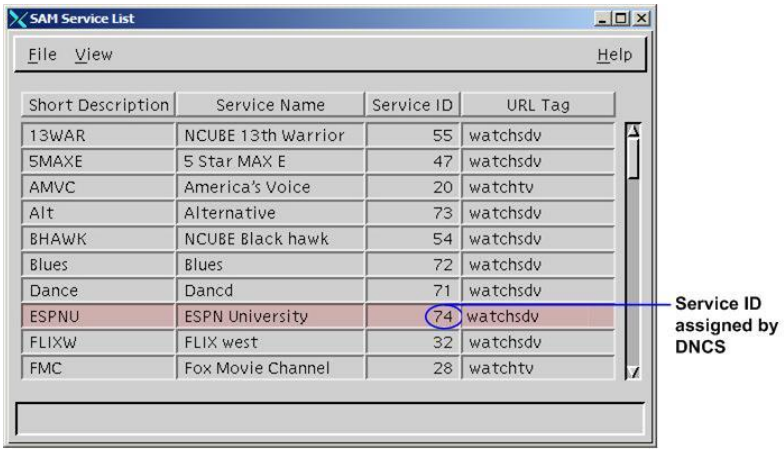
1. Click the **Application Interface Modules** tab, and then click **SAM Service**. The SAM Service List window opens.
2. Click **File** and select **New**. The Set Up SAM Service window opens.

3. In the Application URL field, enter **bfs://resapp/watchsdv** and then enter the appropriate data in the remaining fields of the window.

4 Click **Save**.

Results:

- The Set Up SAM Service window closes.
- The service is added or updated in the SAM Service List.
- The DNCS assigns a service ID for a new service. This service ID is required to place the service on the channel map.



5 Do you want to create another service?

- If **yes**, repeat steps 2–4.
- If **no**, click **File** and select **Close** to close the SAM Service List window.

6 Go to *Place the SDV Service on a Channel Map* (on page 61).

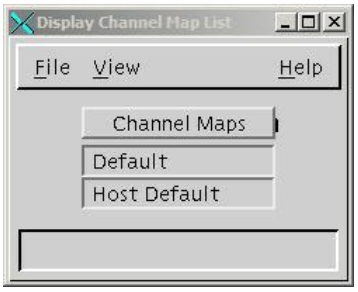
Place the SDV Service on a Channel Map

Overview

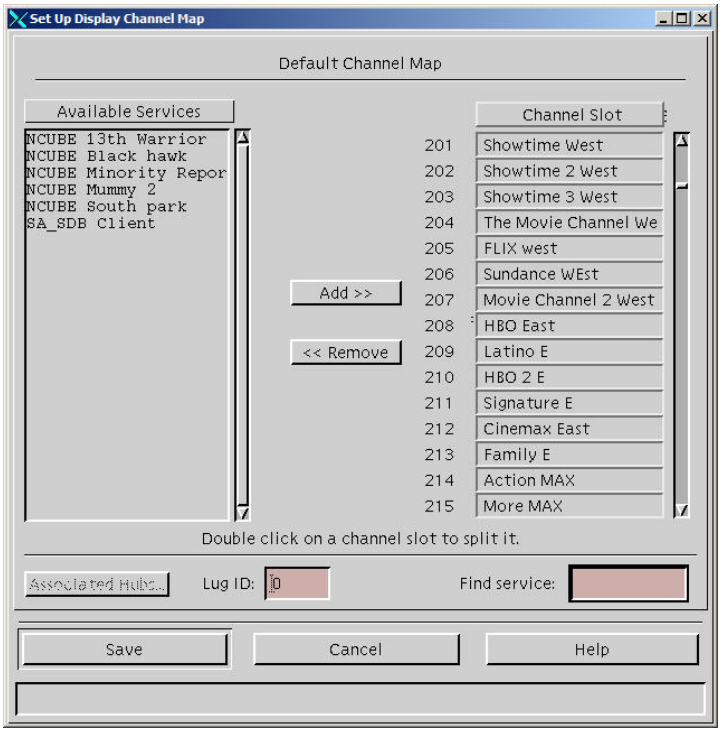
This section describes how to place the services provisioned for SDV on the channel map. This will enable subscribers who are authorized for the SDV application to tune to SDV services.

Placing SDV Services on a Channel Map

1 Click the **Application Interface Modules** tab, and then click **Channel Maps**. The Display Channel Map List window opens.



2 Select the appropriate channel map, click **File**, and select **Open**. The Set Up Display Channel Map window opens for the channel map you selected.



3 Scroll through the **Available Services** list and select the service you want to add to the channel map.

4 Scroll through **Channel Slot** list until you see the channel slot to which you want to assign the service, and then click the channel slot to select it.

5 Click **Add**. The service moves from the Available Services list to the Channel Slot list you selected.

6 Click **Save** to save the channel map information in the DNCS database and close the Set Up Display Channel Map window.

Note: By default, the system waits 20 minutes to build new channel maps. However, the amount of time that elapses between a change to a channel map and the time that a new channel map is built and broadcast to DHCTs varies according to the SAM Update Timer setting. For this reason, allow an appropriate amount of time to pass before testing the service to verify that channels were added.

7 Do you want to add another service to a channel slot?

- If **yes**, repeat steps 3–6.
- If **no**, go to step 8.

8 On the Display Channel Map List window, click **File** and then select **Close**. The Display Channel Map List window closes and the DNCS Administrative Console returns to the forefront.

Place the Service in the IPG Service List (Optional)

Overview

Each service that you create should be included in the IPG service list. This list ensures that the program descriptions, which the DBDS receives from an IPG provider, correctly match each service listed in the IPG.

Note: If you have added a new service to an existing source, you only need to modify the channel slot in the channel map for the new service.

Placing the Service on the IPG Service List

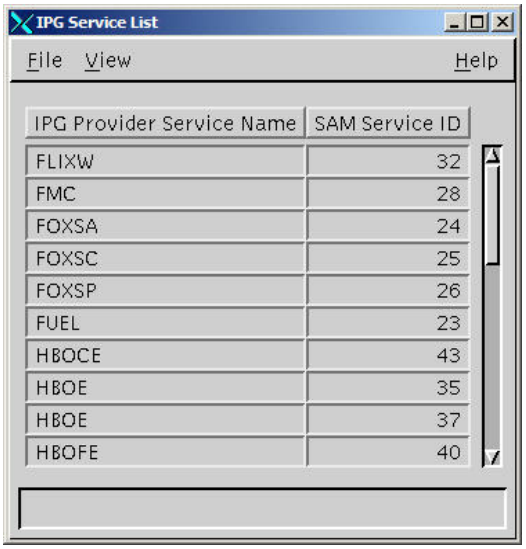
The procedures for placing a service on the IPG Service List differ when you are adding a new service to the channel map as opposed to editing an existing service on the channel map. To add a new service, go to ***Adding a Service to the IPG Service List*** (on page 63). To edit an existing channel slot in the channel map, go to ***Editing an IPG Service*** (on page 65).

Important: We recommend that you perform either service map procedure during a maintenance window as it can take up to 30 minutes.

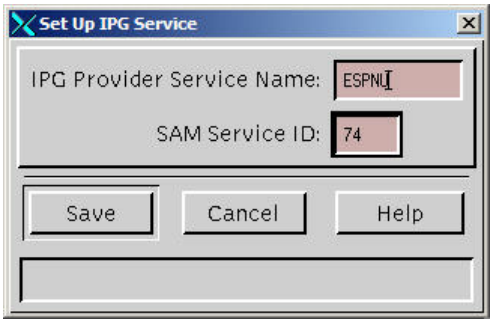
Adding a Service to the IPG Service List

1 Click the **Server Applications** tab, and then click **IPG**. The IPG Server List window opens.

2 Select the appropriate IPG server, click **File**, and then select **Services**. The IPG Service List window opens.



3 Click **File** and select **New** to add a new service to the IPG server. The Set Up IPG Service window opens.



4 In the IPG Provider Service Name field, type the name that your IPG provider has given to the service.

5 In the SAM Service ID, enter the number that the DNCS automatically generated when you entered the service in the SAM Service List.

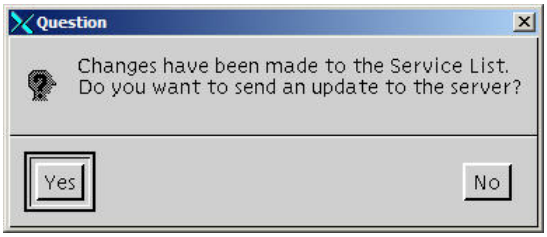
Note: To obtain the SAM service ID, go to step 4 in ***Setting Up a New SAM Service for an SDV Multicast Source*** (on page 59).

6 Click **Save**. The new service is listed in the IPG Service List window.

7 Do you want to add another service to the IPG service list?

- If **yes**, repeat steps 3–6.
- If **no**, go to step 8.

8 From the IPG Server List window, click **File** and select **Close**. The following message appears.



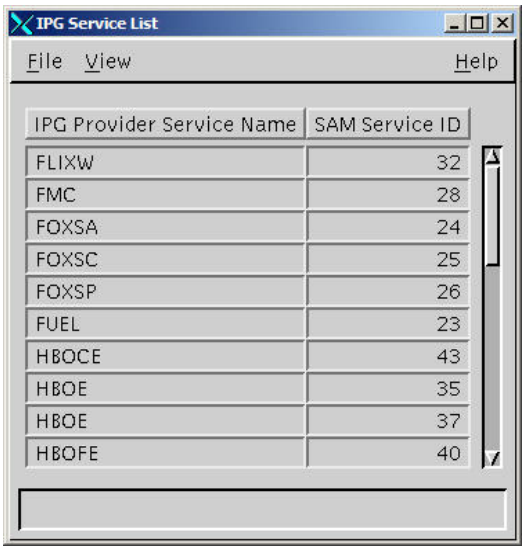
9 Click **Yes** to send an update to the server.

10 From the IPG Server List window, click **File** and select **Close**.

Editing an IPG Service

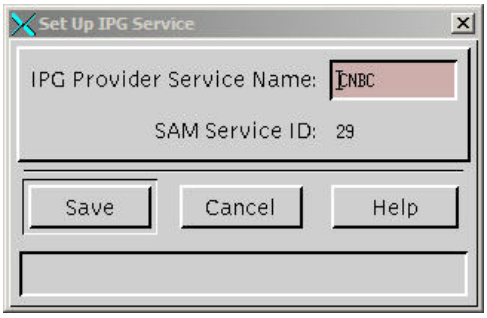
1 Click the **Server Applications** tab, and then click **IPG**. The IPG Server List window opens.

2 Select the appropriate IPG server, click **File**, and then select **Services**. The IPG Service List window opens.



3 From the IPG Service List window, select the row of the desired IPG service.

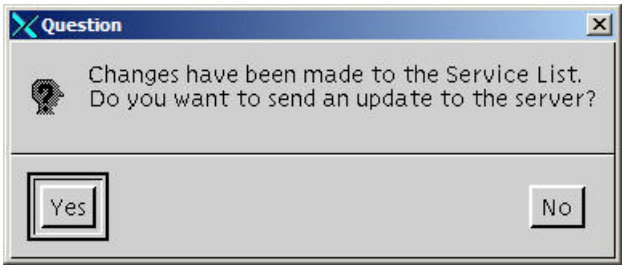
4 From the File menu, click **Open**. The Set Up IPG Service window opens.



5 Edit the service name in the IPG Provider Service Name area and then click **Save**.

Note: You can only change the IPG Provider Service Name. You cannot change the SAM Service ID.

6 From the Set Up IPG Service List window, click **File** and select **Close**. A message appears asking if you want to send an update to the server.



7 Click **Yes** to send an update to the server.

3

Downloading New Software to an SDV Server

Introduction

When new software images are available for an SDV server, they can be downloaded directly to an SDV server from the DNCS. Prior to downloading new software to an SDV server for the first time, you must run an sdvProvisionKeys script to synchronize the keys used by the download protocol. Running this script for each SDV server only one time enables you to directly download new software from the DNCS for any future software images.

This chapter provides instructions for running the sdvProvisionKeys script for each SDV server that requires a software download, loading the software image onto the DNCS, and downloading new software from the DNCS to each SDV server.

In This Chapter

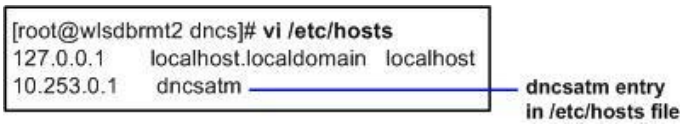
Update the SDV Server Host File

Overview

The hosts file is used to store the host names that are mapped to the IP addresses on the SDV server. This file must include an entry that identifies the dncsatm. This section provides instructions to add the dncsatm entry to the hosts file.

Updating the Host File

1. From the DNCS Administrative Console, click the **Utilities** tab, and then click **xterm**. An xterm window opens.
2. Complete the following steps to log on to the xterm window as root user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Type the following command: **cd /etc**
4. Open the hosts file using an editor of your choice. The hosts file opens in editor mode.



   Note: This hosts file is a sample that includes the dncsatm entry.

   Important: Do not add or remove any entries in your host file unless you are absolutely certain that they are not required for your environment.
5. Add the dncsatm entry to your hosts file.
6. Save the changes to the hosts file and exit the editor.
7. Remain logged in as root user and go to ***Run the sdvProvisionKeys Script*** (on page 69).

Run the sdvProvisionKeys Script

Overview

The sdvProvisionKeys script is a script that allows you to synchronize the SDV server keys used by the download protocol. The script enables an SDV server to download new software directly from the DNCS.

Important: Run the sdvProvisionKeys script once for each SDV server.

Note: The sdvProvisionKeys script is included in your SDV package.

Running the sdvProvisionKeys Script

Complete the following steps to run the sdvProvisionKeys script for each SDV server that will require new software.

1. From the xterm window where you are logged in as root user, type the following command: **cd /dvs/dncs/bin**
2. Type **./sdvProvisionKeys <IP Address of SDV Server>** and press **Enter**. The script begins to run.

   Note: The script will take a few minutes to complete.
3. Did the script successfully run?
   - If **yes**, the last few lines at the end of the script will resemble the following output.

     ```
     setup ssh/scp access from dncs@172.22.0.10 => dncs@dncsatm...
     success placing private key (/export/home/dncs/.ssh/sdvKey) in 172.22.0.10:/home/dncs/.ssh/dncsatm.dncs
     success placing public key (/export/home/dncs/.ssh/sdvKey.pub) in 172.22.0.10:/home/dncs/.ssh/dncsatm.dncs.pub
     success adding key (/export/home/dncs/.ssh/sdvKey.pub) to local /export/home/dncs/.ssh/authorized_keys
     ```
   - If **no**, contact Cisco Services.
4. Do you want to run the sdvProvisionKeys script for another SDV server?
   - If **yes**, repeat steps 2–3.
   - If **no**, go to step 5.
5. Type **exit** to then press **Enter** to exit from the root user.
6. Keep the xterm window open and go to *Install the SDV Software on the DNCS* (on page 70).

Install the SDV Software on the DNCS

Overview

This section describes how to install the SDV software from our FTP site or from a CD. The file is an RPM (Red Hat Package Manager) file.

Installing the SDV Software from Our FTP Server

Access to the FTP server requires current FTP server site access information. Because many sites do not allow an open Internet connection to the DNCS for security reasons, the following procedure provides generic instructions to access the FTP server and download the software onto the DNCS.

1. From the xterm window, type **cd /export/home/dncs**. This becomes your working directory.
2. Log on to the FTP server.

   Notes:

   - The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

     Note: The address for the FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.
   - The username is **anonymous**.
   - The password is the e-mail address of the person logging in.
3. Choose one of the following options to navigate to the directory in which the file is located:
   - If you are *outside* our firewall, type **cd /pub/scicare/RELEASED**
   - If you are *inside* our firewall, type **cd /external_pub/scicare/RELEASED**
4. Type **bin** and press **Enter**. The system sets the FTP transfer mode to binary.
5. Type **hash** and press **Enter**. The system configures itself to display hash marks that show file-transfer progress.
6. Type **prompt** and press **Enter**. The system indicates that interactive mode is off.
7. Type **get sdb-[version number].rpm** and press **Enter**. The system begins copying the file (or files) from the FTP site to the current directory on your DNCS.
8. Type **bye** and press **Enter** to log out of the FTP server.
9. Go to ***Download New Software to an SDV Server*** (on page 72).

Installing the SDV Software from a CD

1. Insert the SDV CD into the CD-ROM drive of the DNCS.
2. Did the File Manager window display?
   - If **yes**, the CD mounted successfully. Go to step 4.
   - If **no**, type **df –k** to determine where the CD is mounted and go to step 3.
3. Is /cdrom listed in the output?
   - If **yes**, go to step 4.
   - If **no**, call Cisco Services.
4. From the xterm window where you are logged in as root user, type **cd /cdrom/cdrom0** and press **Enter** to access the cdrom0 directory.
5. Type **ls –lr**. The output will resemble the following data.

   -r—r—r-- 1 root root 926380 May 31 14:00 sdb-1.1.7.1.i386
6. Copy the RPM file to the /export/home/dncs directory on the DNCS.

   Example: cp sdb-1.1.7-1.i386.rpm /export/home/dncs
7. Go to ***Download New Software to an SDV Server*** (on page 72).

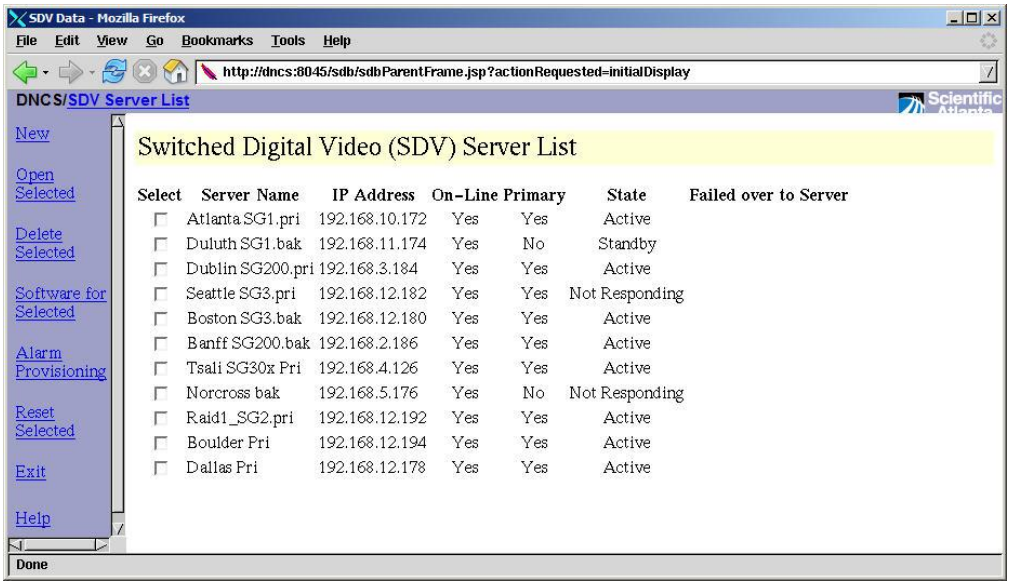
Download New Software to an SDV Server

Overview

This section describes how to download or to download and install new software from the DNCS directly to an SDV server. Procedures are also included that enable you to verify the status of the download and installation.

Downloading the New Software to an SDV Server

1 From the DNCS Administrative Console, click the **Network Element Provisioning** tab, and then click **SDV Server**. The Switched Digital Video (SDV) Server List opens.



2 Click the **Select** box adjacent to the server to which you want to download the new software, and then click **Software for Selected**. The Software Download for Server <Name of SDV Server> window opens.

3 Enter the following in the Software Download for Server <Name of SDV Server> window.

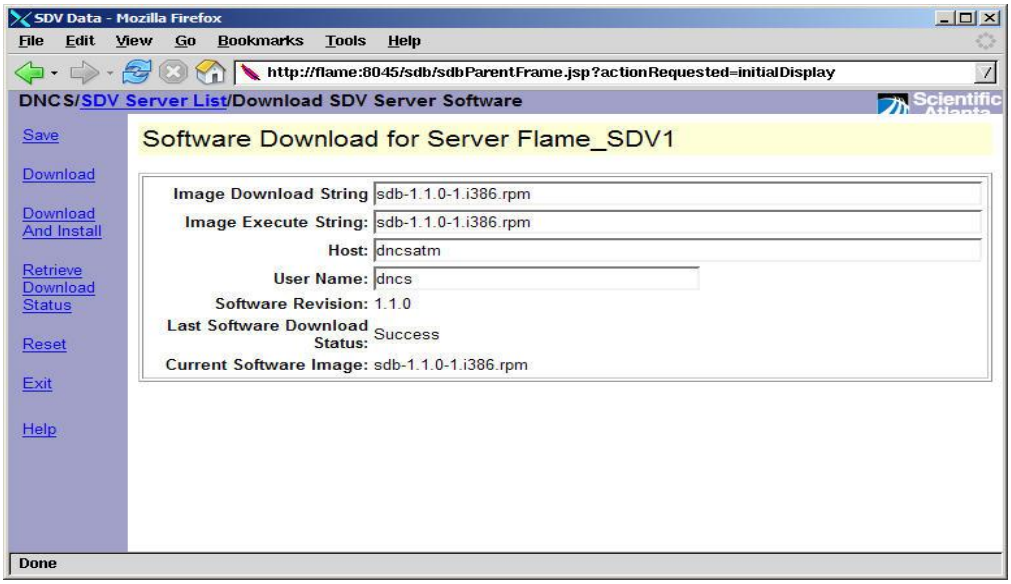
a In the Image Download String and the Image Execute String fields, type the name for the image file (for example, sdb-[version].rpm)

b In the Host field, type **dncsatm**.

c In the User Name field, type **dncs**.

Example:

Note: The screen on your system may differ slightly from the screen shown here.



4 Choose one of the following options to download software to an SDV server:

- Click **Download** to only download the software to the SDV server, and then go to step 5.
- Click **Download And Install** to download and install the software image simultaneously, and then go to step 9.

5 Wait for a "successful download" message and select **OK**. The Last Software Download Status remains InProgress unless Retrieve Download Status is selected.

6 Click **Retrieve Download Status**.

7 Does the download status state "success"?

- If **yes**, you have successfully retrieved the software image. Go to step 8.
- If **no**, contact Cisco Services.

8 Do you want to install the software?

- If **yes**, click **Reset** and then go to step 9.
- If **no**, you have completed the procedures to retrieve the latest software.

9 Wait for "InProgress" to appear in Last Software Download Status field and then click **Retrieve Download Status**.

10 Did the Software Revision and Current Software Image fields change to reflect the new software version?

- If **yes**, you have successfully downloaded and installed the new software.
- If **no**, wait a few minutes and click **Retrieve Download Status** because the download and install function may not have completed. If these fields do not update with the current software, contact Cisco Services.

11 Repeat this procedure for each SDV server that requires the new software image.

4

Customer Information

If You Have Questions

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

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

A

Provisioning PPV Services for SDV

Introduction

This appendix describes how to provision secure pay-per-view (PPV) broadcasts for SDV services. The procedures duplicate some of the procedures used to provision clear channels for SDV services; however, unique procedures exist for PPV broadcasts. These unique procedures will be described in this appendix.

In This Appendix

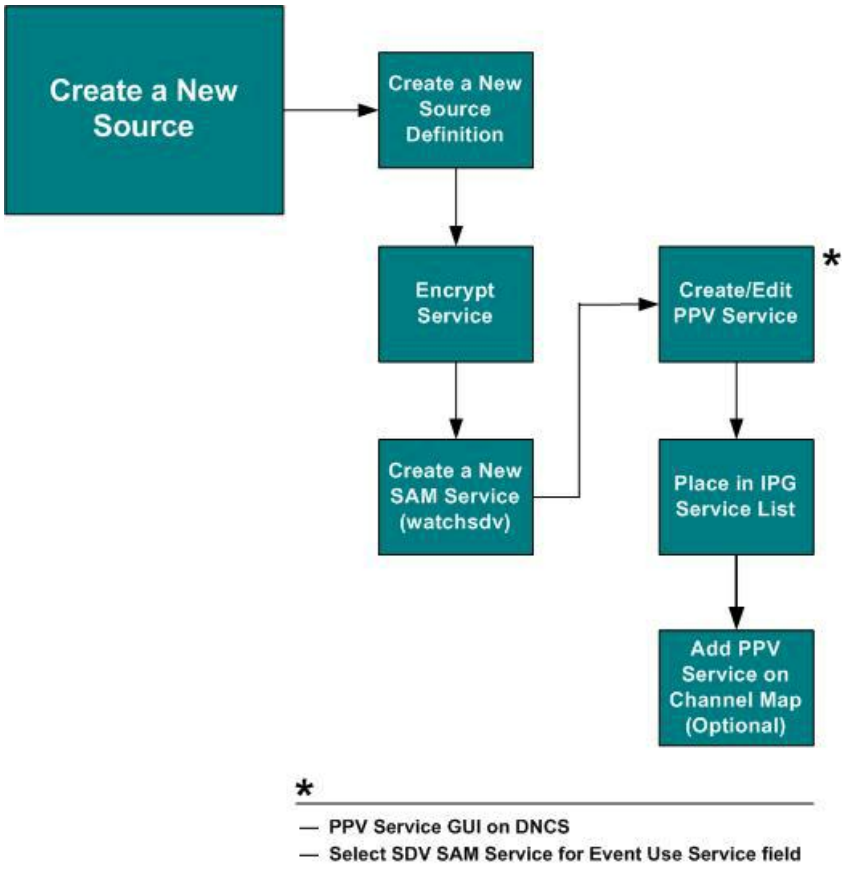
Creating a PPV Service for SDV

Introduction

Provisioning PPV broadcasts requires you to create a source to deliver content to subscribers, as well as to define and build a session that delivers the data to set-tops. After you create the source and encrypt it, you will create a SAM Service that includes the watchsdv URL.

Unlike clear services, you must create a PPV service using the PPV Service feature on the DNCS GUI. Because the system automatically registers the PPV service with SAM, the service is defined with the **bfs://resapp/ippv** application URL. Therefore, when creating or editing an existing PPV service for SDV, you must link the service to the SDV SAM service (watchsdv URL) in the Event Use Service field within the PPV Service GUI.

Example: Flowchart to create a new PPV service for SDV



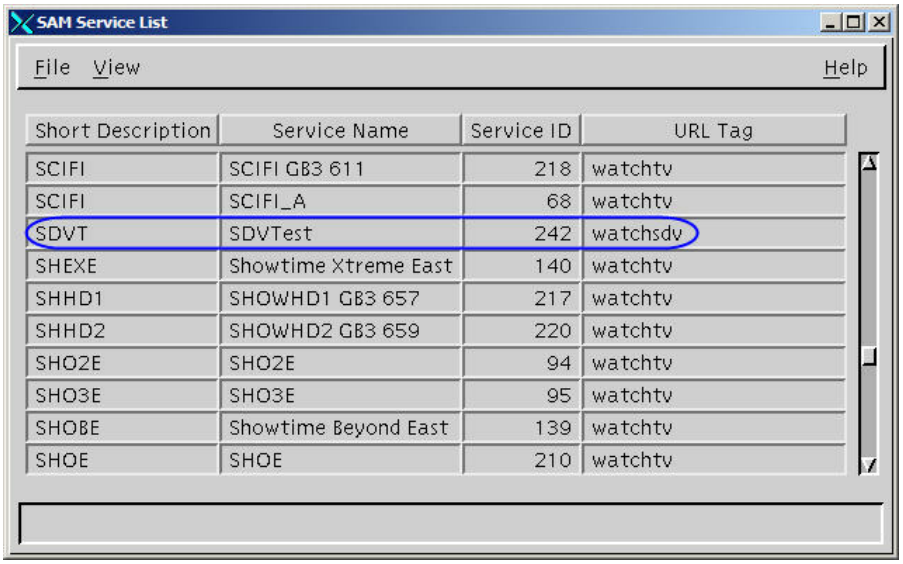
Overview of Procedures to Create PPV Service for SDV

Provisioning a PPV Service for SDV

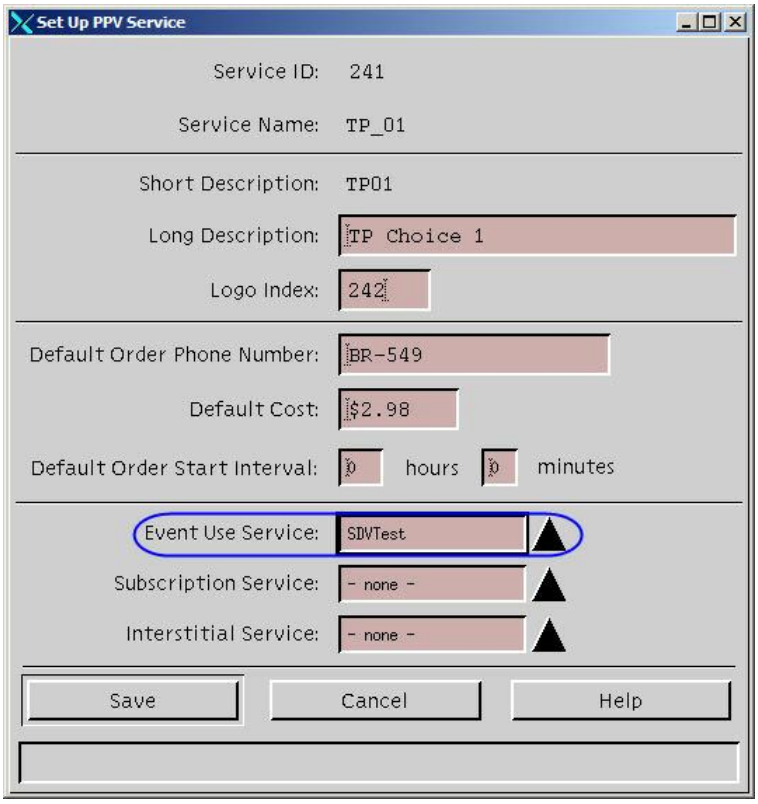
To provision a PPV service for SDV, use the following outline as a guide.

1 Create or edit a source definition that is enabled for SDV.

2 Create a SAM service that includes the watchsdv URL.



3 Using the PPV Service GUI on the DNCS, select the PPV SAM Service (set up for SDV) from the Event Use Service field.



Results:

- After saving this information, a new SAM Service is created with the bfs://resapp/ippv URL.
- The newly created SAM Service is placed on the switched digital channel map.

B

Reducing the Number of Shell Sessions for Existing Service Groups

Introduction

SDV requires the creation of shell sessions, each of which contains a session identifier (session ID), a nominal bandwidth (capacity or throughput), and an RF carrier assignment. You can think of a shell session as a pipe used to facilitate a program request from the SDV server by binding it with a desired program stream.

Whenever the system resource manager (SRM) processes are restarted, no new exclusive sessions can be created (for example, no new VOD sessions can be created). When there are a large number of shell sessions, the time in which new exclusive sessions cannot be created is extended.

Therefore, to reduce the number of shell sessions and expedite this process we recommend changing the fundamental bandwidth unit to 3.75 Mbps and the session group rate to 37.5 Mbps. This will also reduce the number of sessions requests from the SDV server to the DNCS,

This appendix describes the procedures to reduce the number of shell sessions for existing service groups defined on the DNCS for SDV.

Important: If you are provisioning SDV for the first time, follow the procedures in Chapter 2, ***Provisioning SDV Services on the DNCS*** (on page 13).

In This Appendix

Overview

You will need to perform the following procedures to reduce the number of shell sessions for existing service groups:

Important: These procedures should be performed during a maintenance window.

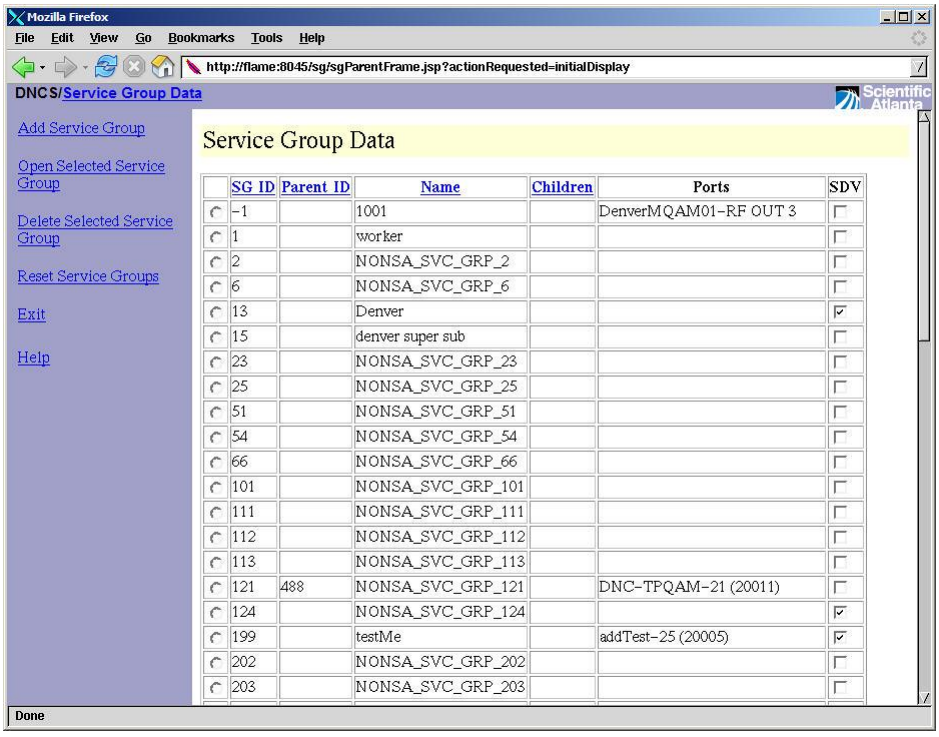
- Change the maximum bandwidth for each SDV service group to zero (tears down the shell session for the service group)
- Modify the fundamental bandwidth unit on the DNCS from 1.875 Mbps to 3.75 Mbps
- Modify the maximum bandwidth, contiguous bandwidth, and rate on the DNCS for each service group

  Example for 1 QAM:

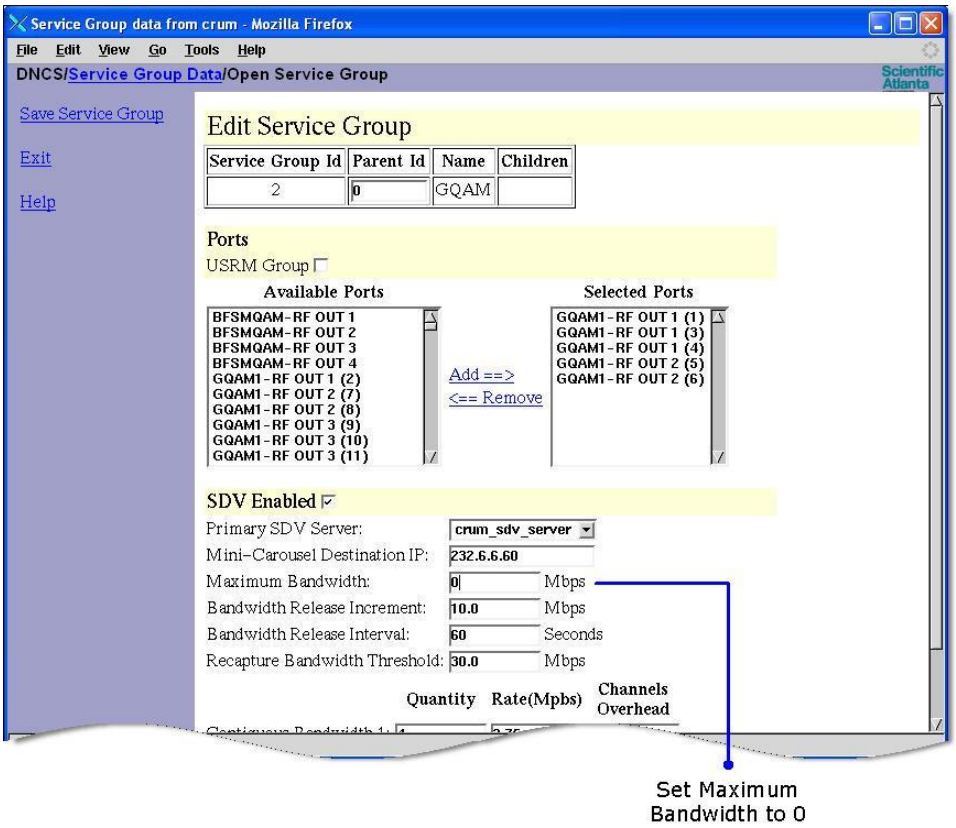
  - Maximum Bandwidth = 37.5 Mbps
  - Contiguous Bandwidth Quantity = 1
  - Contiguous Bandwidth Rate = 37.5 Mbps

Stopping SDV Processes

1 From the DNCS Administrative Console, click **Network Element Provisioning** and then click **Service Group**. The Service Group Data window opens.



2 Select the radio button for the first SDV-enabled service group and click **Open Selected Service Group**. The Edit Service Group window opens.



3 From the Maximum Bandwidth field, type **0** (zero).

Note: Setting the Maximum Bandwidth to zero will tear down the sessions associated with this service group.

4 Click **Save Service Group**. The Edit Service Group window closes and you are returned to the Service Group Data window.

5 Select the radio button for the next SDV-enabled service group and click **Open Selected Service Group**. The Edit Service Group window opens.

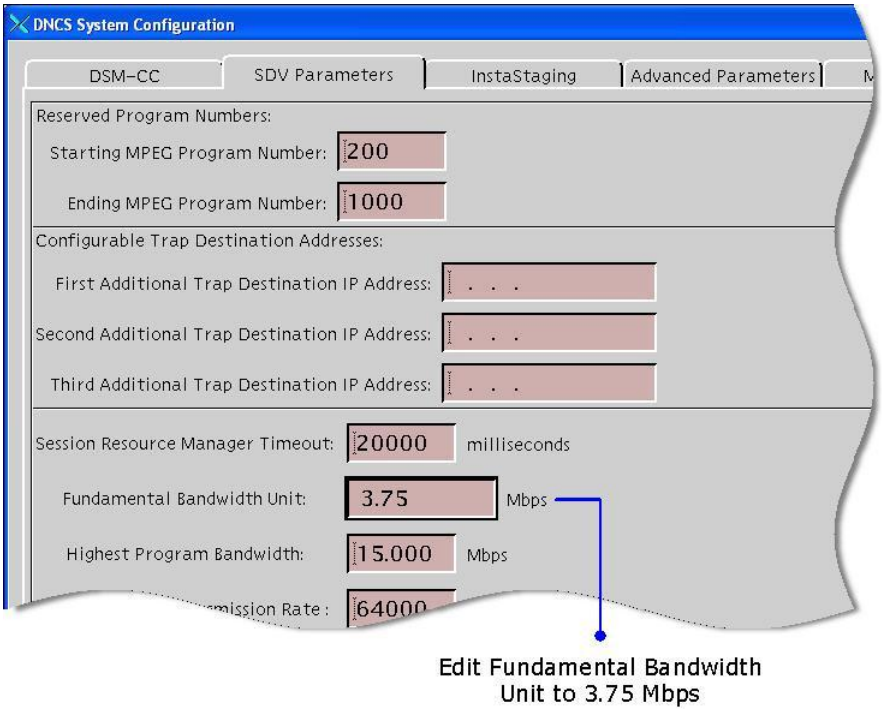
6]From the Maximum Bandwidth field, type **0** (zero).

7 Click **Save Service Group**. The Edit Service Group window closes and you are returned to the Service Group Data window.

8 Repeat steps 5 through 8 for each remaining SDV-enabled service group.

Modifying the Fundamental Bandwidth Unit

1 From the DNCS Administrative Console, click **System Provisioning** and then click **Sys Config**. The DNCS System Configuration window opens.



2 Click the **SDV Parameters** tab.

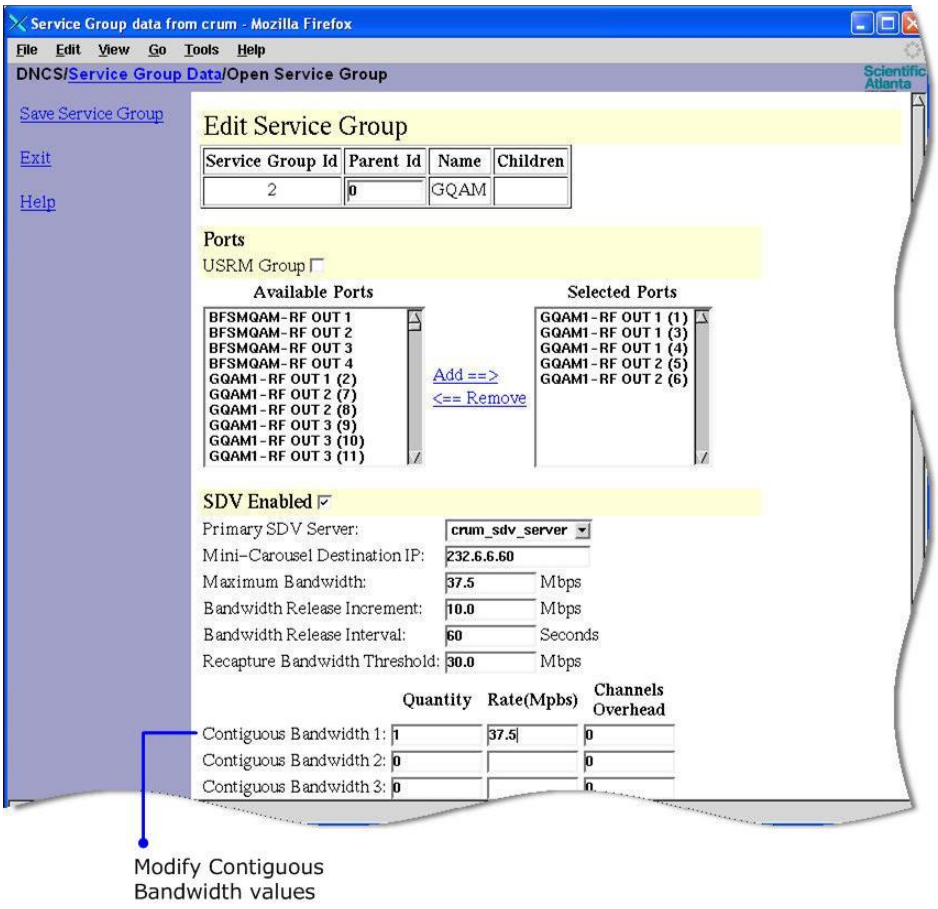
3 From the Fundamental Bandwidth Unit field, highlight the current entry and type **3.75**. Click **Save**.

Modifying the Contiguous Bandwidth Rate

Important: If you have a large number of service groups, you can choose to modify them all at once during a single maintenance window or over a period of days during different maintenance windows.

1 From the DNCS Administrative Console, click **Network Element Provisioning** and then click **Service Group**. The Service Group Data window opens.

2 Select the radio button for the first SDV-enabled service group and click **Open Selected Service Group**. The Edit Service Group window opens.



3 From the Contiguous Bandwidth 1 Quantity field, enter the value that is appropriate for your system.

4 From the Contiguous Bandwidth 1 Rate field, highlight the current value and enter **37.5**.

5 Click **Save Service Group**. The Edit Service Group window closes and you are returned to the Service Group Data window.

6 Select the radio button for the next SDV-enabled service group and click **Open Selected Service Group**. The Edit Service Group window opens.

7 From the Contiguous Bandwidth 1 Quantity field, enter the value that is appropriate for your system.

8 From the Contiguous Bandwidth 1 Rate field, highlight the current value and enter **37.5**.

9 Click **Save Service Group**. The Edit Service Group window closes and you are returned to the Service Group Data window.

10 Repeat steps 6 through 9 for each remaining SDV-enabled service group.

C

Provisioning Services for SDV in an RNCS Environment

Introduction

Important: This procedures in this appendix pertain to sites that are running an SDV server software prior to version 1.4.2 and a procedure for sites that are running version 1.4.2 or later.

This appendix describes how to provision services on the DNCS for SDV in a Remote Network Control System (RNCS) environment. Use the procedures in this appendix, along with the comprehensive procedures for setting up and configuring SDV service on the DNCS in ***Provisioning SDV Services on the DNCS*** (on page 13).

In This Appendix

Before You Begin

Provisioning services for SDV in an RNCS system requires preparation. Preceding the provisioning process, please ensure that your system meets specific prerequisites. Then determine whether you need to add a new service or use an existing service to set up SDV for the remote sites.

Prerequisites

To utilize SDV in an RNCS environment, your system must meet the following prerequisites:

- The DNCS must be operating at System Release (SR) 4.2 SP 2 or later.
- Headend components (for example, GQAM, Netcrypt Bulk Encryptor devices) must include the software versions that are defined in *System Release 2.7/3.7/4.2 Service Pack 2 Release Notes and Installation Instructions* (part number 4019475)
- SDV must be enabled and operating on your system.
- RNCS must be enabled and operating at the main and remote sites for your system.

Should I Create a New Service or Use an Existing Service?

Before adding services to your system, determine whether you need to create a new service or use an existing one. The criteria for making your decision is provided in the following list:

- **Adding a New Service:** If you are running an SDV server software version *prior* to version 1.4.2, you must complete the procedures in ***Creating a New Source ID and Source Definition for a Remote Site*** (on page 89). Procedures include how to add a new source ID and source definition for SDV at an RNCS site.
- **Using an Existing Service**: If you are running SDV server software version 1.4.2 or later, have low memory set-tops on your system, and want to associate individual service groups to unique zones , complete the procedures in ***Creating a Source Definition for an Existing Source ID*** (on page 97). Using this procedure will help to eliminate the need for duplicate sources which can cause memory issues.

Add Source IDs for SDV Services in an RNCS Environment

This section provides the procedures to add new sources or use existing sources for SDV in an RNCS environment. Depending on the SDV server software you are running, go to ***Creating a New Source ID and Source Definition for a Remote Site*** (on page 89) or ***Creating a Source Definition for an Existing Source ID*** (on page 97).

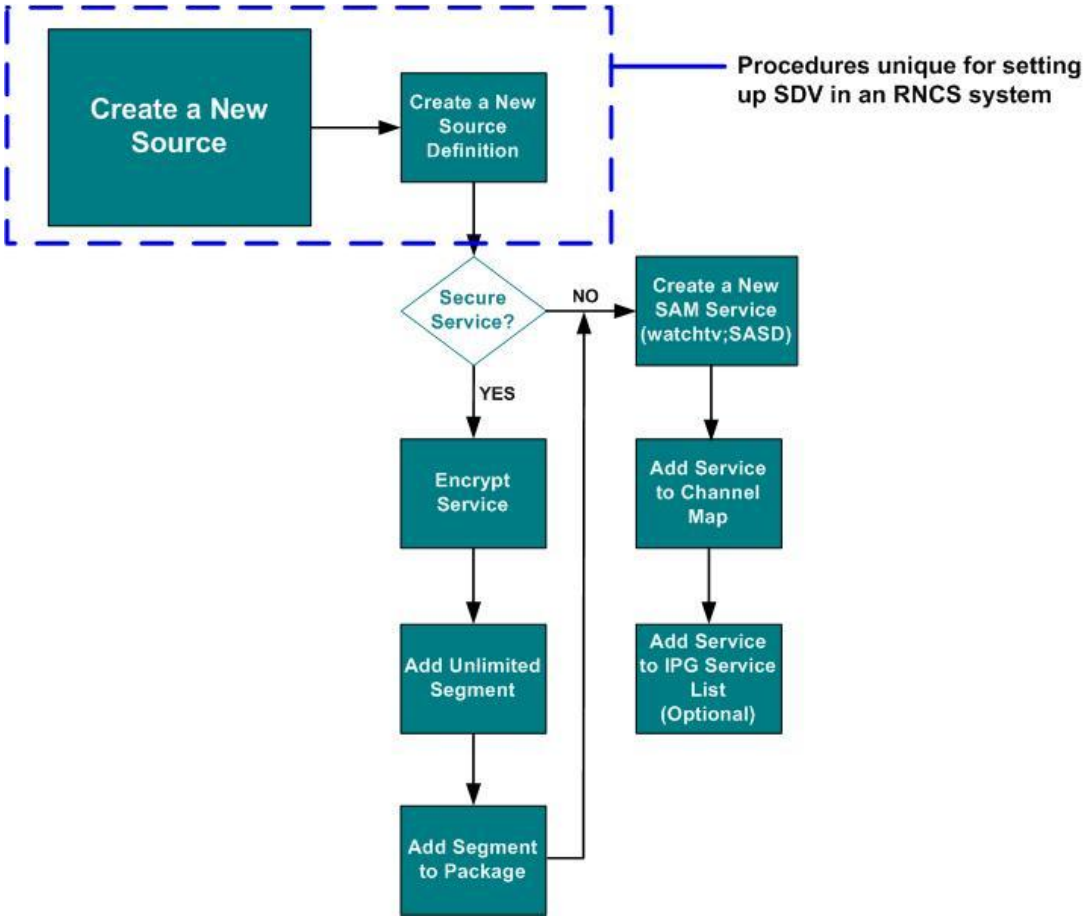
Creating a New Source ID and Source Definition for a Remote Site

Important: These procedures are written for systems that are running an SDV Server software version *prior* to version 1.4.2.

Adding a New Source ID

Refer to the following diagram for an overview of the procedures that must be completed to add a new SDV multicast source and source ID to your system.

Important: The procedures in the following diagram that are enclosed in the dashed box are unique for provisioning SDV at remote sites and, therefore, include steps that differ from provisioning procedures for the main DNCS site.

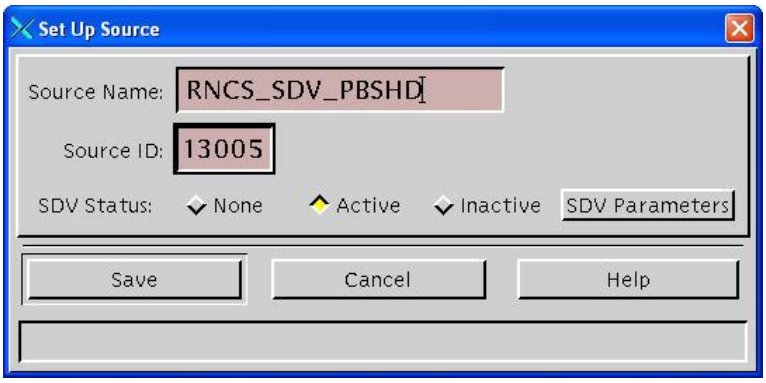


Complete the following steps to set up a new SDV multicast source for SDV services at a remote site.

1 Click the **DNCS** tab and then click the **System Provisioning** tab.

2 Click **Source.** The Source List window opens.

3 Click **File** and select **New**. The Set Up Source window opens.



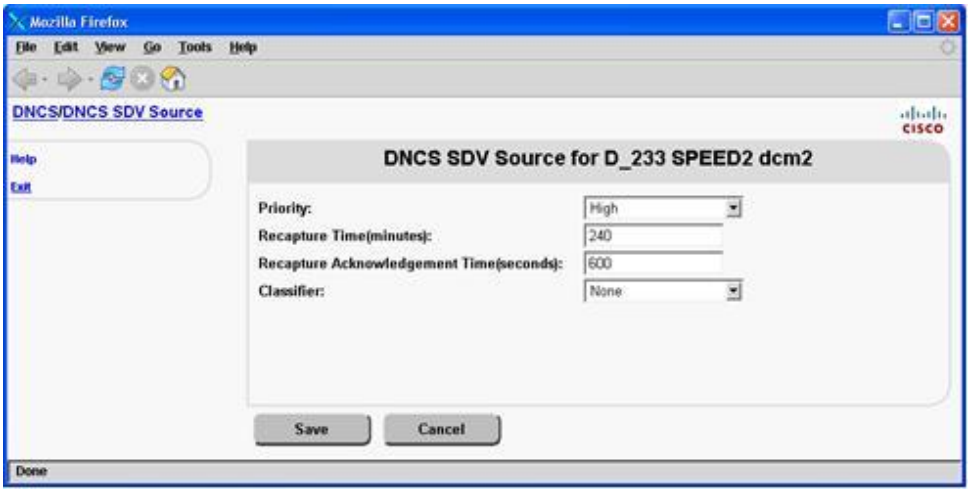
4 Enter a name in the **Source Name** field and an ID value in the **Source ID** field.

Important: Spaces are not permitted in the Source Name field.

5 From the SDV Status field, click **Active** to define the source to use SDV services.

Note: Selecting **Inactive** will set up the source for SDV services, but it will remain inactive until it is changed to Active. Selecting **None** will not set up the source for SDV services.

6 Click **SDV Parameters** to set up parameters for the SDV source. The DNCS SDV Source window opens.



7 Maintain the default values or change them to different values that are specific to your system.

8 Did you make changes to the DNCS SDV Source window?

- If **yes**, click **Save** and then click **Exit**.
- If **no**, click **Exit**.

9 From the Set Up Source window, click **Save**. The new source is listed in the Source List window

10 Do you need to create another new source ID?

- If **yes**, repeat steps 1–9.
- If **no**, go to ***Creating a Source Definition*** (on page 92).

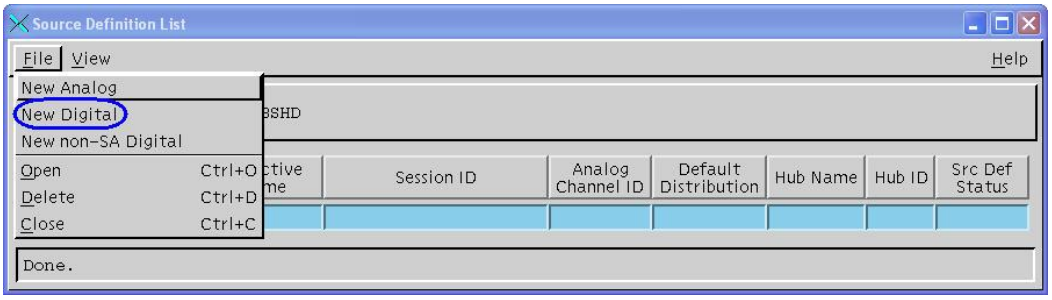
Creating a Source Definition

CAUTION:

You must create new Source IDs for each SDV service. Creating an SDV Source Definition from an existing Source ID, such as a broadcast service, causes the system to bind an SDV session even when tuning to the broadcast session. This may cause the system to run out of SDV bandwidth quickly.

Sessions define and allocate the resources that the network uses to deliver sources. Complete the following steps to define a new source definition (session) for the SDV source you just created.

1 From the Source List window, select the new SDV source, click **File**, and then select **Source Definitions**. The Source Definitions window opens.

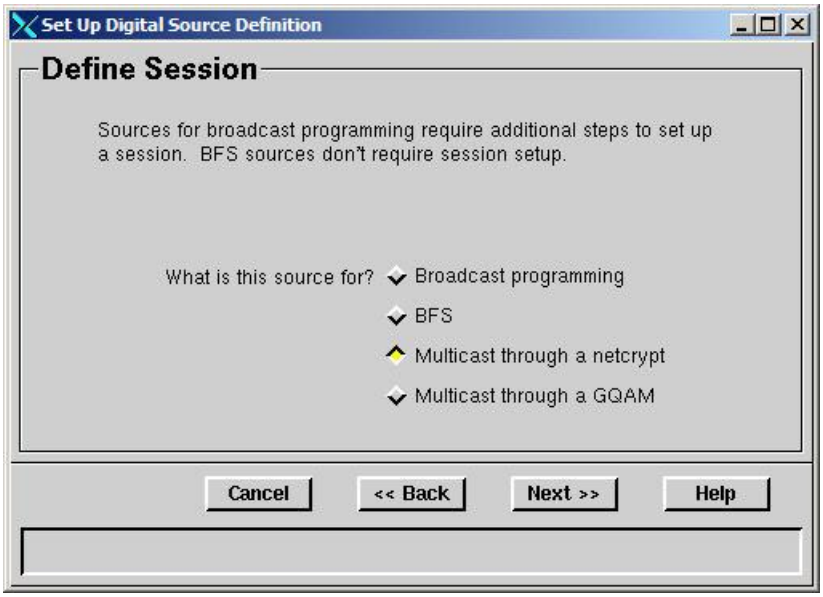


2 From the File menu, select **New Digital**. The Set Up Digital Source Definition window opens.

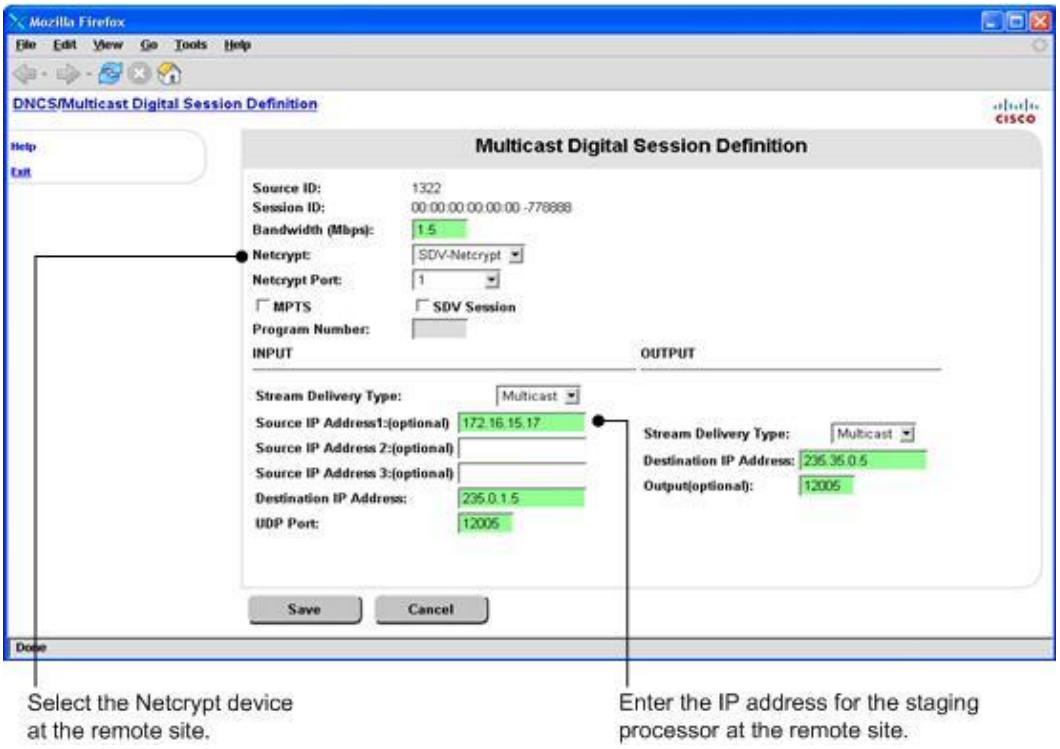
3 For the **Session ID** field, type the following: **00:00:00:00:00:00 nnnnn**, where "nnnnn" is the source ID that you entered when you added the source to the Source List.

Example: For source ID 13005, enter 00:00:00:00:00:00 13005.

4 Click **Next**. The Define Session window opens.



5 Click **Multicast through a netcrypt** and then click **Next**. The Multicast Digital Session Definition window opens.



6 Enter the appropriate values in the following fields:

- **Bandwidth (Mbps)**: Enter the bandwidth rate for the SDV service.
- **Netcrypt**: Select the Netcrypt device at the *remote location* that will be multicasting the content for this service group.
- **Netcrypt Port**: Select the Netcrypt GbE port that will be multicasting the content (the same port that is receiving the content from the staging processor or other source).
- **MPTS**: Leave this option disabled. Enabling MPTS indicates that the incoming stream to the Netcrypt is a Multiprogram Transport Stream (MPTS).

  Important: In an SDV environment, SPTS (Single Program Transport Stream) should be the standard; therefore, MPTS should never be enabled.
- **SDV Session:** Check the SDV Session check box to enable the SDV session.
- **Program Number** (is active only when MPTS is selected): You do not need to enter a program number in an SDV environment. Go to step 7.

7 Select or enter the following values for the stream delivery type you selected in step 6:

INPUT

- **Stream Delivery Type:** Select Multicast.
- **Source IP Address 1: (optional)**: The IP address of the staging processor (for example, DCM, Mentor, BMR, or Terayon device) interface that is sourcing the video *at the remote site*.
- **Source IP Address 2 (optional)**: The IP address of an additional staging processor interface that is sourcing the video *at the remote site*. An additional staging processor provides redundancy, if needed.
- **Source IP Address 3 (optional)**: The IP address of an additional staging processor interface that is sourcing the video *at the remote site*. An additional staging processor provides redundancy, if needed.
- **Destination IP Address**: The destination IP address of the multicast stream incoming to the Netcrypt device.
- **UDP Port**: The destination UDP port number for the incoming content.

OUTPUT

- **Stream Delivery Type:** Select Multicast.
- **Destination IP Address**: The multicast IP address for the destination output source that the Netcrypt device is sending video to.
- **Output (optional)**: The destination UDP port that the Netcrypt device will use when sending the content to the network.

8 Click **Save**.

9 Do you need to create an additional source definition for this service ID?

- If **yes**, repeat steps 1–8.
- If **no**, you have completed this procedure and should refer to the flow chart in ***Adding a New Source ID*** (on page 89) to complete the remaining provisioning procedures.

Creating a Source Definition for an Existing Source ID

This section describes how to create additional source definitions for an existing source ID when the source definitions are specific to ad zone programming.

Important:

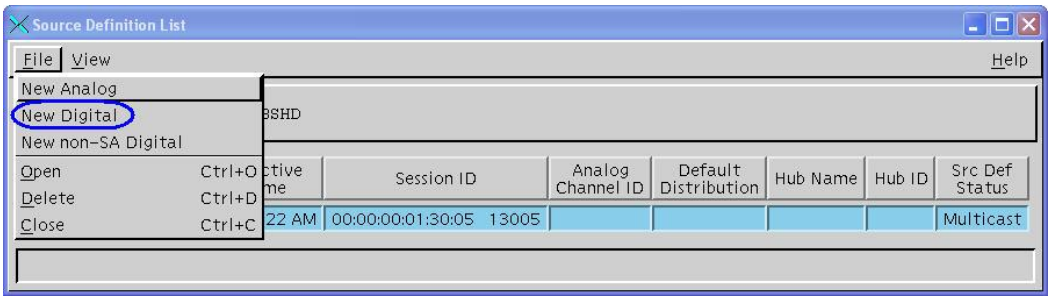
- To set up ad zones, refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584).
- To successfully provision new services for an existing source for SDV at a remote site (i.e., using the ad zone provisioning feature on the SDV Server), you *must* be running SDV Server software version 1.4.2 or later.

Note: For setting up new source definitions for source redundancy, refer to ***Creating a Redundant Source Definition For an Existing Source*** (on page 54).

Creating a Source Definition for an Existing SDV Source

Complete the following steps to define a new source definition (session) for an existing SDV source. Sessions define and allocate the resources that the network uses to deliver sources.

1 From the Source List window, select the existing SDV source, click **File**, and then select **Source Definitions**. The Source Definitions window opens.

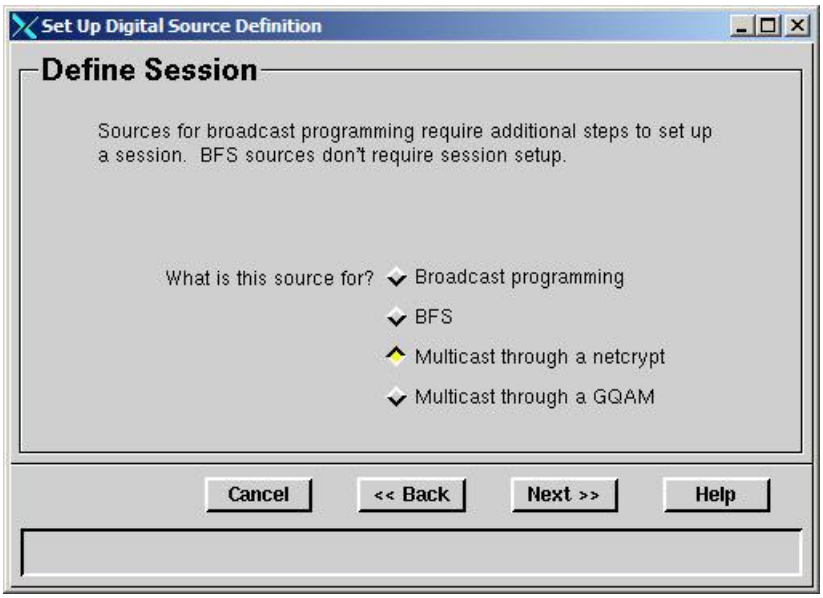


2 From the File menu, select **New Digital**. The Set Up Digital Source Definition window opens.

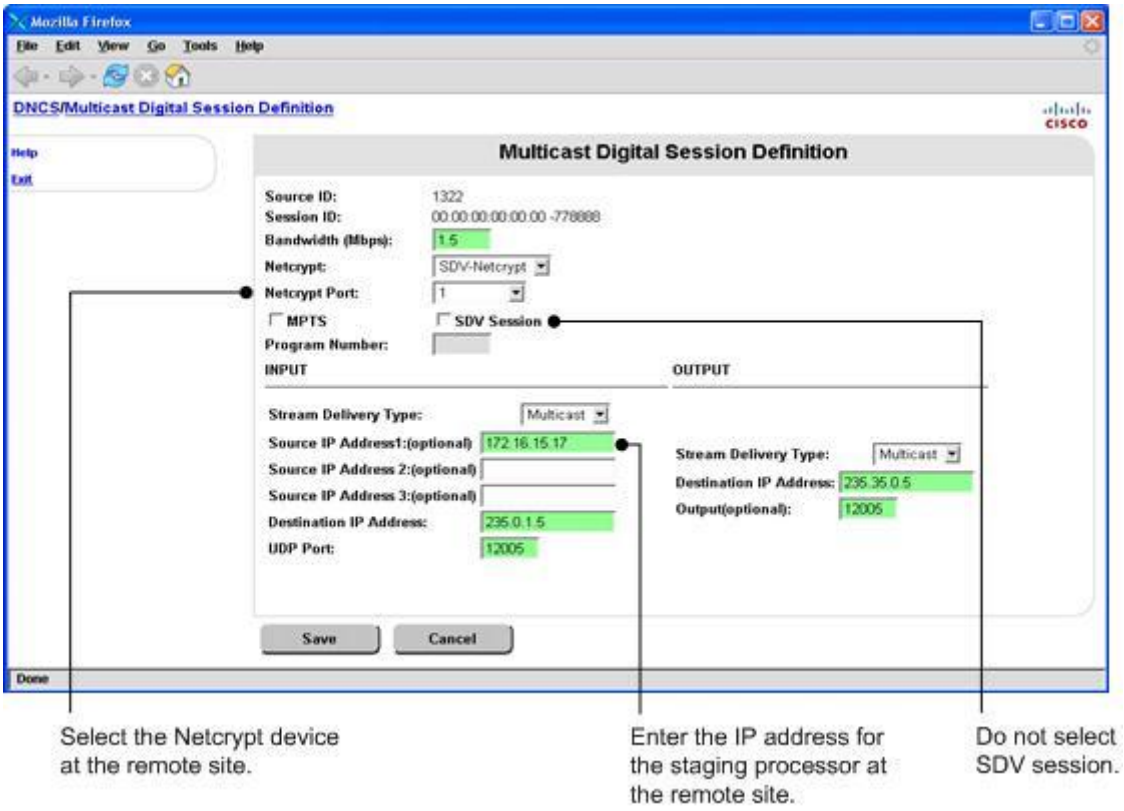
3 For the **Session ID** field, type the following: **00:00:00:00:00:00 nnnnn**, where "nnnnn" is the source ID that you entered when you added the source to the Source List.

Example: For source ID 13005, enter 00:00:00:00:00:00 13005.

4 Click **Next**. The Define Session window opens.



5 Click **Multicast through a netcrypt** and then click **Next**. The Multicast Digital Session Definition window opens.



6 Enter the appropriate values in the following fields:

- **Bandwidth (Mbps)**: Enter the bandwidth rate for the SDV service.
- **Netcrypt**: Select the Netcrypt device for the *remote location* that will be multicasting the content for this service group.
- **Netcrypt Port**: Select the Netcrypt GbE port that will be multicasting the content (the same port that is receiving the content from the staging processor or other source).
- **MPTS**: The incoming stream to the Netcrypt is Multi Program Transport Stream (MPTS).

  Important: In an SDV environment, SPTS (Single Program Transport Stream) should be the standard; therefore, MPTS should never be enabled.
- **SDV Session:** Do *not* enable this option.
- **Program Number** (is active only when MPTS is selected): You do not need to enter a program number in an SDV environment. Go to step 7.

7 Select or enter the following values for the stream delivery type you selected in step 6:

INPUT

- **Multicast:** Select Multicast.
- **Source IP Address 1 (optional)**: The IP address of the staging processor (for example, DCM, Mentor, BMR, or Terayon device) interface that is sourcing the video *at the remote site*.
- **Source IP Address 2 (optional)**: The IP address of an additional staging processor interface that is sourcing the video *at the remote site*. An additional staging processor provides redundancy, if needed.
- **Source IP Address 3 (optional)**: The IP address of an additional staging processor interface that is sourcing the video *at the remote site*. An additional staging processor provides redundancy, if needed.
- **Destination IP Address**: The destination IP address of the multicast stream incoming to the Netcrypt device.
- **UDP Port**: The destination UDP port number for the incoming content.

OUTPUT

- **Multicast:** Select Multicast.
- **Destination IP Address**: The multicast IP address for the destination output source that the Netcrypt device is sending video to.
- **Output (optional)**: The destination UDP port that the Netcrypt device will use when sending the content to the network.

8 Click **Save**.

9 Do you need to create an additional source definition for this service ID?

- If **yes**, repeat steps 1–8.
- If **no**, you have completed this procedure and should refer to the flow chart in ***Adding a New Source ID*** (on page 89) to complete the remaining provisioning procedures.

Provisioning Ad Zones on the SDV Server

Important: To provision ad zones, refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584).

You can associate individual service groups to unique ad zones for RNCS zone functionality. For each offered program in the SDV tier, ad zone versions of the program can be created. When a client requests an SDV program, the server tests to see if an ad zone version of the program exists. If it exists, the program is delivered to the requesting client.

Provisioning ad zones is done on the SDV Server Web UI by an SDV operator who has administrative privileges.

To provision ad zones, refer to *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584).

D

Configuring Sources for Secondary BFS QAMs in a Distributed BFS System

Introduction

If you are currently utilizing Distributed BFS and you are upgrading your system to support SDV, you must add a number of BFS sources to your BFS source list. These additional sources will need to be added to all of your secondary BFS QAMs.

This appendix provides procedures for sites using either a BFS BIG or a Direct ASI model.

In This Appendix

Adding BFS Sources - Sites Using a BFS BIG

Complete the following procedure if your DNCS uses a BFS BIG to distribute the BFS carousel data.

1. Confirm that the BFS sources are enabled for SDV services. Refer to ***Confirm the BFS Source for Switched Digital Services*** (on page 7) for details.
2. Open the Set Up BIG window by following the quick path:
   DNCS Administrative Console > Network Element Provisioning tab > BIG > File > Open
3. Click **PAT Configuration** to open the BIG PAT window.
4. Verify the BIG PAT Session Number and Program Number data, making sure that your Program Numbers are sequentially in order and in line with the Session Numbers.

   Note: Your DNCS sessions 2 through 22 should not change; however, DNCS sessions greater than 22 must be deleted and reentered with the correct sequential Program Number.

   Example: BIG PAT Session Number and Program Number Data (Program Numbers in Sequential Order and in line with Session Numbers)

Session Number	Program Number
2	128
4	129
6	130
8	131
10	132
12	133
14	134
16	135
18	136
20	137
22	138
24	139
26	140

Session Number	Program Number
28	141
30	142
32	143
199	144

Important: Cisco recommends that you go ahead and add all SDV sources 24 through 32 to reduce the number of times that the PAT Configuration table has to be edited.

5 After the SDV sessions are built, if the sessions are not immediately utilized, then disable the DNCS ATM source by following the quick path:

DNCS Administrative Console > Application Interface Modules tab > BFS Admin > select DNCS > File > Select > Sources tab > select source to be modified > File > Open > set source to Disable > Save

6 Once the PAT Configuration Table has been modified, update any secondary BFS QAMs by tearing down any session greater than 22 and rebuilding the session with the correct Program Number.

Adding BFS Sources - Sites Using Direct ASI

Complete the following procedure if your DNCS uses the Direct ASI option to distribute BFS data.

Note: A benefit of using the Direct ASI option is that you only need to build sessions *as you need them* on your primary and secondary BFS QAMs. There is no need to tear down any DNCS sessions greater than 22 as you would do within a BFS QAM system.

1. Confirm that the BFS sources are enabled for SDV services. Refer to ***Confirm the BFS Source for Switched Digital Services*** (on page 7) for details.
2. Manually add your BFS sources by following the quick path:

   DNCS Administrative Console > DNCS tab > Source
3. As BFS sources are built, the DNCS automatically retrieves the next available program number from the source list. As a result, there is no need to update the PAT Configuration Table by hand.

   In the following example, note that Session 22 is Program Number 138, while Session 199 is Program Number 139, and Session 24 is Program Number 140.

   When Session 24 was built, it took the next available Program Number, which was 140. With the Direct ASI model, you can have Program Numbers out of sequence in the PAT Configuration table.

   Example:

Session Number	Program Number
2	128
4	129
6	130
8	131
10	132
12	133
14	134
16	135
18	136
20	137
22	138
24	140
26	141
28	142

Session Number	Program Number
30	143
32	144
199	139

4 After adding the BFS sources, update any secondary BFS QAMs by adding the same sessions to the secondary BFS QAMs.

Example: If you added sessions 24 and 26 to the primary BFS QAM, you must add the same sessions to all secondary BFS QAMs as Continuous Feed sessions.

E

EID Conversion Table

Introduction

The Entitlement ID (EID) allows you to control whether subscribers are authorized for a service. When you create a package, the system displays the EID in hexadecimal. To use the EID as part of a SAM service to authorize a service, you must enter the EID as a decimal value. Use the conversion table in this appendix to convert the EID to a decimal value.

In This Appendix

Convert a Package EID to Decimal

Converting a Package EID from Hexadecimal to Decimal

After you determine the package EID, use the following table to convert the EID from the hexadecimal value that is given to a decimal value that is required.

Convert the hexadecimal value by locating the EID in the **HEX** (hexadecimal) column and then finding the value in the adjoining DEC (decimal) column to obtain the decimal equivalent. For example, if the package EID is **1f**, its 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

T12289

F

Basic Checklist for Network Connectivity

Introduction

This appendix includes a basic checklist to help ensure that your SDV network is properly configured and is communicating appropriately along the network interfaces.

This appendix also includes a sample configuration for a Layer 3 GigE video switch.

In This Appendix

Network Connectivity Checklist

Use the following checklist to ensure that you have properly configured your SDV network.

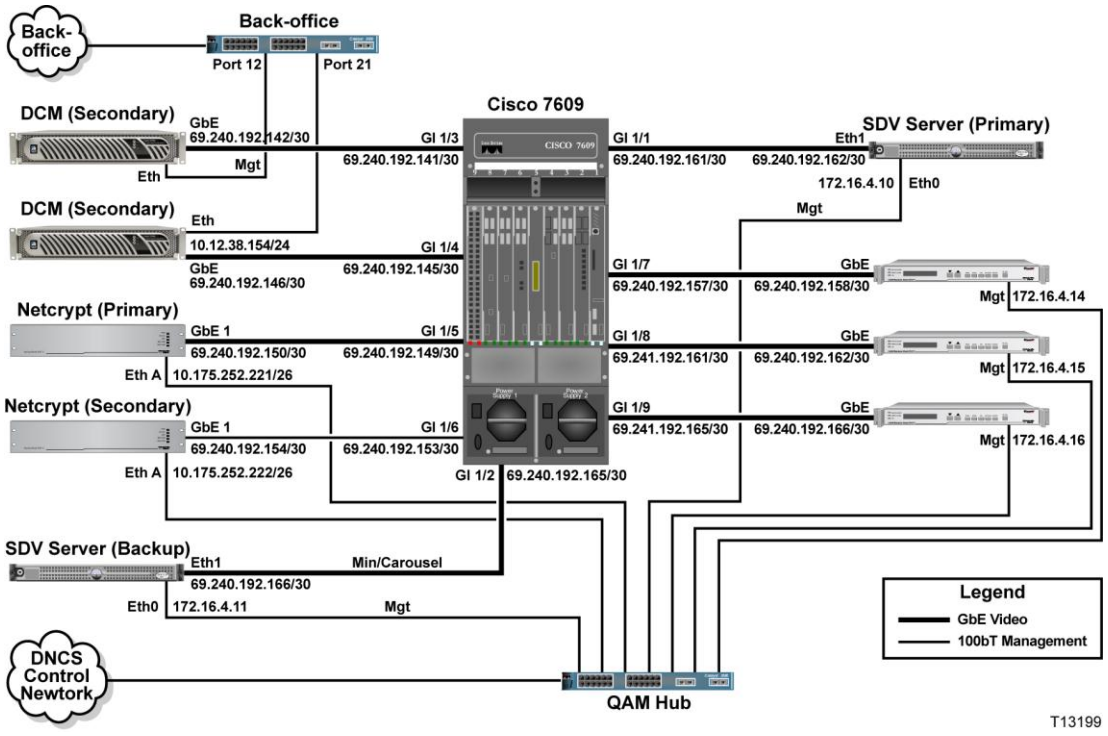
- ❒ Make sure the SDV server can ping the IP addresses for the following network elements:
  - DNCS
  - GQAM mgt port
  - DHCT network
- ❒ Make sure the video switch can ping the IP addresses for the following elements:
  - SDV server MiniCarousel interface

    Note: The location of this interface varies and is based on the configuration of the SDV server. Please confirm your configuration by examining the /opt/sdb/ConfigFiles/interaces.txt file on the SDV server.
  - Video port for staging processor (for example, DCM, Mentor, BMR, or Terayon device)
  - Video port Gateway IP address for the Netcrypt device
  - Video port for the GQAM modulator
- ❒ Make sure the DNCS can ping the following elements:
  - SDV server SNMP port interface

    Note: The location of this interface varies and is based on the configuration of the SDV server. Please confirm your configuration by examining the /opt/sdb/ConfigFiles/interfaces.txt file on the SDV server.
  - Mgt port for the Netcrypt device
  - Mgt port for the GQAM modulator
  - DHCT network

Layer 3 GigE Video Switch Sample Configuration

The following SDV network diagram and sample configuration is a basic example for configuring a Layer 3 GigE video switch.



```
CiscoSDV#sh run
Building configuration...

Current configuration: 2976 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname CiscoSDV
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$ebiF$oVlWZmbaU4bJTXKQL/HfV1
!
no aaa new-model
vtp mode transparent
ip subnet-zero
!
ip multicast-routing            ← ENABLE MULTICAST ROUTING
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/1
 description SDV Primary server
 no switchport
 ip address 69.240.192.161 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet1/2
 description SDV Backup server
 no switchport
 ip address 69.240.192.165 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet1/3
 description DCM Primary
 no switchport
 ip address 69.240.192.141 255.255.255.252
 ip pim sparse-mode
```

```
!
interface GigabitEthernet1/4
 description DCM Backup
 no switchport
 ip address 69.240.192.145 255.255.255.252
 ip pim sparse-mode
 !
interface GigabitEthernet1/5
description Netcrypt Primary
 no switchport
 ip address 69.240.192.149 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3              ← ONLY NEEDED FOR NETCRYPT
                                    CODE 1.2.3 OR LATER
!
interface GigabitEthernet1/6
description Netcrypt Backup
 no switchport
 ip address 69.240.192.153 255.255.255.252
 ip pim sparse-mode
ip igmp version 3               ← ONLY NEEDED FOR NETCRYPT
                                    CODE 1.2.3 OR LATER
!
interface GigabitEthernet1/7
 description GQAM video SFP
 no switchport
 ip address 69.240.192.157 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet1/8
 description GQAM video SFP
 no switchport
 ip address 69.240.192.161 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet1/9
 description GQAM video SFP
 no switchport
 ip address 69.240.192.165 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
!
interface Vlan1
 no ip address
!
no ip http server
!
ip pim ssm default      ← ENABLES SOURCE-SPECIFIC MULTICAST
                            (igmp v3 will use 232/8)
```

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

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

Part Number 4012948 Rev F
June 2012 Printed in USA