Troubleshooting Switched Digital Video

for System Release 2.8/3.8/4.3

Please Read

Important

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

Notices

Trademark Acknowledgments

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

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

This guide provides troubleshooting information that will help you to verify the proper configuration and performance of the Cisco Switched Digital Video (SDV) feature. This document also includes tips about the Digital Network Control System (DNCS) and the SDV server, as well as troubleshooting assistance for common issues.

Purpose

The purpose of this document is to provide tips and helpful hints to properly set up SDV services, as well as to provide solutions and troubleshooting techniques that could occur on channels configured for SDV.

Scope

The contents of this document apply to Digital Broadband Delivery Systems (DBDS) that include the Cisco SDV feature and System Release (SR) 2.8/3.8/4.3.

Audience

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

Document Version

This is the first release of this document.

1

General Tips

Introduction

This chapter includes troubleshooting tips common to the DNCS and the SDV server. These troubleshooting suggestions are not comprehensive procedures; however, they can serve as a starting point for more in-depth troubleshooting processes.

In This Chapter

Accessing the SDV Server

To access the SDV server, use one of the following options:

- **Command Line Interface (CLI)**
  - SSH login (supported)
  - Enter username/password (root/generic), when prompted
- **Web Interface** (http://IP, where IP is the address of the SDV server)
  - To login as an administrator, type the following: username/password
    Example: admin/admin
  - To login as a non-administrative user, type the following: username/password
    Example: (user/user)

Starting the SDV Server Application

The SDV server application should be started in the "supervised" mode regardless of whether it is a primary or backup server. To access the SDV application, complete the following steps.

Note: The sdvManager on the DNCS manages the primary and backup SDV servers accordingly.

1. From the DNCS, open an xterm window.
2. Access the SDV server and enter the following SSH command: **ssh root@xxx.xxx.xxx.xxx**, where xxx.xxx.xxx.xxx is the IP address for the SDV server

   Example: ssh root@192.168.40.141
3. When prompted, enter your password.

   Important: The password is **generic**.
4. Type **# cd /opt/sdb** and press **Enter**.
5. Type **./sdb -d --supervised** and press **Enter**. The SDV Server boots up.

   Notes:

   - The "-d" in the command line indicates that the SDV server is started in daemon mode.
   - The backup SDV server is also started as if it is a primary server.

The Watchdog Application

The SDV Server uses a watchdog application to assure up time and to manage SDV server upgrades. When the SDV server software is installed on the DNCS, the watchdog application starts automatically upon boot.

Important: The watchdog application is used in the event of a server reboot; therefore, this process should be running at all times.

If a reboot occurs, the SDV server is restarted with the last known command line option. Command line options include:

- **/etc/init.d/tnoswdog start** — starts the watchdog
- **/etc/init.d/tnoswdog stop** — stops the watchdog
- **/etc/init.d/tnoswdog restart** — restarts the watchdog
- **/etc/init.d/tnoswdog status** — displays the status of the watchdog
- **#cd /opt/sdb/ConfigFiles**
  - **[root@SDV-backup ConfigFiles]#** — more tnoswdog.conf
  - **IMAGE:sdb-1.2.0-1.i386.rpm** — installed image
  - **LASTIMAGE:**
  - **LASTINSTALLED:sdb-1.2.0-1.i386.rpm**
  - **ONETIME:sdb-1.1.10-1.i386.rpm**
  - **MODE:OFF**
  - **COMMANDLINE:sdb -d -supervised** — last known command line option
  - **WDPERIOD:20000**

Determining How the SDV Server Application Started

To determine how the SDV server application started for the primary or backup SDV server, use the following command: **ps -ef |grep -i sdb**, respectively.

Results:

- If the SDV server was started from the Watchdog application, the following data will appear:
  - root 1984 1 0 13:42 ? 00:00:00 /opt/sdb/**tnoswdog**
    root 2558 2525 0 15:07 pts/0 00:00:00 grep -i sdb

    Note: These two processes should be running at all times.
- If the SDV server was started from the Command Line Interface, the following data will appear:
  - root 3263 1 0 12:25 ? 00:00:00 ./sdb -d **-supervised**
    root 3491 3370 0 15:25 pts/0 00:00:00 grep -i sdb

    Note: These two processes should be running at all times.

Verifying the Installed Version of SDV Software

There are two methods in which to determine what version of SDV software is currently installed on the server. These methods include:

- Using the following commands on the Command Line Interface:
  - **#cd /opt/sdb/ConfigFiles**
  - **./sdb -v** (provides the version number to three decimal places [for example, 1.4.2])
  - **./sdb -x** (provides the build number [for example, 1.4.2-13])
- Using the Web interface to access the SDV server
  - From the Main Menu, click **Software** and select **Software Revision**

SDV Server Disk Clean Up Activity

Deleting EventLog Files

Complete the following steps to delete any unnecessary EventLog files on the SDV server.

1. On the SDV server, log in as **root** user.
2. Type **df -k** and press **Enter** to determine the percentage of disk usage by partition.
3. Type **cd /opt/sdb/EventLog/** and press **Enter** to make the opt/sdb/EventLog directory the working directory.
4. Type **rm <file name>** and press **Enter** to delete any unnecessary text files from the opt/sdb/EventLog directory.

   Important: If you need to remove any files, we recommend that you delete the oldest files first.

   Note: The event log file name is in the format ddmmmyyyy.txt.

   Example: rm 31Jan2008.txt
5. Type **df -k** and press **Enter** to check the disk usage by partition again. Because you deleted unnecessary Log files in this procedure, the percentage of disk usage should now be reduced.
6. Type **exit** and press **Enter** to log out as root user.
7. Type **exit** and press **Enter** to close the xterm window.

Notes:

- Check the EventLog directory on the SDV server. Consider reducing the number of days you have configured on the DNCS to delete SDV event logs from your system.
- Using the **Log All** setting causes the Event Log to fill faster.

Deleting ActivityLog Files

Complete the following steps to delete any unnecessary ActivityLog files on the SDV server.

1. On the SDV server, log in as **root** user.
2. Type **df -k** and press **Enter** to determine the percentage of disk usage by partition.
3. Type **cd /opt/sdb/ActivityLog/** and press **Enter** to make the opt/sdb/ActivityLog directory the working directory.
4. Type **rm <file name>** and press **Enter** to delete any unnecessary text files from the opt/sdb/EventLog directory.

   Important: If you need to remove any files, we recommend that you delete the oldest files first.

   Note: The event log file name is in the format ddmmmyyyy.txt.

   Example: rm 30Jun2006.txt
5. Type **df -k** and press **Enter** to check the disk usage by partition again. Because you deleted unnecessary Log files in this procedure, the percentage of disk usage should now be reduced.
6. Type **exit** and press **Enter** to log out as root user.
7. Type **exit** and press **Enter** to close the xterm window.

Note: Check the ActivityLog directory on the SDV server. Consider reducing the number of days you have configured on the DNCS to delete SDV event logs from your system.

Monitoring DNCS Logs

Introduction

Use the DNCS system logs to identify and monitor SDV system issues. We suggest that you review the DNCS log files each morning to determine if any new issues have occurred since the previous day.

The following DNCS logs are pertinent to monitoring the SDV system:

- sdvManager
- qamManager
- pkeManager
- drm
- dsm

Configuring DNCS System Logging Levels

Use the Logging utility to fine-tune log levels for DNCS processes and their associated libraries.

The Logging utility is most useful when you are experiencing problems and want to capture information that can help you resolve the problem. After you adjust the logging level for a specific site and process, you can open the DNCS log and view the data that the DNCS has recorded. You can also open the log for an individual process.

Note: For more information on how to configure and use the Logging utility, refer to the DNCS Online Help file for the system release you are using or refer to *Provisioning the DNCS to Support SDV Services User Guide* (part number 4012948).

Accessing DNCS Log Files

After you configure your logging levels, make sure you know how to access the DNCS log file and the log files for individual processes. You can open the DNCS log in **/var/log/dncsLog** and view the data that the DNCS has recorded.

You can find the most recent log files for an individual process in **/dvs/dncs/tmp/[name of process.*]**. The file name of the log for an individual process is the name of the process followed by a 3-digit counter. For example, the file name for the qamManager log might be qamManager.000.

Notes:

- All processing logging levels can be viewed in **/dvs/dncs/tmp**.
- Only the Emergency, Alert, and Critical logging levels can be viewed in **/var/log/dncsLog**.
- Error logging levels can be viewed in **/dvs/dncs/tmp/processName**.

For more information on how to use log files to maintain a healthy system, see *Maintenance Recommendations for the DBDS* (part number 4002341).

Performance Monitoring

Use the Performance Monitoring tool to display data collected from DNCS processes in a graphical format, such as a line chart. DHCT and VOD performance data is gathered from DNCS processes in comma separated value (CSV) files and is displayed in a graphical format to help you in maintaining and troubleshooting your system should the need arise.

Data can be collected and displayed for the drm, dsm, and qamManager processes.

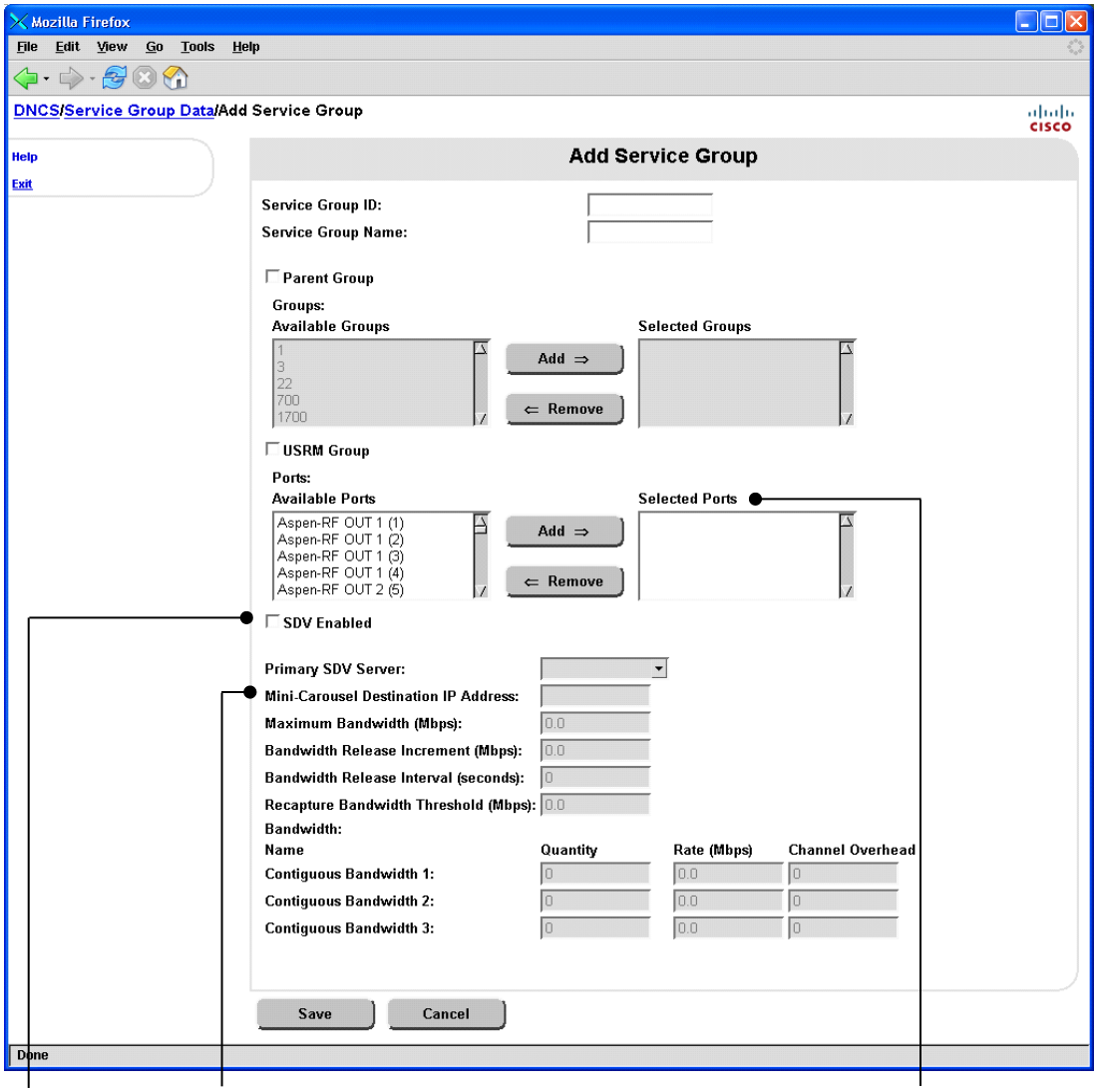
For more information about using the Performance Monitoring tool, see the DNCS Online Help for the system release you are using.

Enabling Service Groups for SDV

To enable a service group for SDV, you must access the Service Group GUI on the DNCS and manually select **SDV Enabled**. You must also define valid GQAM radio frequency (RF) ports and SDV server information.

Note: Refer to *Provisioning the DNCS to Support SDV Services User Guide* (part number 4012948) for details about adding and enabling a service group.

Example:



Monitoring the Number of Available Service Groups

Important: This section pertains to sites that are running SR 4.2.1 or later.

You must actively monitor the number of SDV-enabled service groups on your system. Complete the following steps to monitor the number of SDV-enabled service groups on your system.

Note: For additional details on configuring your system for SDV, refer to *Provisioning the DNCS to Support SDV Services User Guide* (part number 4012948).

1. In the DNCS Monitor window on the DNCS Administrative Console, observe the status of the sgManager process. The light adjacent to this process should be green.
2. If the sgManager was unsuccessful in adding the MCDiscovery file to a BFS carousel, the sgManager process light will turn yellow.
3. To verify that the number of SDV-enabled services groups on your system has exceeded 475, open the sgManager log file and locate an entry that indicates that the carousel is full.
4. Go to ***Expanding the Number of Available Service Groups*** (on page 13).

Expanding the Number of Available Service Groups

Important: This section pertains to sites that are running SR 4.2 SP2 or later.

To expand the number of available service groups, you must manually build the additional BFS carousels. Complete the following procedure for each available service group in the exact order shown.

Important: Complete this procedure for one BFS source (for example, BFS source 26) before enabling the next available BFS source (for example, BFS source 28).

1. To enable an additional set of 475 service groups in your system, enable the next available BFS source (26, 28, 30, or 32) from the DNCS BFS Admin GUI sequentially and in the exact order shown here. Then, go to step 2. For example:
   - To expand the number of available service groups to between 476 and 950 enable BFS source 26 (SGM IB1).
   - To expand the number of available service groups to between 951 and 1,425, enable BFS source 28 (SGM IB2).
   - To expand the number of available service groups to between 1,426 and 1,900, enable BFS source 30 (SGM IB3).
   - To expand the number of available service groups to between 1,901 and 2,375 enable BFS source 32 (SGM IB4).

   Important: See the *Digital Network Control System Online Help* on your system for additional details on configuring and enabling BFS sources.
2. Stop the sgManager process.
3. Using a text editor, edit the /dvs/dncs/etc/sgManager.conf file, and add a new sequential 4-digit source ID to the existing list (for example "0026"), and then save the file.
4. Restart the sgManager process.
5. Do you want to enable an additional BFS source?
   - If **yes**, repeat this procedure from step 1.
   - If **no,** you have completed this procedure

   Important: To expand the number of available service groups beyond 2,375, contact Cisco Services for further assistance.

Controlling Service Group PassThru Messages

Enabling Service Group PassThru Messages

In 2.7/3.7/4.2 SP2, all Service Group PassThru messages are disabled. To enable the PassThru (0x8065) message on your system, you must edit the .profile file to add the environment variable **SEND_SG_PASSTHRU=true** and then stop and restart the sgManager process.

Note: 0x8065 PassThru messages are sent only when service group hierarchical changes are made. For example, when parent-child relationships are changed, both the parent and child service groups are included in the 0x8065 PassThru message. Therefore, only enable this variable if a hierarchical service group architecture exists on the system.

Disabling Service Group PassThru Messages

To disable the PassThru message, comment out the **SEND_SG_PASSTHRU=true** entry in the .profile file by adding a **#** at the beginning of the line and then restart the sgManager process.

Managing Bandwidth and Service Groups

Overview

Because the SDV technology is designed to recover bandwidth from infrequently-viewed channels, fine-tuning of access network bandwidth is an important management aspect of your SDV system.

Careful management of service groups is another important consideration for your SDV system. For example, you should split service groups in the event that the DHCT threshold capacity of the SDV service group is exceeded. Increases in channel demand also could warrant the need for splitting service groups.

This section provides information for properly managing your SDV bandwidth and service groups.

Fine Tuning SDV Bandwidth

This section provides procedures you can follow to monitor and fine tune your bandwidth.

Check SDV Server Specifications

Refer to the *Series D9500 Switched Digital Video Servers Installation and Operation Guide* (part number 4012584) to verify that your system conforms to maximum specification limits listed for the following:

- QAM modulators
- DHCTs
- Service Groups

  Note: See ***Expanding the Number of Available Service Groups*** (on page 13) for procedures to expand the number of service groups available on your system.

Monitor Alarms

Use your Network Management System (NMS) to monitor your system for the following session and server capacity alarms:

- Alarm 101
- Alarm 204
- Alarm 205
- Alarms 207 through 209
- Alarm 400

If these alarms are occurring frequently and consistently, follow the recommended check and correct procedures for these alarms. See ***Monitoring SDV Alarms*** (on page 27). You can also do one or more of the following:

- Add bandwidth to the SDV service group
- Split your SDV service groups to decrease the number of DHCTs in the service group
- If the number of subscribers viewing a program is consistently greater than 1, consider making the program a broadcast program
- Add QAM carriers to the affected service group

Checking SDV Service Groups

The sgmParse.pl Utility

The sgmParse.pl utility can be used to read the service group map file. Service group map files contain all of the frequencies, transport stream identifiers (TSIDs), and modulation types that are assigned to a service group on gigabit quadrature amplitude modulation (GQAM) and multiple QAM (MQAM) modulators.

Complete the following steps to run the sgmParse.pl utility.

1. If necessary, open an xterm window on the DNCS.
2. Type **cd /dvs/dvsFiles/SGM** and then press **Enter**.

   Important: Make sure you type a space before typing /dvs.
3. Type **ls** and then press **Enter** to list the service group map files.

   Example: The following sample output shows the list of SGM files:
   core sdb sdv servicegroupmap.dat
4. Type **sgmParse.pl <service group map file name>** and then press **Enter**.

Example: The following sample output shows the contents of the service group map file.

TSID	SGID	TRANS	INNER	SPLIT	MODUL	SYMBOLRATE	FREQUENCY
8001	1	2	0	0	16	5360537	729000000
50004	2	2	0	0	16	5360537	735000000
3001	1	2	0	0	16	5360537	741000000
3002	1	2	0	0	16	5360537	747000000
3003	1	2	0	0	16	5360537	753000000
3004	1	2	0	0	16	5360537	759000000
3005	1	2	0	0	16	5360537	765000000
3006	1	2	0	0	16	5360537	771000000
3007	1	2	0	0	16	5360537	777000000
3008	1	2	0	0	16	5360537	783000000

The mcParse.pl Utility

The mcParse.pl utility can be used to read the service group files for the mini carousel protocol (MCP) TSID, as well as the frequencies for service groups. When this utility is executed, only the SDV enabled ports are displayed.

Complete the following steps to run the mcParse.pl utility.

1. If necessary, open an xterm window on the DNCS.
2. From the dvs/dvsFiles/SGM directory, type **cd sdv** and then press **Enter**.
3. Type **ls** and then press **Enter** to list the service group files.

   Example: The following sample output shows the list of service group files:

   00000002 00000005 00000009 0000000c 0000000f 00000012 00000015 00000018 00000066 00000069 0000006c 00000003 00000006 0000000a 0000000d 00000010 00000013 00000016 00000032 00000067 0000006a 00000004 00000007 0000000b 0000000e 00000011 00000014 00000017 00000065 00000068 0000006b
4. Type **mcParse.pl <service group file number>** and press **Enter**.

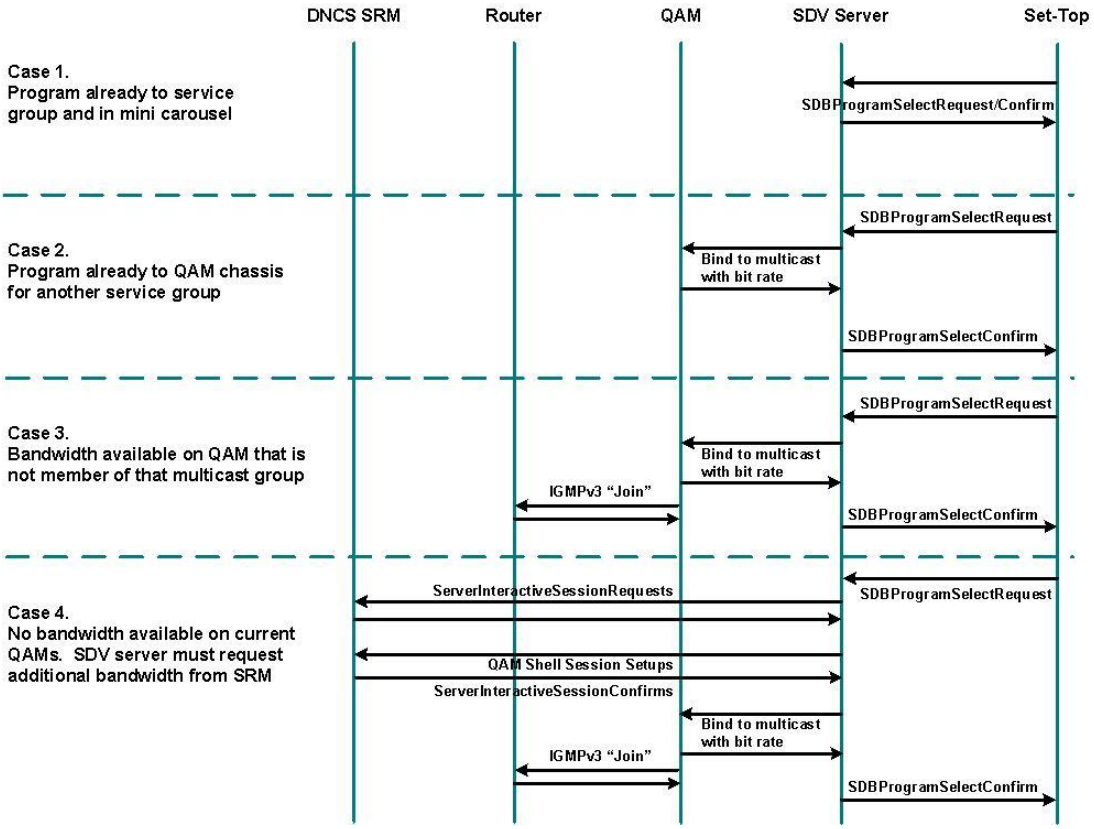
Example: The following sample output shows the mini-carousel TSID and frequencies for Service Group 1.

```
[563]$ .mcParse.pl* /dvs/dvsFiles/SGM/sdv/00000001
Time Stamp              Wed Jul  5 13:26:18 2006  (1152120375)
Service Group           1
Parent Service Group    0
Unique RF outputs       8

TSID        SYMBOLRATE    FREQUENCY     MODUL
 3001          5360537     741000000       16
 3002          5360537     747000000       16
 3003          5360537     753000000       16
 3004          5360537     759000000       16
 3005          5360537     765000000       16
 3006          5360537     771000000       16
 3007          5360537     777000000       16
 3008          5360537     783000000       16
[564]$
```

Interaction of SDV Components

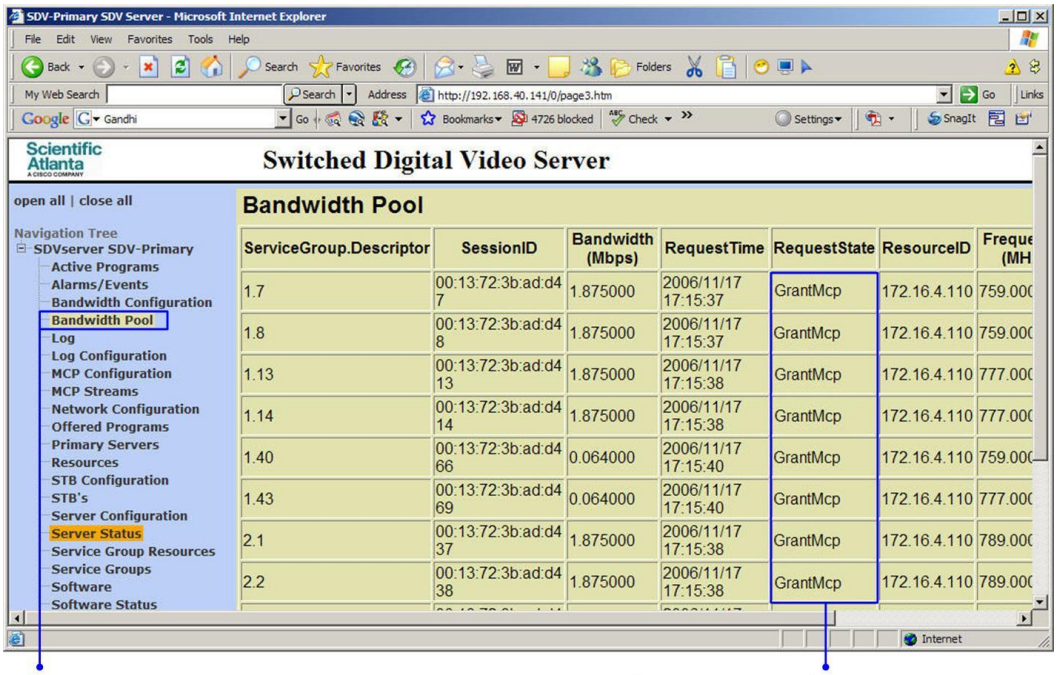
This sequence diagram depicts the interaction between SDV components and the session resource manager (SRM).



Verifying the Mini Carousel Session on the SDV Server GUI

1. Access the SDV server GUI. The Switched Digital Video Server window opens.
2. Click **Bandwidth Pool** from the left frame of the window. The Bandwidth Pool area opens.
3. Verify that GrantMcp is defined in the RequestState field for each RF carrier (TSID).

   Example:



Verifying Offered Programs on the SDV Server

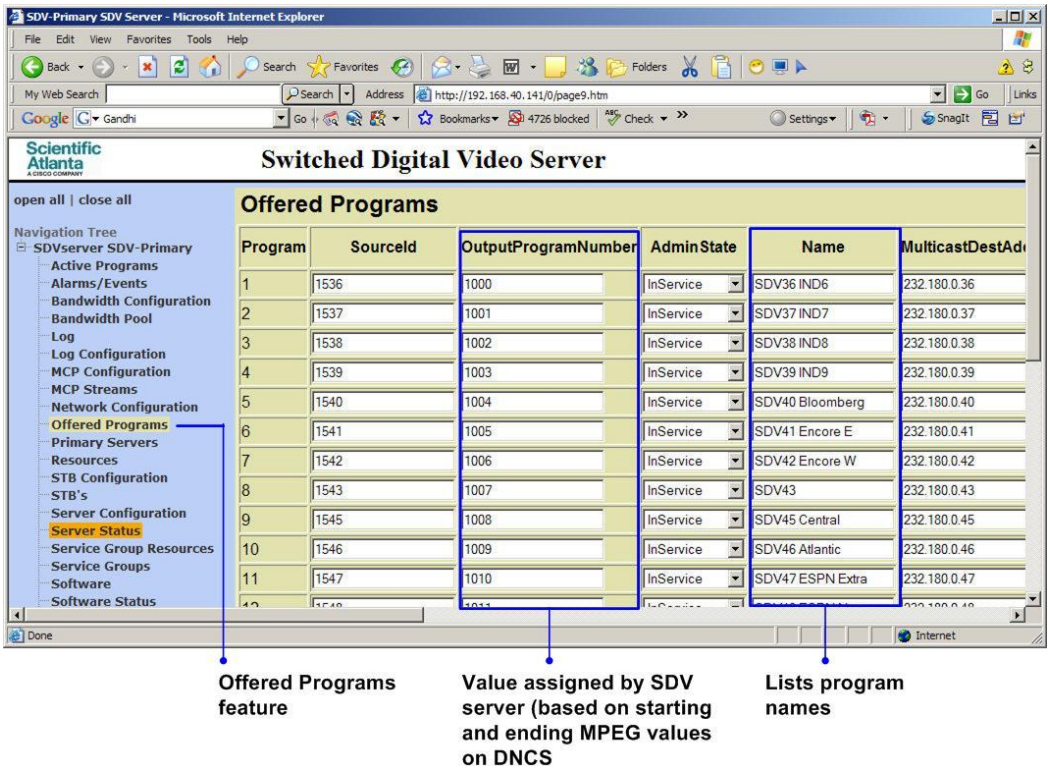
The SDV server GUI includes an Offered Programs feature that allows you to view those programs that are configured for SDV services. Programs that are included in this list are assigned with the watchtv;SASD URL. To verify these programs, complete the following steps:

Note: The watchtv;SASD URL is assigned to programs in the SAM Configuration GUI on the DNCS.

1 Access the SDV server GUI. The Switched Digital Video Server window opens.

2 Click **Offered Programs** from the left frame of the window. The Offered Programs area opens.

Example:



Verifying Active Programs on the SDV Server

The Active Programs feature on the SDV server GUI lists the programs that are currently bound to GQAMs. This feature also lists the total number of users that are actively viewing the program.

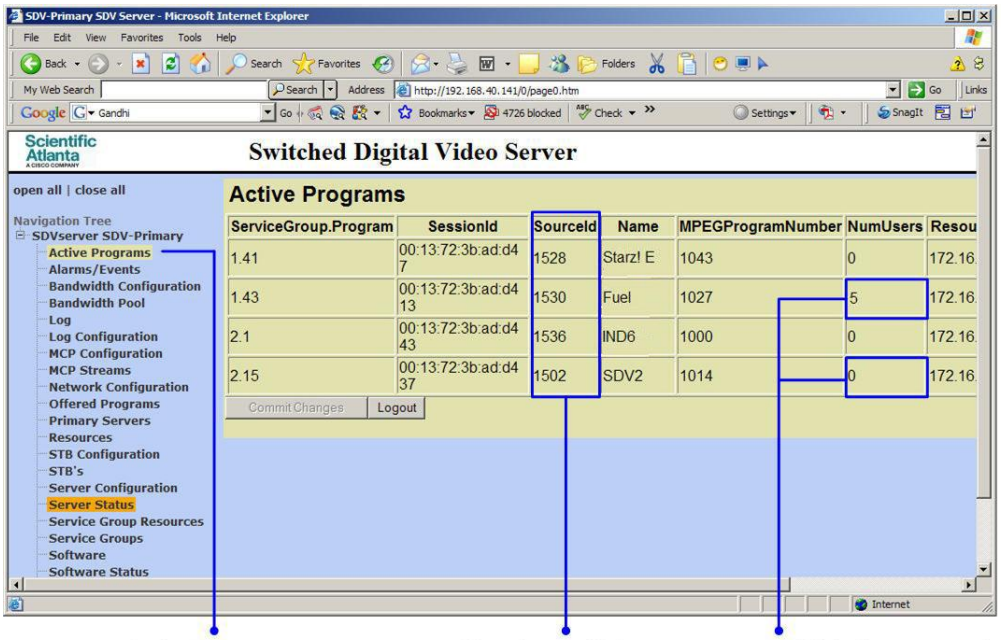
Note:

- The active programs listed in the Active Programs WUI are the same as the list of programs in the mini carousel.
- Programs that are bound to a GQAM, but do not have any active users, are listed as well. The value in these cases is zero.

To view the active program, complete the following steps:

1. Access the SDV server GUI. The Switched Digital Video Server window opens.
2. Click **Active Programs** from the left frame of the window. The Active Programs area opens.

Example:



Network Commands

See the following list to view the most common network commands, along with example output.

Note: The example output for each network command originates at the network switch.

- **show interfaces summary**—displays a summary of statistics for one interface or for all interfaces that are configured on a networking device

  Example:

 # show interfaces summary

*: interface is up
IHQ: pkts in input hold queue — IQD: pkts dropped from input queue
OHQ: pkts in output hold queue — OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec) — RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec) — TXPS: tx rate (pkts/sec)
TRTL: throttle count

Interface	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
Vlan1	0	0	0	0	0	0	0	0	0
* GigabitEthernet1/1	0	0	0	0	1000	1	1000	2	0
* GigabitEthernet1/2	0	0	0	0	67000	15	0	0	0
* GigabitEthernet1/3	0	0	0	0	0	0	0	0	0
* GigabitEthernet1/4	0	0	0	0	216226000	19817	0	0	0
* GigabitEthernet1/5	0	0	0	0	0	0	0	0	0
* GigabitEthernet1/6	0	0	0	0	0	0	53705000	4924	0
* GigabitEthernet1/7	0	0	0	0	158836000	14568	215648000	19785	0
* GigabitEthernet1/8	0	0	0	0	0	0	0	0	0

- **show ip igmp interface** — displays multicast-related information about an interface

  Example:

```
# show ip igmp interface gigabitEthernet 1/6

GigabitEthernet1/6 is up, line protocol is up
  Internet address is 172.16.15.10/30
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 292 joins, 287 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 172.16.15.10 (this system)
  IGMP querying router is 172.16.15.10 (this system)
  No multicast groups joined by this system
```

- **show ip igmp groups** — displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).

  Example:

```
# sh ip igmp groups

IGMP Connected Group Membership
Group Address   Interface          Uptime    Expires   Last Reporter
232.101.1.1     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.1     GigabitEthernet2/6 1w4d      stopped   172.16.15.53
232.3.1.1       GigabitEthernet2/4 1w5d      stopped   172.16.15.49
232.101.1.2     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.3     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.4     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.5     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.6     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.8     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.101.1.9     GigabitEthernet2/4 1w4d      stopped   172.16.15.49
232.1.1.23      GigabitEthernet2/6 02:56:18  stopped   172.16.15.53
239.1.1.25      GigabitEthernet1/7 00:01:27  00:02:01  172.16.15.21
```

- **show ip mroute <group>**—displays the contents of the IP multicast routing table

  Example:

```
# sh ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

 (172.16.42.1, 232.0.0.1), 6d21h/00:02:57, flags: sTI
  Incoming interface: GigabitEthernet1/2, RPF nbr 0.0.0.0
  Outgoing interface list: (should NOT be NULL)
    GigabitEthernet1/6, Forward/Sparse, 6d21h/00:02:51, H
```

- **show ip mroute active**—displays the rate that active sources are sending to multicast groups

  Example:

```
# sh ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 232.0.0.1, (?)
   Source: 172.16.42.1 (?)
     Rate: 7 pps/18 kbps(1sec), 18 kbps(last 0 secs), 19 kbps(life avg)
```

- **show ip mroute [ip address]**—displays the rate that active sources from a specific IP address of a multicast source are sending to multicast groups

```
# show ip mroute 232.10.0.59

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B – Bidir Group, s – SSM Group, C - Connected,
       L - Local, P – Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M – MSDP created entry,
       X – Proxy Join Timer Running, A – Candidate for MSDP Advertisement,
       U – URD, I – Received Source Specific Host Report, Z – Multicast Tunnel
       Y – Joined MDT-data group, y – Sending to MDT-data group
Outgoing interface flags: H – Hardware switched, A – Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.182.110.6, 232.10.0.59), 00:16:48/00:02:54 flags sTI
  Incoming interface: TenGigabitEthernet4/1, RPF nbr 10.182.96.246, RPF-MFD
  Outgoing interface list:
    GigabitEthernet9/8, Forward/Sparse, 00:16:48/00:02:24, H
```

2

Monitoring SDV Alarms

Introduction

The SDV server is capable of sending third-party network management system (NMS) alarms, or traps. These alarms are generated to provide system operators with an indication of an abnormal hardware or software condition.

The health of the SDV server is vital to your system operations. We recommend that you monitor the SDV alarm data as a part of your daily SDV system checks.

Note: The Alarm Manager NMS can be used to check on the status of your SDV server alarms. Contact the representative that handles your account for more information.

This chapter provides detailed procedures for identifying, troubleshooting, and clearing the SDV server alarms to keep your SDV system running properly.

In This Chapter

SDV Alarms

This section provides detailed information for troubleshooting alarms that are generated by the SDV server.

Because there are several different categories of SDV server alarms, the alarms are divided into the following individual sections:

- ***SDV System Communications Alarms*** (on page 29)
- ***SDV Server Process Alarms*** (on page 32)
- ***SDV Session Alarms*** (on page 40)
- ***SDV Server Capacity Alarms*** (on page 42)
- ***SDV Maintenance and Provisioning Alarms*** (on page 54)
- ***SDV Program Management Alarms*** (on page 56)
- ***SDV Redundancy Alarms*** (on page 57)

The alarms are arranged in the ascending numerical order of the trap identifiers. For your convenience, the alarms are listed in both decimal and hexadecimal format. You can look up the possible causes and then follow the Check and Correct procedures for each alarm to help you troubleshoot and clear the alarm.

SDV System Communications Alarms

SDV Server Trap 1 (1 Hex)

Alarm Summary:

SDV Server Unable to Communicate with DNCS SRM

Description:

This alarm occurs when the resource manager of the SDV server failed to acquire bandwidth from the DNCS SRM.

Severity:

Major

Service Impact:

- An initializing SDV SRM cannot acquire bandwidth for SDV programs.
- SDV servers already running cannot acquire additional bandwidth as needed.

Check and Correct:

Possible Causes	Check and Correct Instructions
■ The DNCS is not responding. ■ The DNCS SRM is not responding. ■ There is a possible network problem between the SDV server and the DNCS. ■ A VASP entry for the SDV server is not entered into the DNCS database.	■ Investigate and troubleshoot your network, as this issue could be network-related. Contact Cisco Services for further assistance. ■ Verify that the correct VASP ID is entered for the SDV server. **Note:** In rare cases, you may see toggling between the primary and backup SDV servers. This condition should be resolved within approximately 1 minute.

SDV Server Trap 2 (2 Hex)

Alarm Summary:

SDV Server Unable to Communicate with Partner SDV Server

Description:

This alarm occurs when the secondary SDV server attempts to connect with the primary SDV server.

Severity:

Minor

Service Impact:

When this alarm occurs, no protection switch or failover can take place between the secondary and primary server.

Check and Correct:

Possible Causes	Check and Correct Instructions
■ The primary SDV server is not responding. ■ The primary SDV server High Availability Manager is not responding. ■ There is a possible network problem between the SDV server and the DNCS. ■ The incorrect IP Address is entered for the primary SDV server.	■ Investigate and troubleshoot your network, as this issue could be network-related. Contact Cisco Services for further assistance. ■ Verify that the correct IP Address is entered for the primary SDV server.

SDV Server Trap 6 (6 Hex)

Alarm Summary:

SDV Server Failed to Communicate with Edge Device

Description:

This alarm occurs when the SDV SRM process cannot ping the edge device or GQAM modulator.

Severity:

Major

Service Impact:

When this alarm occurs, an SDV program cannot be established on the edge device.

Check and Correct:

Possible Cause	Check and Correct Instructions
The network between the SDV server and the edge device is not responding.	1 Try to ping the edge device and/or query it through SNMP using an alternate route (for example, not through the SDV server). 2 If the edge device responds, the problem is probably within the network between the edge device and SDV server. 3 If the edge device does not respond, then proceed to the next possible cause. 4 Check and verify the amount of bandwidth allotted for your service groups.
The edge device is not responding.	Try to assess the cause of the failure, and then reset the QAM device to restore service.

SDV Server Process Alarms

SDV Server Trap 50 (32 Hex)

Alarm Summary:

SDV Server Resource Manager Stopped

Description:

This alarm occurs when the SDV server SRM process stops.

Severity:

Critical

Service Impact:

When this alarm occurs, some CCMIS requests for new SDV programs will fail, if the Resource Manager bandwidth is exhausted. The SDV server cannot create new program bindings on the edge device or request additional bandwidth from the DNCS as needed.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Server Trap 51 (33 Hex)

Alarm Summary:

SDV Server CCMIS Process Stopped

Description:

This alarm occurs when the SDV server CCMIS process has stopped.

Severity:

Critical

Service Impact:

When this alarm occurs, all CCMIS requests for SDV programs fail, and new SDV programs cannot be established on the edge device. The mini carousel will not contain tuning information for new programs.

Note: If this alarm is the only failure, then the SDV server will continue to multicast the mini carousel.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services to request an examination of the memory logs.

SDV Server Trap 52 (34 Hex)

Alarm Summary:

SDV Server MCMIS Process Stopped

Description:

This alarm occurs when the SDV server MCMIS process has stopped.

Severity:

Critical

Service Impact:

When this alarm occurs, mini carousel data is not available for the DHCTs to update program tuning information.

Note: DHCTs will be able to get program tuning information through CCMIS requests. However, new DHCTs that are trying to access the SDV service will not be able to register or receive programming information.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Server Trap 53 (35 Hex)

Alarm Summary:

SDV Server Bandwidth Manager Stopped

Description:

This alarm occurs when the SDV Bandwidth Manager process has stopped. The SDV bandwidth manager monitors bandwidth to enable the SDV server to stay ahead of demand for new programs.

Severity:

Major

Service Impact:

When this alarm occurs, the SDV server cannot monitor bandwidth utilization and request bandwidth to stay ahead of the demand. The SDV server will need to request bandwidth or unbind low priority programs in real-time in this situation. CCMIS requests may also experience some latency when this alarm occurs.

Note: There is a setting on the Server Configuration page called **Demand BW Request**. The default setting is **Off**. If the server Bandwidth Manager fails in this configuration, the server will not go out and request bandwidth from the DNCS. The server will only use what it has existing in its pool. If the Demand BW Request setting is **On**, then the screen will go out and request bandwidth in real time. This is a manual setting, not automatic.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Server Trap 54 (36 Hex)

Alarm Summary:

SDV Server Program Manager Stopped

Description:

This alarm occurs when the SDV Program Manager process has stopped. The program manager manages SDV program attributes and ranks program priorities.

Severity:

Minor

Service Impact:

When this alarm occurs, the SDV server is unable to activate new programs or tear down old programs.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Server Trap 55 (37 Hex)

Alarm Summary:

SDV Server Maintenance Manager Stopped

Description:

This alarm occurs when the maintenance manager process has stopped. The maintenance manager monitors the health of the SDV server system.

Severity:

Minor

Service Impact:

When this alarm occurs, the SDV server cannot perform scheduled maintenance on itself and the devices it controls.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Server Trap 56 (38 Hex)

Alarm Summary:

SDV Server Web Server Stopped

Description:

This alarm occurs when the Web Server has stopped. The Web Server allows access to the SDV server platform from a Web interface.

Severity:

Minor

Service Impact:

When this alarm occurs, the SDV server Web interface is not available.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Server Trap 57 (39 Hex)

Alarm Summary:

SDV Server Redundancy Process Stopped

Description:

This alarm occurs when the redundancy process has stopped. The redundancy process is responsible for protection switches between partner SDV servers and the communications between these servers.

Severity:

Major

Service Impact:

Until this alarm is resolved, protection switches are not possible.

Check and Correct:

Possible Cause	Check and Correct Instructions
A software bug such as a memory leak or exceptions.	1 Reboot the SDV server. 2 Contact Cisco Services immediately to request an examination of the memory logs.

SDV Session Alarms

SDV Server Trap 100 (64 Hex)

Alarm Summary:

SDV Session Bind Failure

Description:

This alarm occurs when the server fails to bind a program to a session on the edge device.

Severity:

Major

Service Impact:

When this alarm occurs, the SDV client is denied service because a new program could not be established on the edge device.

Check and Correct:

Possible Cause	Check and Correct Instructions
The edge device may be unreachable.	1 Analyze the error code associated with the alarm and determine if the SDV Server Alarm ID 6 (6 Hex) also occurred. 2 If SDV Server Alarm ID 6 has occurred, then refer to the Check and Correct procedures for ***SDV Server Trap 6 (6 Hex)*** (on page 31). 3 If the SDV Server Alarm ID 6 has not occurred, then proceed to the next possible cause. 4 Check and verify the amount of bandwidth allotted for the service groups.
Edge device software error.	Investigate the edge device alarms and try to assess the cause of the error.

SDV Server Trap 101 (65 Hex)

Alarm Summary:

SDV SRM Interactive Session Bandwidth Request Denied

Description:

This alarm occurs when the DNCS denies the SDV server's request for more bandwidth.

Severity:

Major

Service Impact:

This condition may hamper the following abilities of the SDV server:

- The ability to stay ahead of demand for new programs
- The ability to satisfy a new CCMIS request in real-time

Check and Correct:

Possible Cause	Check and Correct Instructions
No available edge device bandwidth.	1 Check the bandwidth allocated for the affected service group and verify that the maximum bandwidth is allocated. 2 Verify that all allocated QAMs are operational. 3 Verify that all service group resources are being fully utilized. 4 The service group may need to be re-engineered to provide additional QAM capacity. Contact Cisco Services for further assistance.

SDV Server Capacity Alarms

SDV Server Trap 200 (C8 Hex)

Alarm Summary:

SDV Server Disk Full

Description:

This alarm occurs when the server's hard disk is full.

Severity:

Critical

Service Impact:

The server stops logging data when this condition occurs.

Check and Correct:

Possible Cause	Check and Correct Instructions
Unnecessary files are taking up disk space on the SDV server.	**Note:** Check the ActivityLog and EventLog directories on the SDV server. Consider reducing the number of days you have configured on the DNCS to delete SDV activity and event logs from your system. **(Quick Path: DNCS > SDV Server List > Update SDV Server > Constraints)** Follow these steps to delete any unnecessary ActivityLog and/or EventLog files on the SDV server. 1 On the SDV server, log in as **root** user. 2 Type **df -k** and press **Enter** to determine the percentage of disk usage by partition. 3 Type **cd /opt/sdb/ActivityLog/** and press **Enter** to make the opt/sdb/ActivityLog directory the working directory. 4 Type **rm <file name>** and press **Enter** to delete any unnecessary text files from the opt/sdb/ActivityLog directory. 5 **Note:** The activity log filename is in the format ddmmmyyyy.txt. For example: rm 30Jun2006.txt. 6 Type **cd /opt/sdb/EventLog/** and press **Enter** to make the opt/sdb/EventLog directory the working directory. 7 Type **rm <file name>** and press **Enter** to delete any unnecessary text files from the opt/sdb/EventLog directory. 8 **Note:** The event log filename is in the format **ddmmmyyyy.txt**. For example: **rm 30Jun2006.txt**. 9 Type **df -k** and press **Enter** to check the disk usage by partition again. (Because you deleted unnecessary Log files in this procedure, the percentage of disk usage should now be reduced.) 10 Type **exit** and press **Enter** to log out as root user. 11 Type **exit** and press **Enter** to close the xterm window.

SDV Server Trap 201 (C9 Hex)

Alarm Summary:

SDV Server Memory Threshold Exceeded

Description:

This alarm occurs when the SDV server exceeds the configured memory usage threshold that triggers a major alarm.

Severity:

Major

Service Impact:

When this alarm occurs, the SDV server is within 10% of reaching the maximum memory usage threshold.

Important! If this alarm occurs frequently, you should consider upgrading the SDV server memory, as this condition might impact your overall SDV server performance.

Check and Correct:

Possible Cause	Check and Correct Instructions
SDV server loading problems.	If loading problems periodically occur, it could be a result of too much load on your system. You may need to reduce the size of your service groups or upgrade your server memory. Contact the representative that handles your account for more information.to arrange a memory upgrade for your SDV server.
Memory leak.	Call Cisco Services immediately for further assistance.

SDV Server Trap 202 (CA Hex)

Alarm Summary:

SDV Server DHCT Table Full

Description:

This alarm occurs when the SDV server exhausts the capacity of its DHCT table. (The SDV server keeps track of the DHCT population across all service groups.)

Severity:

Major

Service Impact:

DHCTs will not be able to tune to additional SDV channels.

Check and Correct:

Possible Cause	Check and Correct Instructions
The DHCT table for the SDV server is full.	1 Consider moving a service group to another SDV server. 2 Consider purchasing an SDV server license capable of handling more DHCTs. Contact the representative that handles your account for more information.

SDV Server Trap 203 (CB Hex)

Alarm Summary:

SDV Server Total DHCT Capacity Threshold Exceeded

Description:

This alarm occurs when the SDV server exceeds the default threshold of its DHCT table. (The SDV server keeps track of the DHCT population across all service groups.)

Severity:

Minor

Service Impact:

When this alarm occurs, the SDV server is within 10% of the maximum number of DHCTs that the server can support across the server's service groups.

Check and Correct:

Possible Cause		Check and Correct Instructions
The DHCTs table for the SDV server is approaching the maximum threshold value due to the number of DHCTs per service group on the SDV server.	1	Consider moving a service group to another SDV server.
	2	Consider purchasing an SDV server license capable of handling more DHCTs. Contact the representative that handles your account for more information.

SDV Server Trap 204 (CC Hex)

Alarm Summary:

SDV Server Bandwidth Utilization Threshold Exceeded

Description:

This alarm occurs when a customer-defined threshold based on the maximum bandwidth for the service group has been exceeded. The SDV server keeps track of the bandwidth utilization per service group.

Severity:

Minor

Service Impact:

When this alarm occurs, the service group bandwidth utilization is within 10% of reaching your defined bandwidth threshold.

Check and Correct:

Possible Cause	Check and Correct Instructions
Too many DHCTs in the SDV server service group.	1 Consider splitting the service group for the SDV server and moving the new service group to a different server. 2 Consider adding additional QAMs to your system. Contact the representative that handles your account for more information.

SDV Server Trap 205 (CD Hex)

Alarm Summary:

SDV Server Bandwidth Exhausted

Description:

This alarm occurs when the service group bandwidth is fully utilized. When this event occurs, the server cannot fit any additional programs on the remaining bandwidth.

Severity:

Major

Service Impact:

This event limits the ability of the SDV server to satisfy CCMIS requests for new programs.

Check and Correct:

Possible Cause		Check and Correct Instructions
Service group bandwidth is fully utilized.	1	Check the bandwidth allocated for the affected service group and verify that the maximum bandwidth is allocated.
	2	Consider adding additional QAMs to your system. Contact the representative that handles your account for more information.

SDV Server Trap 206 (CE Hex)

Alarm Summary:

SDV Server Disk Exceeding Threshold

Description:

This alarm occurs when the SDV server exceeds its hard disk capacity threshold.

Severity:

Major

Service Impact:

When this alarm occurs, the SDV server is within 10% of reaching the hard disk capacity threshold.

Check and Correct:

Possible Cause	Check and Correct Instructions
Too many non-service affecting files are taking up disk space on the SDV server.	**Note:** Check the ActivityLog and EventLog directories on the SDV server. Consider reducing the number of days you have configured on the DNCS to delete SDV activity and event logs from your system. **(Quick Path: DNCS > SDV Server List > Update SDV Server > Constraints)** Follow these steps to delete any unnecessary ActivityLog and/or EventLog files on the SDV server. 1 On the SDV server, log in as **root** user. 2 Type **df -k** and press **Enter** to determine the percentage of disk usage by partition. 3 Type **cd /opt/sdb/ActivityLog/** and press **Enter** to make the opt/sdb/ActivityLog directory the working directory. 4 Type **rm <file name>** and press **Enter** to delete any unnecessary text files from the opt/sdb/ActivityLog directory. 5 **Note:** The activity log filename is in the format **ddmmmyyyy.txt**. For example: **rm 30Jun2006.txt**. 6 Type **cd /opt/sdb/EventLog/** and press **Enter** to make the opt/sdb/EventLog directory the working directory. 7 Type **rm <file name>** and press **Enter** to delete any unnecessary text files from the opt/sdb/EventLog directory. 8 **Note:** The event log filename is in the format **ddmmmyyyy.txt**. For example: **rm 30Jun2006.txt**. 9 Type **df -k** and press **Enter** to check the disk usage by partition again. (Because you deleted unnecessary Log files in this procedure, the percentage of disk usage should now be reduced.) 10 Type **exit** and press **Enter** to log out as root user. 11 Type **exit** and press **Enter** to close the xterm window.

SDV Server Trap 207 (CF Hex)

Alarm Summary:

SDV Service Group DHCT Capacity Threshold Exceeded

Description:

This alarm occurs when the DHCT capacity threshold is exceeded for a given service group.

Severity:

Minor

Service Impact:

DHCTs will not be able to tune to additional SDV channels.

Check and Correct:

Possible Cause	Check and Correct Instructions
Increased DHCT population.	1 Consider splitting the service group for the SDV server and moving the new service group to a different server. 2 Consider purchasing an SDV server license capable of handling more DHCTs, or purchasing additional SDV servers for your system. Contact the representative that handles your account for more information.

SDV Server Trap 208 (D0 Hex)

Alarm Summary:

SDV Service Group DHCT Capacity Exceeded

Description:

This alarm occurs when the SDV server is getting requests from more DHCTs than the server can support.

Severity:

Major

Service Impact:

DHCTs will not be able to tune to additional SDV channels.

Check and Correct:

Possible Cause	Check and Correct Instructions
Too many DHCTs in service group.	The current SDV server license cannot support any additional DHCTs. Contact the representative that handles your account for more information.

SDV Server Trap 209 (D1 Hex)

Alarm Summary:

SDV Channel Change Request Denied for Lack of Bandwidth

Description:

This alarm occurs when the SDV server denies channel changes for new programs for lack of available bandwidth.

Severity:

Major

Service Impact:

This event affects the end-user experience.

Check and Correct:

Possible Cause		Check and Correct Instructions
SDV server does not have additional bandwidth available.	1	Check the bandwidth allocated for the affected service group and verify that the maximum bandwidth is allocated.
	2	Verify that all allocated QAMs are operational.
	3	Verify that all allocated QAMs are fully loaded based on bandwidth allocation.
	4	Consider adding additional QAMs to your system. Contact the representative that handles your account for more information.

SDV Maintenance and Provisioning Alarms

SDV Server Trap 300 (12C Hex)

Alarm Summary:

SDV Server Initialization Trap

Description:

This event occurs when the SDV server sends an exception to the SDV Manager to request provisioning.

Severity:

Status

Service Impact:

This event is an indication that the SDV server is initializing. No action is required.

SDV Server Trap 301 (12D Hex)

Alarm Summary:

SDV Server Provisioned

Description:

This status event is sent to inform the SDV Manager that the server successfully initialized or provisioned itself.

Severity:

Status

Service Impact:

This event is an indication that the SDV server has initialized. No action is required.

SDV Server Trap 302 (12E Hex)

Alarm Summary:

SDV Server Provision Request Failure

Description:

This alarm occurs when the SDV request for provisioning times out.

Severity:

Major

Service Impact:

If the SDV server is initializing for the first time or is synching up with the SDV Manager after provisioning data loss, the SDV server is unable to provide service.

Check and Correct:

Possible Cause		Check and Correct Instructions
Initialization has timed out too many times.	1	If any SDV System Communications or SDV Server Process alarms occurred, refer to the specific alarm Check and Correct procedures to troubleshoot and resolve any issues.
	2	You may need to reboot the SDV server.

SDV Program Management Alarms

SDV Server Trap 400 (190 Hex)

Alarm Summary:

Program Removed with Viewers

Description:

This alarm occurs when the SDV server removes a program from the edge device to free up bandwidth for a higher-priority program.

Severity:

Minor

Service Impact:

Important: If this alarm occurs frequently, it may be an indicator of insufficient bandwidth allocation for the service group.

Check and Correct:

Possible Cause	Check and Correct Instructions
Program priority or business rule triggered action.	This alarm occurs when one of the following instances occurs: ■ When the DNCS demands the removal of programs from the SDV server ■ When the SDV server detects no recent subscriber activity and bandwidth is required to satisfy a new program request (for example, bandwidth reclamation) If this alarm occurs frequently, consider the following options to add additional bandwidth to the affected service group: ■ Check the bandwidth allocated for the affected service group and verify that the maximum bandwidth is allocated. ■ Add additional QAMs to your system. Contact the representative that handles your account for more information.

SDV Redundancy Alarms

SDV Server Trap 500 (1F4 Hex)

Alarm Summary:

SDV Server Standby Active

Description:

This event occurs when the standby or backup SDV server takes over for the primary SDV server.

Severity:

Status

Service Impact:

None

Check and Correct:

Possible Cause	Check and Correct Instructions
Primary SDV server failure.	Investigate all SDV server alarms that may have occurred around the time of the SDV server failure, as this issue could be network-related. Contact Cisco Services for further assistance.
Forced switchover from primary SDV server to backup SDV server.	No action required.

SDV Server Trap 501 (1F5 Hex)

Alarm Summary:

SDV Forced Protection Switch Failure

Description:

This alarm occurs when the SDV server cannot perform a protection switch to its partner SDV server.

Severity:

Major

Service Impact:

This is a redundancy failure that impacts the ability to use an SDV server as a backup.

Check and Correct:

Possible Cause	Check and Correct Instructions
Communications problem.	Investigate and troubleshoot all SDV System Communications alarms.
Partner SDV server is down.	1 Investigate all SDV server alarms and errors that may have occurred around the time of the SDV server failure, particularly SDV Server Process alarms prior to the time of the failure. 2 Call Cisco Services immediately for further assistance.

SDV Server Trap 502 (1F6 Hex)

Alarm Summary:

SDV Server Heartbeat Trap

Description:

This event is sent to the SDV Manager by a secondary SDV server (operating in standby mode) or by a primary SDV server (if redundancy is not implemented).

Severity:

Status

Service Impact:

If redundancy is implemented, the primary SDV server periodically issues a heartbeat to the backup server and not to the SDV Manager. No action is required.

SDV Server Trap 504 (1F8 Hex)

Alarm Summary:

SDV Server Redundant Network Failure

Description:

This alarm occurs when the backup SDV server cannot communicate with all of its primary servers.

Severity:

Major

Service Impact:

A forced or automatic protection switch cannot take place with any primary server that the backup server cannot communicate with if this condition persists.

Check and Correct:

Possible Cause	Check and Correct Instructions
Communications problem.	1 Investigate and troubleshoot the communications link between the backup SDV server and the primary SDV servers. 2 Contact Cisco Services for further assistance.

3

Accessing SDV Diagnostic Screens

This chapter includes the diagnostic screens specific to SDV, including the fields and parameters that are included within these screens. These screens accumulate data that describe information about the SDV feature, as well as transmission information and the mini carousel.

In This Chapter

Switched Digital Video Diagnostic Screen

Introduction

This section provides an overview of the Switched Digital Video diagnostic screen, and includes information that describes the SDV client and server, including the number of SDV channels that have been authorized for this service. Detailed statistics about the SDV protocol are also included in this diagnostic screen.

Performing Tasks

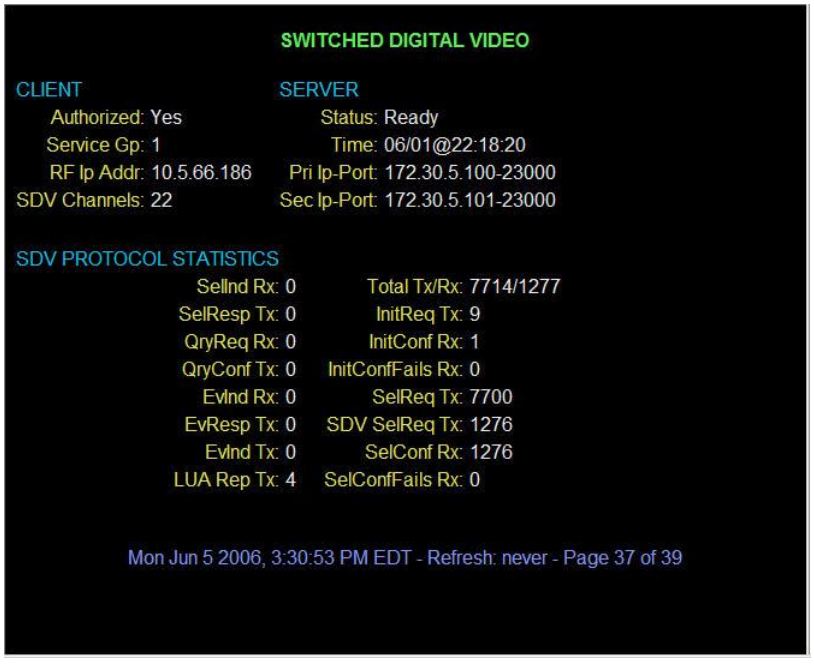
By accessing this diagnostic screen, you can perform the following tasks:

- Determine if the client (DHCT) is authorized for SDV services
- Identify the status of the SDV server
- Verify details about the transmission of data for the SDV service

Screen Components

- Client
- Server
- SDV Protocol Statistics

Example:



Screen Fields and Values

The following table describes the fields and possible values that can appear on the TV screen when you are reviewing the CableCARD diagnostic screens. They can be useful for troubleshooting.

Client

Field Name	Description	Possible Values
Authorized	Indicates whether or not the client is authorized for SDV service (_SASD service) or the_SASD service does not exist	■ **Yes**: service is authorized ■ **No**: service is not authorized ■ **n/a**: service does not exist
Service Gp	The ID of the service group to which this client belongs	■ **[Integer ≥ 1]** ■ **n/a**: service does not exist
RF Ip Address	The IP address for the RF network	■ **[Network-dependent]**
SDV Channels	The number of SDV channels (watchtv;SASD services) in the channel lineup	■ **[Integer ≥ 0]**

Server

Field Name	Description	Possible Values
Status	The current status of the client communications with the SDV server (init request and receiving a response)	■ **Ready**: (desired value) init request is successfully confirmed and accepted by the SDV server ■ **Pending**: the set-top is in the process of establishing communications with the SDV server ■ **Unavailable**: init request failed ■ **Unknown**: init request not yet initiated
Time	The time of the last successful initial request confirmed by the server	■ **[month/day@hh:mm:sec]**
Pri Ip-Port	The IP address and port number (IP address-Port number) for the primary SDV server	■ **[Network-dependent]** **Example**: 192.168.99.5-2300 ■ **0.0.0.0-n/a**: primary SDV server is not available
Sec Ip-Port	The IP address and port number (IP address-Port number) for the secondary SDV server	■ **[Network-dependent]** **Example**: 192.168.99.5-23000 ■ **0.0.0.0-n/a**: secondary SDV server is not available

SDV Protocol Statistics

The SDV Protocol section displays statistics for the external protocol messages used for SDV. These statistics are combined for all sessions and protocols.

Field Name	Description	Possible Values
SelInd Rx	The number of Select Indications received	■ **[Integer ≥ 0]**
SelResp Tx	The number of Select Responses sent	■ **[Integer ≥ 0]**
QryReq Rx	The number of Query Requests received	■ **[Integer ≥ 0]**
QryConf Tx	The number of confirmed Query Responses sent	■ **[Integer ≥ 0]**
EvInd Rx	The number of Event Indications received	■ **[Integer ≥ 0]**
EvResp Tx	The number of Event Responses sent	■ **[Integer ≥ 0]**
EvInd Tx	The number of Event Indications sent	■ **[Integer ≥ 0]**
LUA Rep Tx	The number of LUA (Last User Activity) reports sent	■ **[Integer ≥ 0]**
Total Tx/Rx	The total number of requests sent and received	■ **[Integer ≥ 0]/[Integer ≥ 0]**
InitReq Tx	The total number of init requests sent, excluding retransmissions	■ **[Integer ≥ 0]**
InitConf Rx	Total number of initial confirm messages received from SDV server that indicate success or failure	■ **[Integer ≥ 0]**
InitConfFails Rx	Total number of initial confirms received from the SDV server that indicate failure	■ **[Integer ≥ 0]**
SelReq Tx	The total number of select requests sent for SDV and non-SDV services, excluding retransmissions	■ **[Integer ≥ 0]**
SDV SelReq Tx	The total number of select requests sent for SDV, excluding retransmissions	■ **[Integer ≥ 0]**
SelConf Rx	The total number of select confirm messages received from SDV server that indicate success or failure	■ **[Integer ≥ 0]**

Field Name	Description	Possible Values
SelConfFails Rx	The total number of select confirms received from the SDV server that indicate failure	■ **[Integer ≥ 0]**

SDV Mini Carousel Diagnostic Screen

Introduction

This section provides an overview of the SDV Mini Carousel diagnostic screen, and includes information that describes the Mini Carousel (MC) Discovery Files, as well as details about the MC data. The MC Discovery Files are generated by the DNCS and placed on BFS to support the inband MC discovery process for an SDV client. Only one SDV MC Discovery file exists per service group. It is located in the bfs:///sgm/sdv/ib directory. MC data is generated by the SDV server for each service group and placed in the transport stream as Private MPEG packets.

Important: The DNCS-generated mini carousel discovery files are ignored by the tuning adapter if your system includes a fixed scan list of SDV frequencies in the tuning adapter config file or in the _SASD SAM Service URL. In this case, the mini carousel discovery file information data is populated based on the fixed scan list that you have included on your system. For details about using a fixed scan list, refer to *Provisioning the DNCS to Support SDV Services User Guide* (part number 4012948).

Performing Tasks

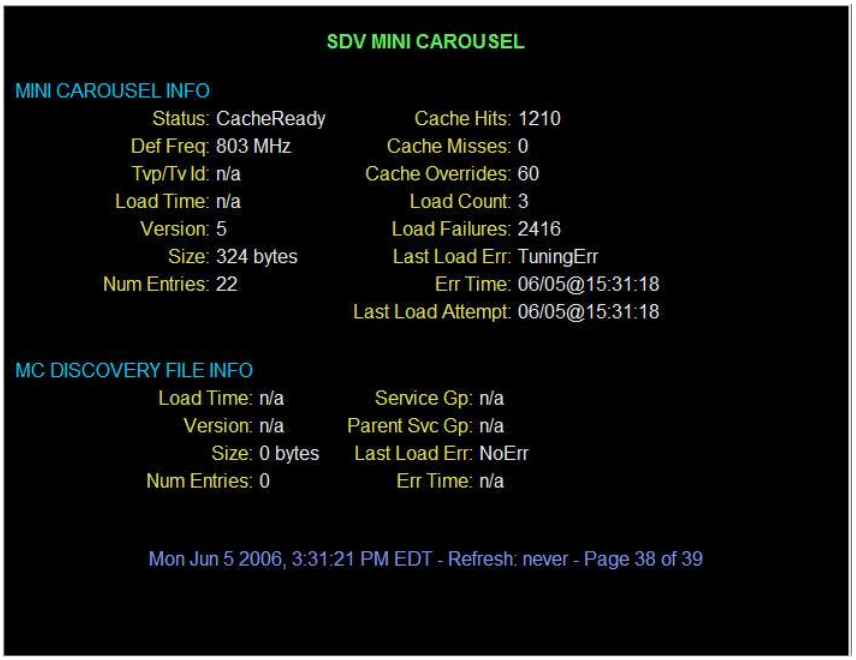
By accessing this diagnostic screen, you can perform the following tasks:

- Determine the date and time that the mini carousel was last loaded in cache
- Determine the current status for the mini carousel
- Identify the version for the mini carousel

Screen Components

- Mini Carousel Info
- MC Discovery File Info

Example:



Screen Fields and Values

The following table describes the fields and possible values that can appear on the TV screen when you are reviewing the CableCARD diagnostic screens. They can be useful for troubleshooting.

Mini Carousel Info

Field Name	Description	Possible Values
Status	The current status of the information from the mini carousel	■ **Init**: initial state at boot time prior to loading mini carousel data. Also the state reported when the set-top is not authorized for SDV ■ **SgDiscovery**: client is performing or waiting to perform the service group discovery process ■ **McpDiscFileRead**: client is reading or waiting to read the BFS file to obtain a list of SDV QAM frequencies to scan for mini carousel data ■ **McpDiscovery**: client is scanning or waiting to scan SDV QAM frequencies in search of mini carousel data ■ **CacheReady**: (desired value) mini carousel loaded and data acquired to allow viewing of SDV channels
Def Freq	The default or home SDV frequency in MHz. The client will tune to this frequency to read the mini carousel data if not already tuned to another SDV frequency	■ **[Integer ≥ 0]**
Tvp/Tv Id	The internal identifier of the logical hardware resource assigned or allocated for loading inband mini carousel data	■ **[Integer ≥ 1]** ■ **n/a**: no logical tuner resource is currently assigned or allocated for loading the inband mini carousel
Load Time	The time when the mini carousel information was loaded into cache	■ **[month/day@hh:mm:sec]**
Version	The version number for the mini carousel cached file	■ **[0 to 31]**
Size	The size of the mini carousel data (bytes)	■ **[Integer ≥ 0]**
Num Entries	The number of programs (channels) in the mini carousel data	■ **[Integer ≥ 0]**

Field Name	Description	Possible Values
Cache Hits	The number of times requested tuning parameters were successfully received from the mini carousel cache **Notes:** ■ This includes cache hits after forcing a reload of the mini carousel. ■ This value is only reset to zero when it rolls over or the agent is reset.	■ **[Integer ≥ 0]**
Cache Misses	The number of times requested tuning parameters were not found in the mini carousel cache even after reloading mini carousel data **Note:** This value is only reset to zero when it rolls over or the agent is reset.	■ **[Integer ≥ 0]**
Cache Overrides	The number of times the cached tuning parameters from the mini carousel have been overridden by fresh tuning parameters received from the SDV server via CCP (Channel Change Protocol) **Note:** This value is only reset to zero when it rolls over or the agent is reset.	■ **[Integer ≥ 0]**
Load Count	The number of times the mini carousel data has successfully been read (or loaded) by the client **Note:** This value is only reset to zero when it rolls over or the agent is reset.	■ **[Integer ≥ 0]**
Load Failures	The number of times the client has failed to read the mini carousel data **Note:** This value is only reset to zero when it rolls over or the agent is reset.	■ **[Integer ≥ 0]**

Field Name	Description	Possible Values
Last Load Err	The type of error for the last load (read) of the mini carousel	■ **NoErr**: last load was successful ■ **ReadErr**: read of last load failed ■ **MemFull**: not enough memory for last load ■ **Aborted**: last load attempt was aborted ■ **TuningErr**: tuning failure during last load ■ **SGMismatch:** service group identified in the mini carousel data does not match the set-top's service group found during service group discovery ■ **UnknownErr**: an unknown error occurred during load
Err Time	The time when the last error occurred in loading	■ **[month/day@hh:mm:sec]** ■ **n/a**: no load errors have occurred since reset
Last Load Attempt	The time when the last load was attempted on the DHCT	■ **[month/day@hh:mm:sec]** ■ **00/00@00:00:00**: no load errors have occurred since reset

MC Discovery File Info

Field Name	Description	Possible Values
Load Time	The time when the MC Discovery file was loaded on the DHCT during discovery	■ **[month/day@hh:mm:sec]** ■ **n/a**: file is not loaded
Version	The current version of the MC Discovery File, expressed as a timestamp of when the file contents were generated by the DNCS	■ **[month/day@hh:mm:sec]**
Size	The size of the MC Discovery File in bytes	■ **[Integer ≥ 0]**
Num Entries	The total number of tuning parameter entries in the MC Discovery File	■ **[Integer ≥ 1]** ■ **0**: no entries
Service Gp	The service group of the currently loaded MC Discovery File **Note:** In systems with no parent/child service groups, this should match the service group identified on the VOD Information and the Switched Digital Video diagnostic pages	■ **[Integer ≥ 1]** ■ **n/a**: MC Discovery file not loaded
Parent Svc Gp	The next higher level parent service group in the hierarchy above the child service group	■ **[Integer ≥ 1]** ■ **n/a**: MC Discovery File not loaded or there is no parent service group above the child service group

Field Name	Description	Possible Values
Last Load Err	The error status from the last load of the mini-carousel data (MCD) in discovery. The status reflects the last error type after a successful load of the MCD	■ **NoErr**: successful load ■ **BadParamErr:** bad parameters specified ■ **OutOfStateErr:** load request denied due to inappropriate state ■ **FileNotFoundErr:** MCD file does not exist on BFS for this service group ■ **OutOfMemoryErr:** insufficient memory to process request ■ **ReadErr**: failed to read MCD file from BFS ■ **TunerConflictErr**: could not load MCD file due to higher priority tuner request ■ **FileChangedErr**: MCD file changed on BFS during read ■ **TimeoutErr**: request timed out ■ **AbortedErr**: request was intentionally aborted ■ **BadDataErr**: the data was loaded successfully but is invalid ■ **UnknownErr**: unknown error occurred during load attempt
Err Time	The time at which the last discovery file load error was reported	■ **[month/day@hh:mm:sec]** ■ **n/a**: no file load has occurred

SDV Session Info Diagnostic Screen

Introduction

This section provides an overview of the SDV Session Info diagnostic screen, and includes information that describe the details of SDV-related sessions, including the current SDV and tuner status.

Performing Tasks

By accessing this diagnostic screen, you can perform the following tasks:

- Determine the current status of an SDV session
- Determine the current status of the tuner
- Verify the name of the current SDV session

Screen Components

- Session-1
- Session-2

Example:

Screen Fields and Values

The following table describes the fields and possible values that can appear on the TV screen when you are reviewing the CableCARD diagnostic screens. They can be useful for troubleshooting.

Field Name	Description	Possible Values
Name – Status	The name and current status of the session	■ **[Name of Session]** and one of the following: • **Ready**: tuning parameters have been acquired • **Idle**: no service is selected for this session • **Pending**: Session Manager is waiting for tuning parameters from either the cache manager or the SDV server • **Unavailable**: failed to acquire tuning parameters for the selected SDV service
Session Id	The 10-byte session ID for the that uniquely identifies the SDV client/server session within the system	■ **[Session-dependent]**
SamSvcId/Type	The SAM service ID identifying the program and type of service defined for that session	■ **[Integer ≥ 0]** and one of the following: • **Switched**: switched digital service • **Broadcast**: broadcast service • **n/a**
Source Id	The ATSC source ID	■ **[Integer ≥ 0]**
Act Time	The time of activation for the session	■ **[month/day@hh:mm:sec]**
Retries/Resends	The number of times a select request has been resent due to timeout or user initiated retry, or due to a resend request for the currently selected service	■ **[Integer ≥ 0]/[Integer ≥ 0]**
Retunes	The number of times the client has received updated tuning parameters for currently selected service requiring a retune	■ **[Integer ≥ 0]**

Field Name	Description	Possible Values
Tuner Status	The tuner status from an SDV perspective	■ **Active**: successfully tuned ■ **Inactive**: not using a tuner ■ **n/a**: session has not yet requested a tuner
Tuner Use	An indication of how the tuner is being used	■ **Main**: tuner is being used for main TV display ■ **Rec**: tuner is being used for a scheduled recording ■ **PPV**: tuner is being used for pay-per-view (PPV) content ■ **PIP**: tuner is being used for picture-in-picture (PIP) ■ **n/a**: no tuner is in use for this session
Tv/Rec Rsrc	The internal identifiers for the logical hardware resources allocated for presenting and recording the SDV service	■ **[Integer ≥ 0]**: current service to viewer is either on main TV, PIP, or AUX OUT ■ **0**: current service to viewer is not on main TV, PIP, or AUX OUT
SDV Freq	The frequency (MHz) used by the agent to tune to the currently selected SDV service	■ **[Integer ≥ 0]**
LUA Tx Time	The time when the last user action was reported to the SDV server	■ **[month/day@hh:mm:sec]** ■ **n/a**

Field Name	Description	Possible Values
Last CCP Err	The last error from the CCP (Channel Change Protocol) for this session	■ **NoErr**: no error was reported ■ **Timeout**: timeout waiting on response from server ■ **OutOfService**: program is no longer available ■ **FormatErr**: invalid format in CCP sent to server ■ **Redirect**: force tune indication from server ■ **InvalidSG**: server cannot identify service group from its topology ■ **UnknownClient**: agent has not registered with server ■ **NoResource**: session resource is unavailable ■ **BWNotAvail**: bandwidth bind on edge device failed ■ **ExceedsCapacity**: server capacity of agents has exceeded ■ **VerNotSupported**: agent version is not supported ■ **unknownErr**: unknown error ■ **n/a**: CCP was not initiated
Err Time	The time that the last error was reported from the CCP for this session	■ **[month/day@hh:mm:sec]** ■ **n/a**: no errors reported

4

Troubleshooting SDV System Issues

Introduction

This chapter identifies how to troubleshoot and resolve any SDV issues that may occur in the field. Common issues are described and diagnostic measures are presented to help you to determine why these system issues might be present.

Note: If the suggested actions to any system issue do not yield results or you are unable to correct a problem that the diagnostics tool seems to demonstrate, contact Cisco Services.

In This Chapter

Troubleshooting Scenarios

This section identifies the SDV troubleshooting scenarios that could arise in the field, and includes the steps for resolving these scenarios.

The most common issues are described and diagnostic measures are presented to help you to determine why these issues might be present.

Note: Suggested resolutions are provided for two groups: field technicians and Customer Service Representatives (CSRs).

Subscribers Are Seeing a Black Screen on an SDV Channel

Description

No picture is displaying for SDV channels on the television screen.

Possible Causes

- An authorization issue exists at the source.
- RF signal is lost.
- QAM signal is lost.

Diagnosing the Issue

See the following table to diagnose why subscribers are seeing a "black screen."

Important: The page number for the SDV diagnostic screens may vary, depending on the set-top model.

Access the following diagnostic screen.	Gather the following parameters.	Action
Page 38–SDV Session Info	ATSCSrcId	Field Techs: Escalate the problem to the appropriate tier
	SDV Freq	Field Techs: Record the frequency value for the agent

Macroblocking Issues

Description

The picture on an SDV channel freezes, shows blocking, or shows tiling (macroblocking).

Possible Causes

- Some type of interference with the external signal.
- The signal-to-noise (S/N) ratio is out of range.
- The signal level is not within the acceptable working range.
- Too much compression has been applied to the signal. (See pages 87–89 for steps to troubleshoot.)

Diagnosing the Issue

See the following table to diagnose why the SDV channel is freezing, showing blocking, or showing tiling.

Important:

- The page number for the diagnostic screens may vary, depending on the set-top model.
- Please check all of the diagnostic screens and fields contained in the following table *before* you call Cisco Services. Various combinations of failures will point to the source of any potential problems as listed in the following examples.

  Examples:

  - If the signal levels are good, the S/N value is poor, and there is a rapid change in byte counts, then noise ingress is present.
  - If the signal levels are poor, the S/N value is poor, and there is a rapid change in byte counts, then there is a "drop" problem.
  - If the signal levels, S/N value, and byte counts are good, and a problem continues to exist, an issue exists prior to the QAM or transport network.

Access the following diagnostic screen.	Evaluate the following field.	What value do I want to see?
Page 1–Status Summary	Tuner (or Tuner 1 if a DVR set-top	**Frequency level of inband tuner should display in the "white"**—acceptable range **-8dBmV** to **+8dBmV**—recommended range **Note:** If the tuner value appears in amber or red, check the signal levels.

Access the following diagnostic screen.	Evaluate the following field.	What value do I want to see?
Page 4–Statuses and Network Parameters **Important:** If all of these values are 0 and macroblocking still exists, call Cisco Services.	MPEG STATS PEI PER SER RST A/V Disc	**0**—desired value **Note:** If all of these values are 0 and macroblocking still exists, check the QAM and the quality of feed coming out of the QAM.
Page 5–RF Status	CURRENT QAM Freq	**Tuner**—should be tuned to correct QAM **Status**—locked (desired value) **Note:** If the status is not "locked," check the QAM and the RF signal levels.
	CURRENT QAM S/N	**QAM-64**—28 dBmV to 34 dBmV desired range (minimum 25 dBmV) **QAM-256**—32 dBmV to 34 dBmV desired range (minimum 39 dBmV) **Note:** If the S/N value is not within the desired range, check the QAM and the RF signal levels.
	CURRENT QAM Corr Bytes and Uncor Blks/Current FDC	**Corr Bytes** and **Uncor Blks should be static**—if the values are incrementing rapidly, the QAM could be sending bad blocks of data. Check the RF signal levels coming out of the QAM and the DHCT connection
	CURRENT FDC Current FDC	**FDC frequency**—should match the frequency on the QPSK **Note:** If the FDC frequency does not match that of the QPSK or is changing, check the RF signal levels and the signal quality coming out of the QPSK and the DHCT connection.

Cannot Tune to SDV Channels

Description

A subscriber cannot tune to an SDV channel.

Possible Causes

- The DHCT is not authorized for the SDV service.
- Verify the DHCT has initialized with the SDV server.
- The reverse path may be down.
- Verify that the mini-carousel is loaded.

Diagnosing the Issue

See the following table to diagnose why the subscriber cannot tune to an SDV channel.

Important: The page number for the SDV diagnostic screens may vary, depending on the set-top model.

Access the following diagnostic screen.	Evaluate the following field.	What value do I want to see?
Page 38–SDV Session Info	CLIENT Authorized	**Yes**—desired value **Note:** If **No** appears, contact your DNCS administrator to verify that the DHCT is authorized for the SDV package.
	SDV PROTOCOL STATISTICS InitConfRx	**1**—desired value **Note:** If value is **0**, reboot the set-top, and then tune to an SDV channel. If unable to tune to SDV channel, the reverse path may be down. Contact Cisco Services for assistance.
Page 39–SDV Mini Carousel	Status	**CacheReady**—desired value

Loss of Two-Way Connectivity

Description

Subscribers are unable to use the DHCT in an interactive mode.

Possible Causes

- The SDV server may be down.

  Note: If the loss of connectivity only affects SDV channels, the SDV server may be down. See ***Cannot Tune to SDV Channels*** (on page 81) for troubleshooting information.

- The DHCT is not receiving UNcfg (User to Network Configuration) messages from the DNCS.
- RF levels may not be set correctly.
- The QPSK has a modulator/demodulator configuration issue.

Diagnosing the Issue

See the following table to diagnose why the DHCT may not be in two-way mode.

Access the following diagnostic screen.	Evaluate the following field.	What value do I want to see?
Page 2–Post and Boot Results	UNcfg	**READY**—desired value; DHCT is in two-way mode **B'cast only**—check the DNCS configuration and RF levels **SEARCHING**—not receiving UNcfg message. Check the RF signal levels. If the signal levels are within range and you still have an issue, call Cisco Services
Page 4–Statuses and Network Parameters	IP Address (in RF Network section)	**IP Address**—DHCT successfully booted in two-way mode **Note:** If **No IP Address** appears, the DHCT did not boot in two-way mode. Contact your DNCS administrator to verify that the DHCT is enabled for two-way communication.

Access the following diagnostic screen.	Evaluate the following field.	What value do I want to see?
Page 5–RF Status	CURRENT FDC/DAVIC	**Connected—**desired value; DHCT is in two-way mode **Note:** If **Ready B'cast Only** appears, the DHCT is in one-way mode. Contact your DNCS administrator to verify that the DHCT is enabled for two-way communication.
	CURRENT RDC/Freq	**Should match frequency of the demodulator at the headend**
	CURRENT RDC/Power	**Refer to specific hardware specifications** ■ If the value is displayed in white the signal level is nominal ■ If the value is displayed in amber the signal level is marginally too high or too low ■ If the value is displayed in red the signal level is unacceptably too high or too low

5

SDV Troubleshooting Flowcharts

Introduction

This chapter includes step-by-step flowcharts that help you to troubleshoot the following four issues that can occur in an SDV system.

These flow charts do not include all of the possible scenarios that could be used to correct an issue; however, they do include the most common methods for correcting an issue.

Important:

- Some flowcharts include suggestions to access SARA-related diagnostic screens specific to SDV. For information about these screens, go to ***Accessing SDV Diagnostic Screens*** (on page 61).
- Some flowcharts include suggestions to access SARA-related diagnostic screens for RF and MPEG information, as well as for various network issues. These diagnostic screens are not included in this guide. For further information, refer to *Understanding Diagnostic Screens for the Explorer Digital Home Communications Terminals Application Guide* (part number 749244).

In This Chapter

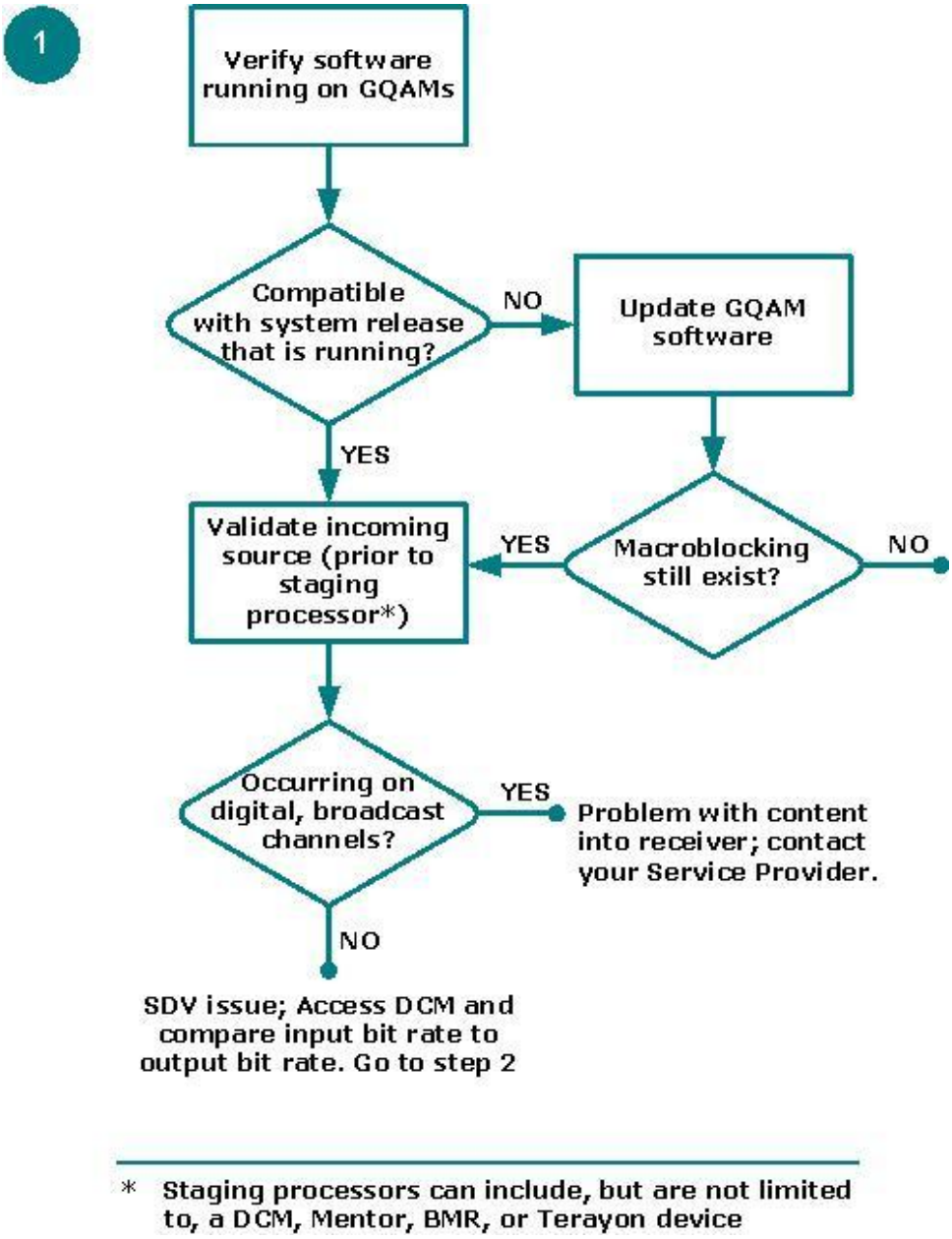
Macroblocking on an SDV Channel

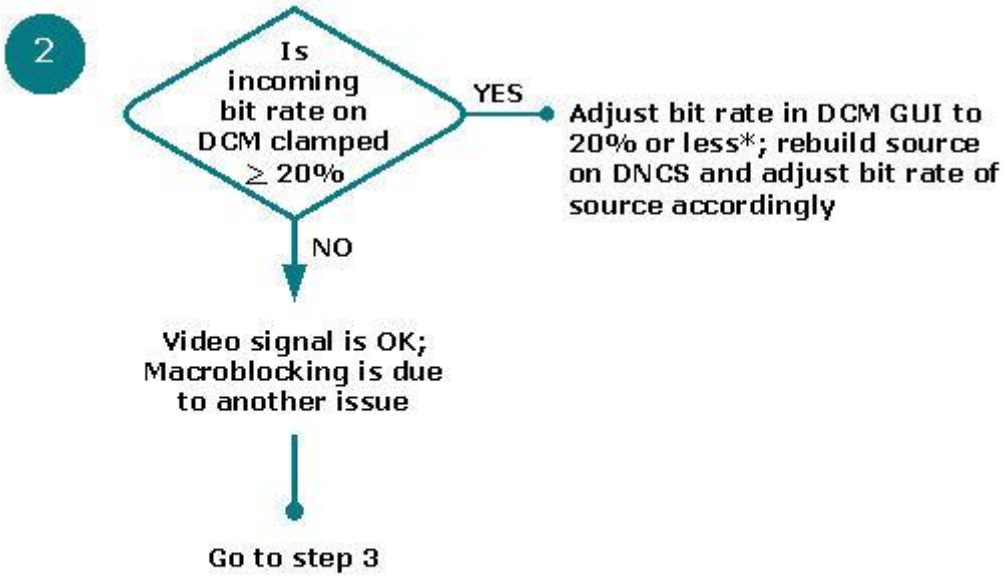
When a subscriber tunes to an SDV channel, a video issue or macroblocking occurs and may result in tiling, blocking, or channel freezing. This issue may occur on a single channel, as well as on multiple channels. To view the sequence of flowcharts for Macroblocking, go to one of the following sections:

- ***Macroblocking: Single Channel*** (on page 87)
- ***Macroblocking: Multiple Channels*** (on page 91)

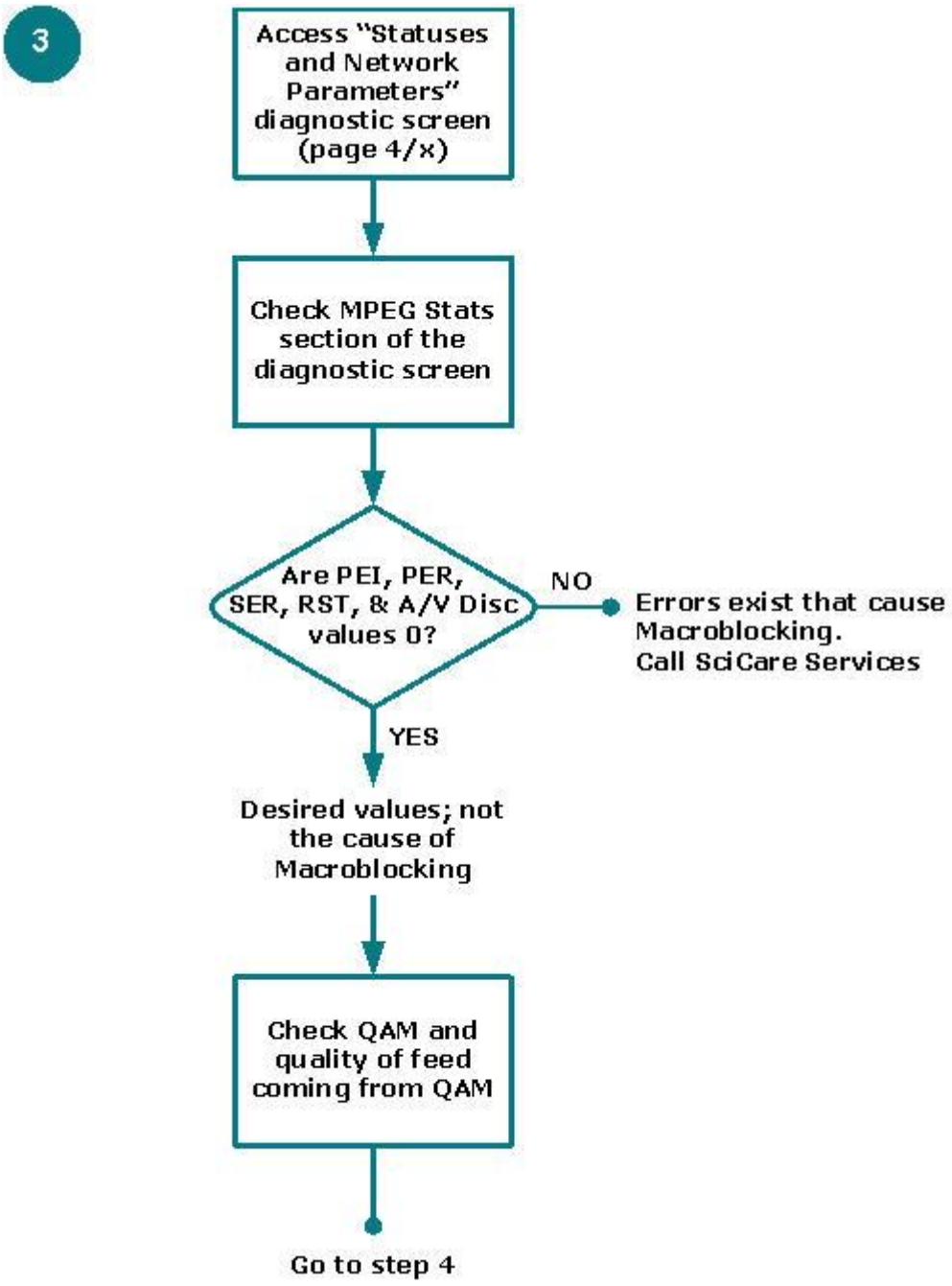
Macroblocking: Single Channel

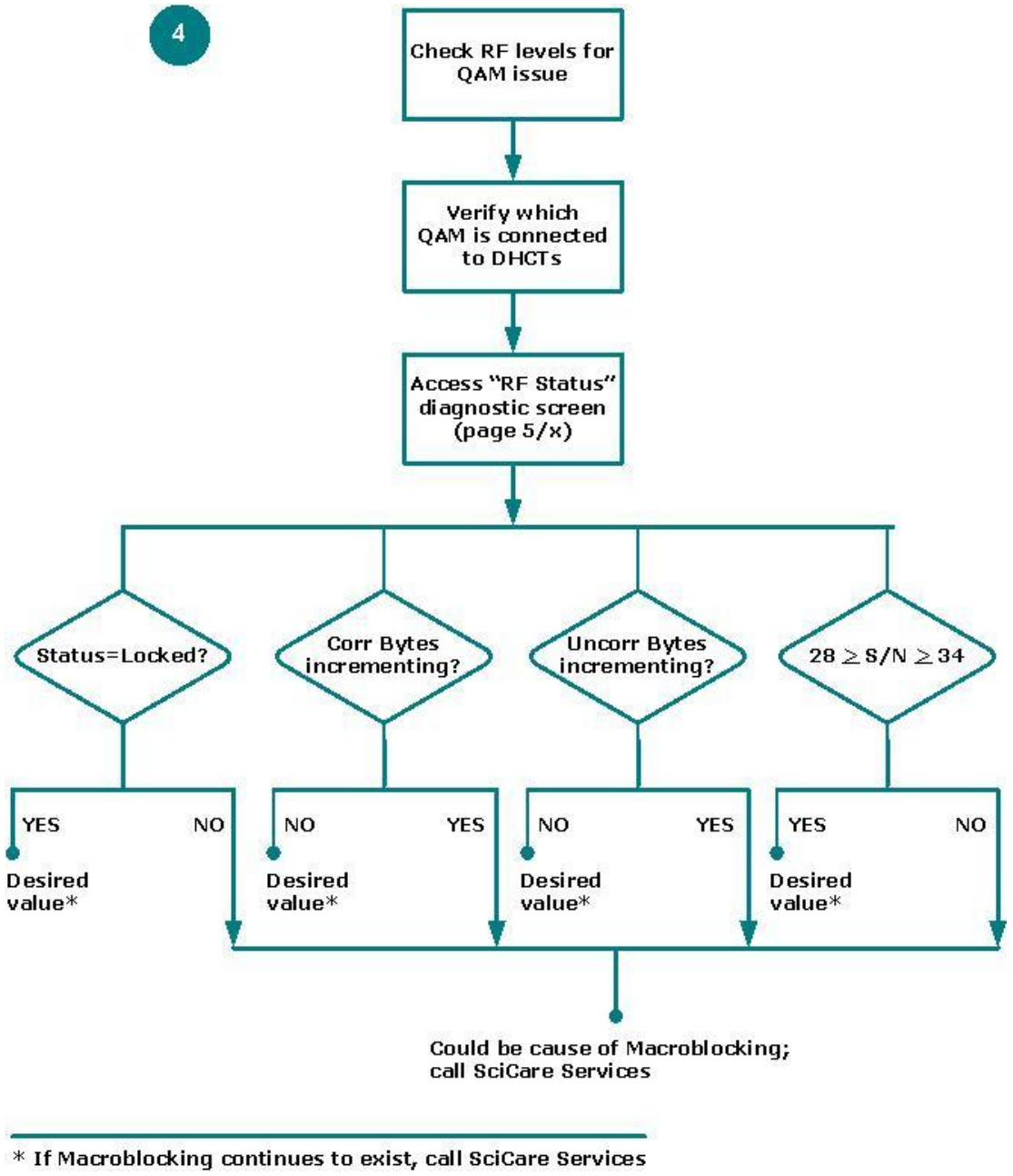
Each flowchart within this sequence is a possible cause for Macroblocking on a single SDV channel. Each individual flowchart provides steps to determine whether or not a possible cause is, in fact, causing this issue.





* From a DCM prospective, setting the bit rate to 20% or less serves only as a guideline.


3
Access "Statuses and Network Parameters" diagnostic screen (page 4/x)
Check MPEG Stats section of the diagnostic screen
Are PEI, PER, SER, RST, & A/V Disc values 0?
NO
Errors exist that cause Macroblocking. Call SciCare Services
YES
Desired values; not the cause of Macroblocking
Check QAM and quality of feed coming from QAM
Go to step 4

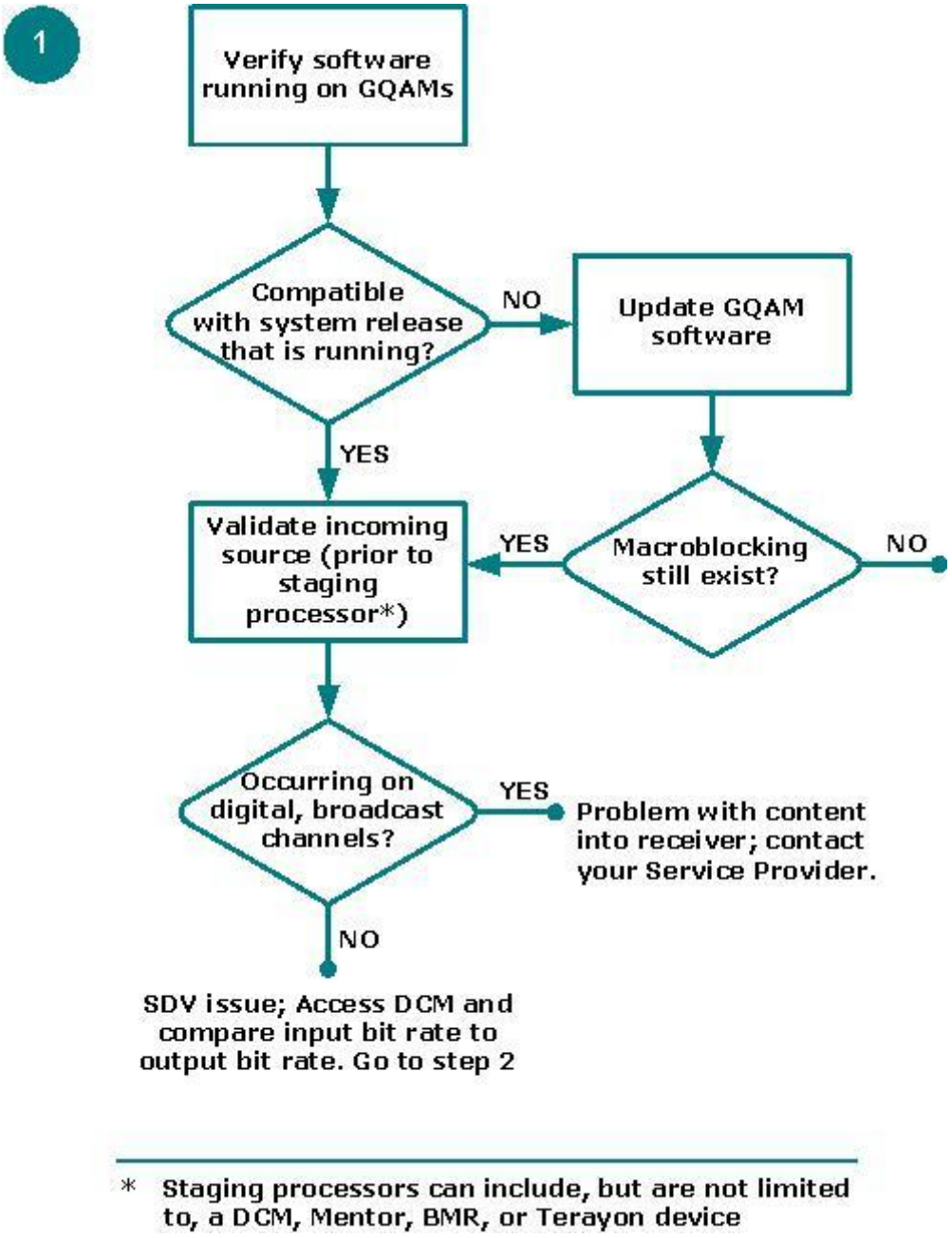


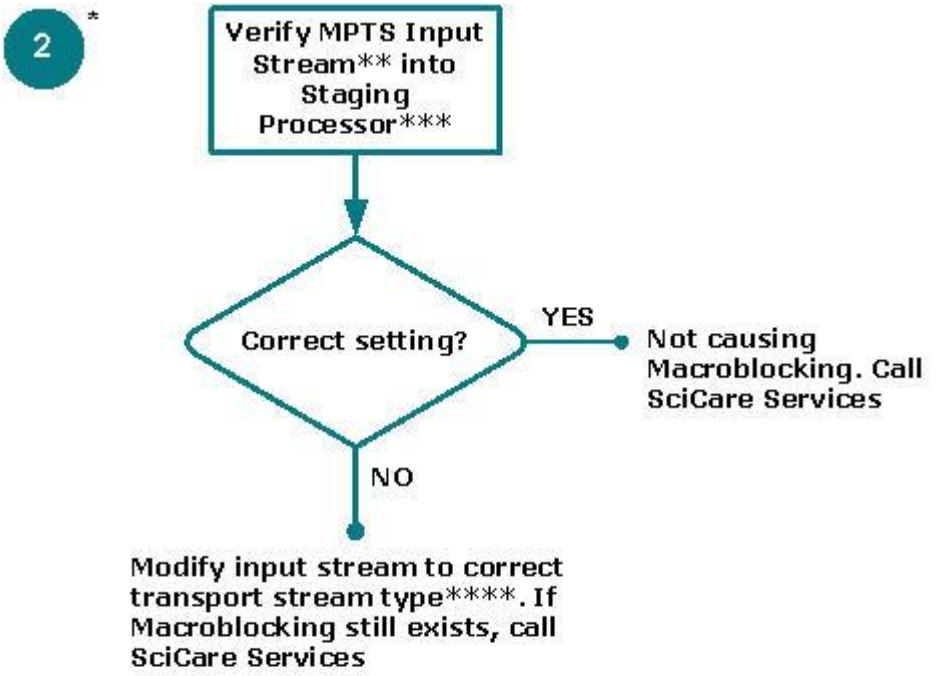
* If Macroblocking continues to exist, call SciCare Services

Macroblocking: Multiple Channels

Each flowchart within this sequence is a possible cause for Macroblocking on multiple SDV channels. Each individual flowchart provides steps to determine whether or not a possible cause is, in fact, causing this issue.

Important: Before you begin troubleshooting issues directly related to SDV, please validate the software version running an all GQAMs in your system. This software version should be compatible to the system release software that you are running.





* This issue could be "Start Over" related.

** The MTPS input stream is the stream prior to being placed in a Transrating Group.

*** Staging processors can include, but are not limited to, a DCM, Mentor, BMR, or Terayon device.

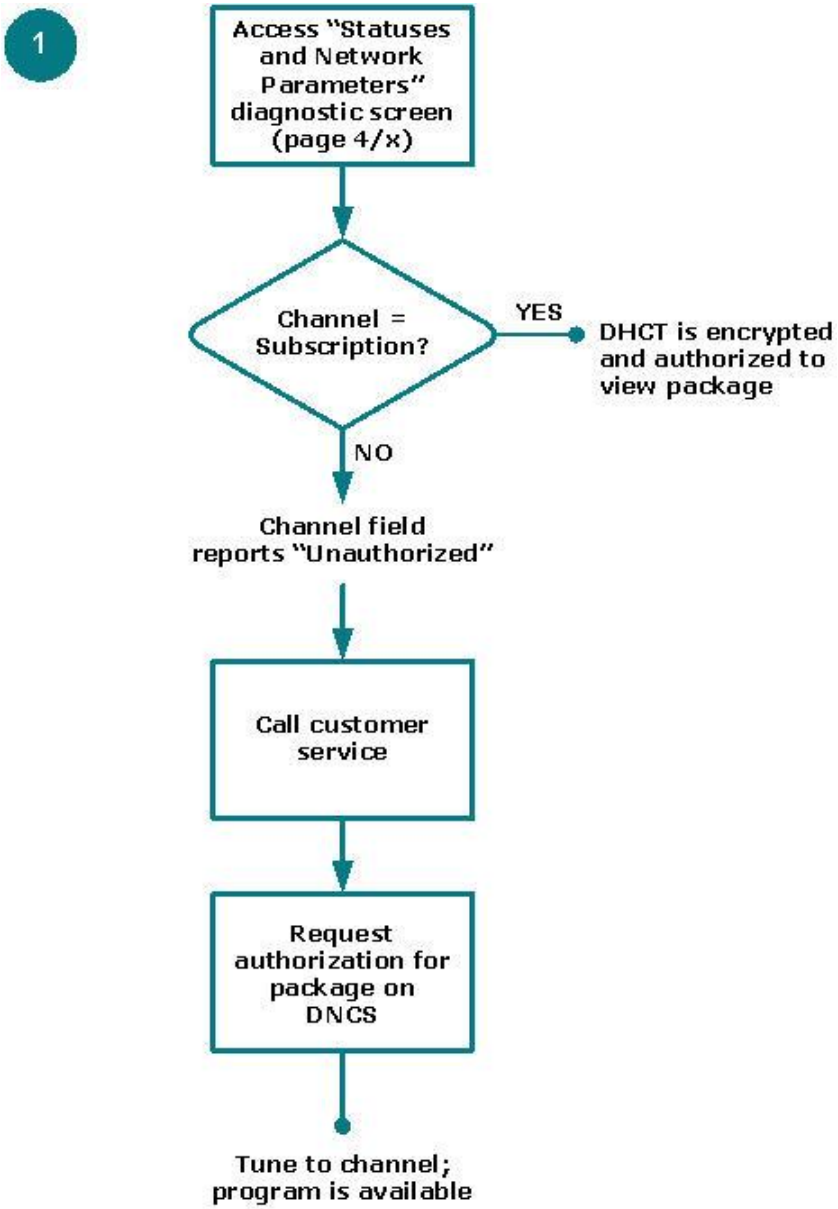
**** Transport stream types include DC-II, ATSC, or DVB.

SDV Channel is Not Authorized for SDV Services

When subscriber tunes to an SDV channel, a "Channel Not Authorized" barker appears. When this occurs, it is *not* an SDV-related issue; it is an encryption issue in which the set-top box is not authorized for the channel or source.

Note: Encrypted sources are typically assigned via a package. In this case, the set-top must be authorized for the package to view the encrypted source.

To authorize the channel, refer to the following flowchart.



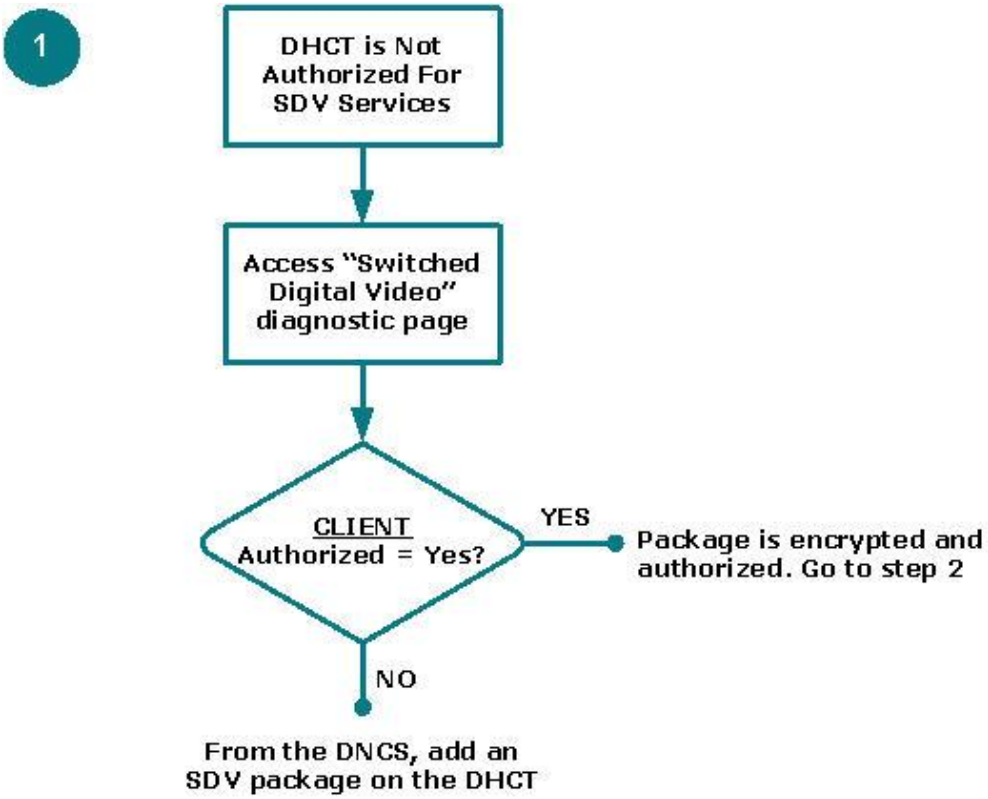
SDV Channel is Not Available

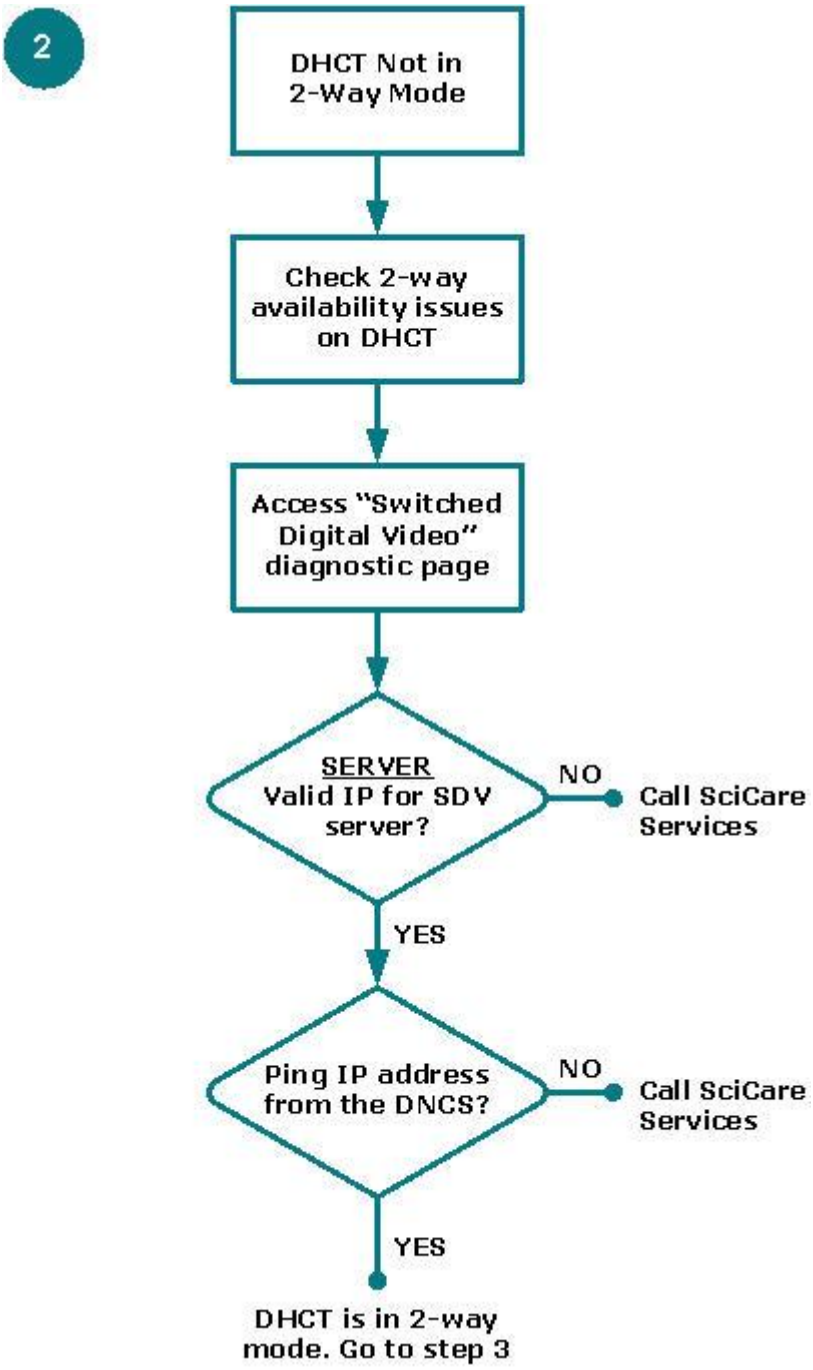
When subscriber tunes to an SDV channel, a “Channel Not Available" barker appears on either a single SDV channel or on multiple SDV channels. To view the sequence of flowcharts for this issue, go to one of the following sections:

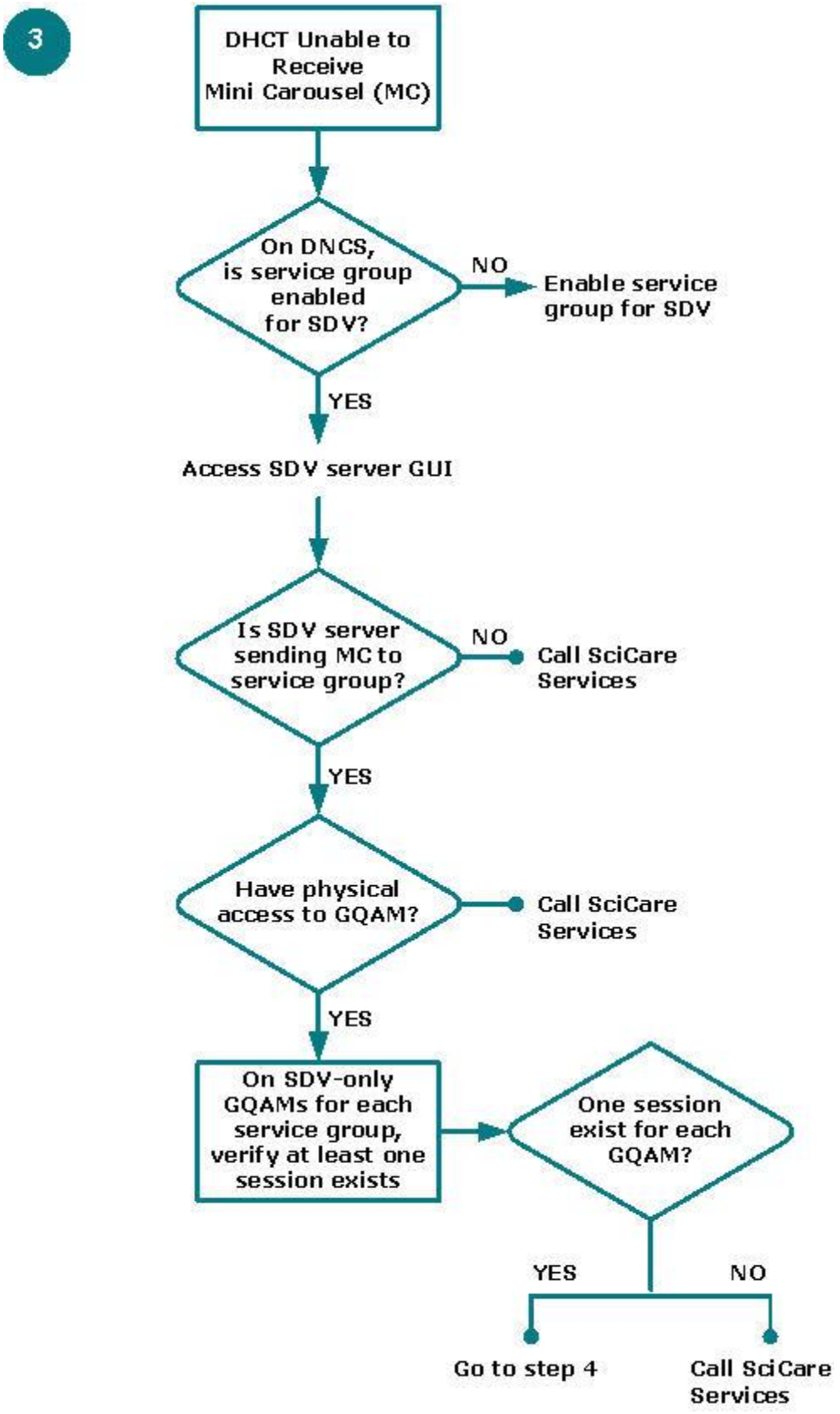
- *SDV Channel Not Available: Single Channel* (on page 94)
- *SDV Channel Not Available: Multiple Channels* (on page 101)

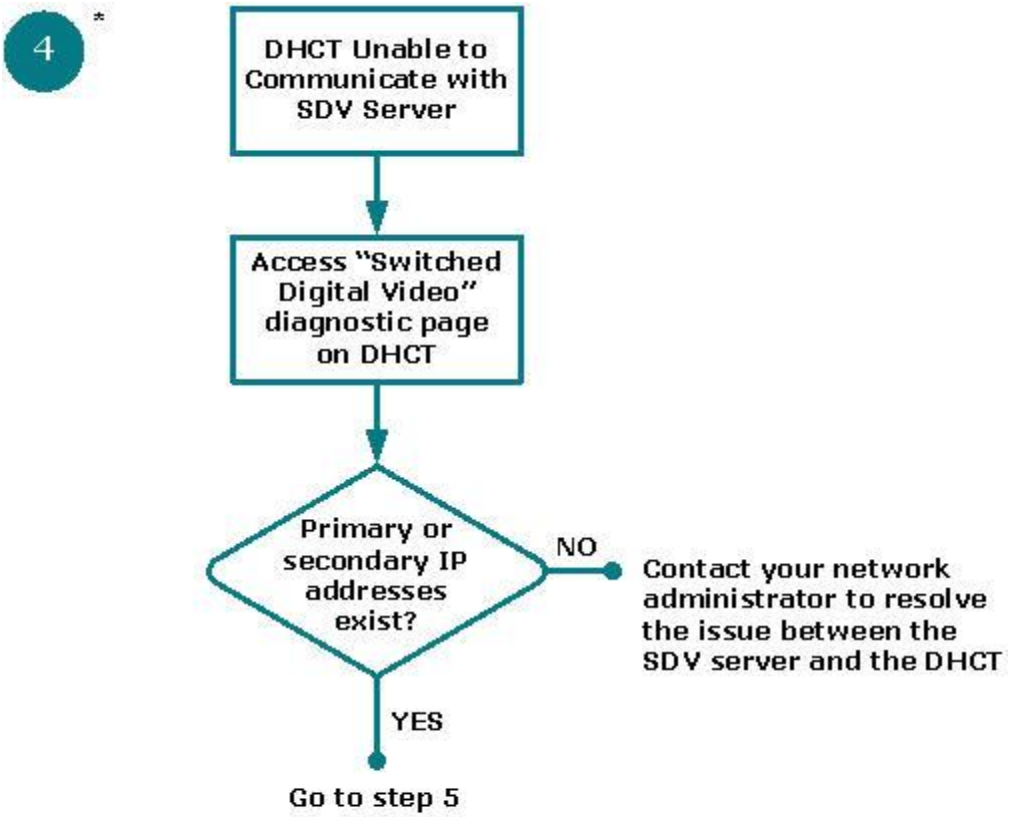
SDV Channel Not Available: Single Channel

Each flowchart within this sequence is a possible cause for the Channel Not Available issue to occur on a single SDV channel. Each individual flowchart provides steps to determine whether or not a possible cause is, in fact, causing this issue.

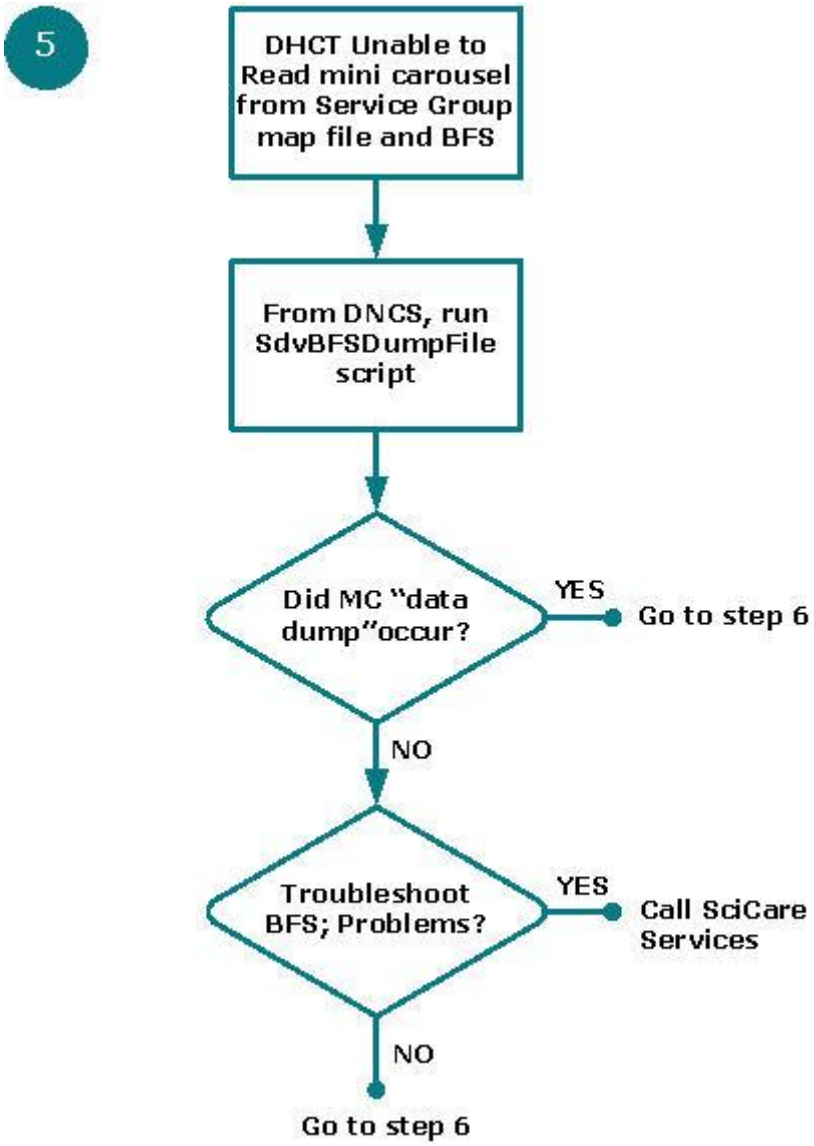


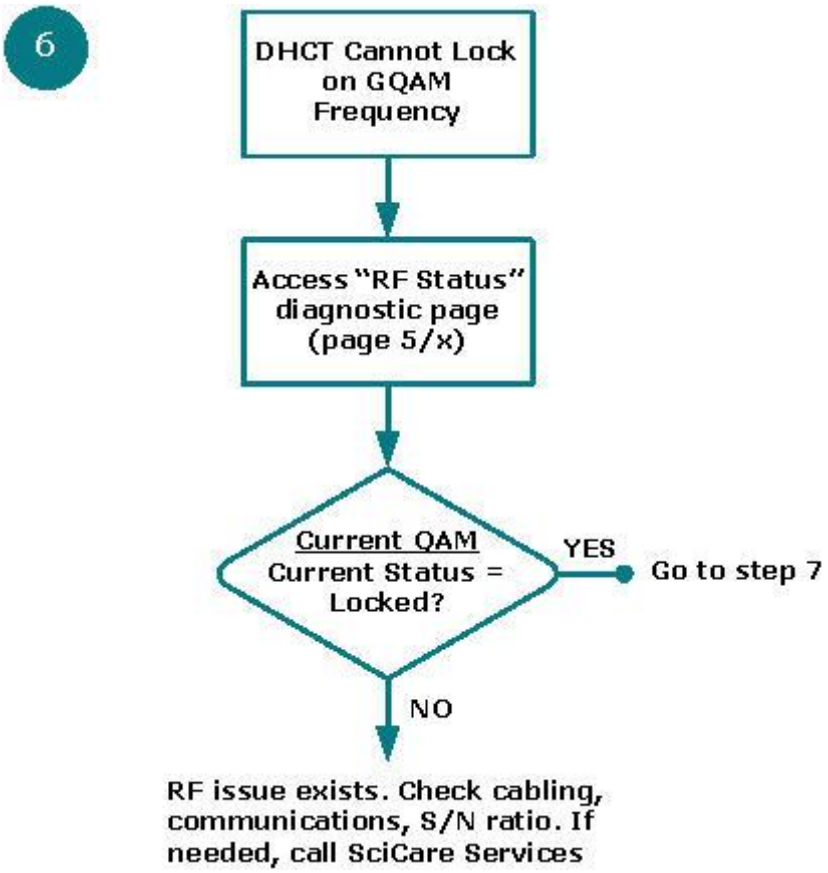

2
DHCT Not in 2-Way Mode
Check 2-way availability issues on DHCT
Access "Switched Digital Video" diagnostic page
SERVER Valid IP for SDV server?
NO
Call SciCare Services
YES
Ping IP address from the DNCS?
NO
Call SciCare Services
YES
DHCT is in 2-way mode. Go to step 3

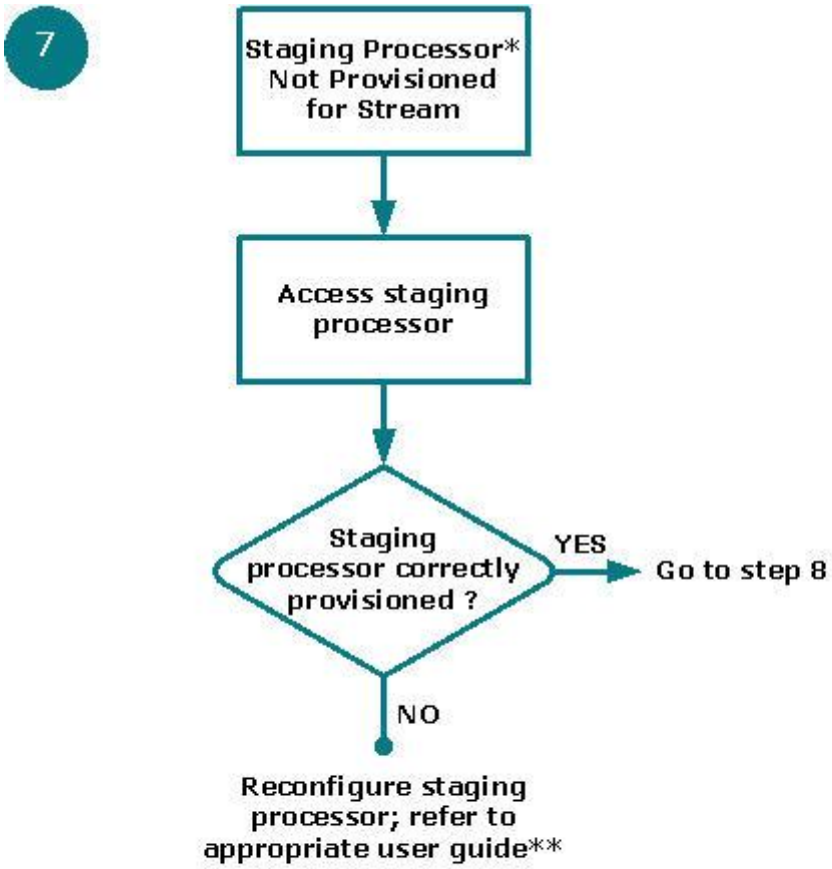

3
DHCT Unable to Receive Mini Carousel (MC)
On DNCS, is service group enabled for SDV?
NO
Enable service group for SDV
YES
Access SDV server GUI
Is SDV server sending MC to service group?
NO
Call SciCare Services
YES
Have physical access to GQAM?
Call SciCare Services
YES
On SDV-only GQAMs for each service group, verify at least one session exists
One session exist for each GQAM?
YES
NO
Go to step 4
Call SciCare Services



* The UDP protocol is used for communication between the set-top and the SDV Server on port 23000.

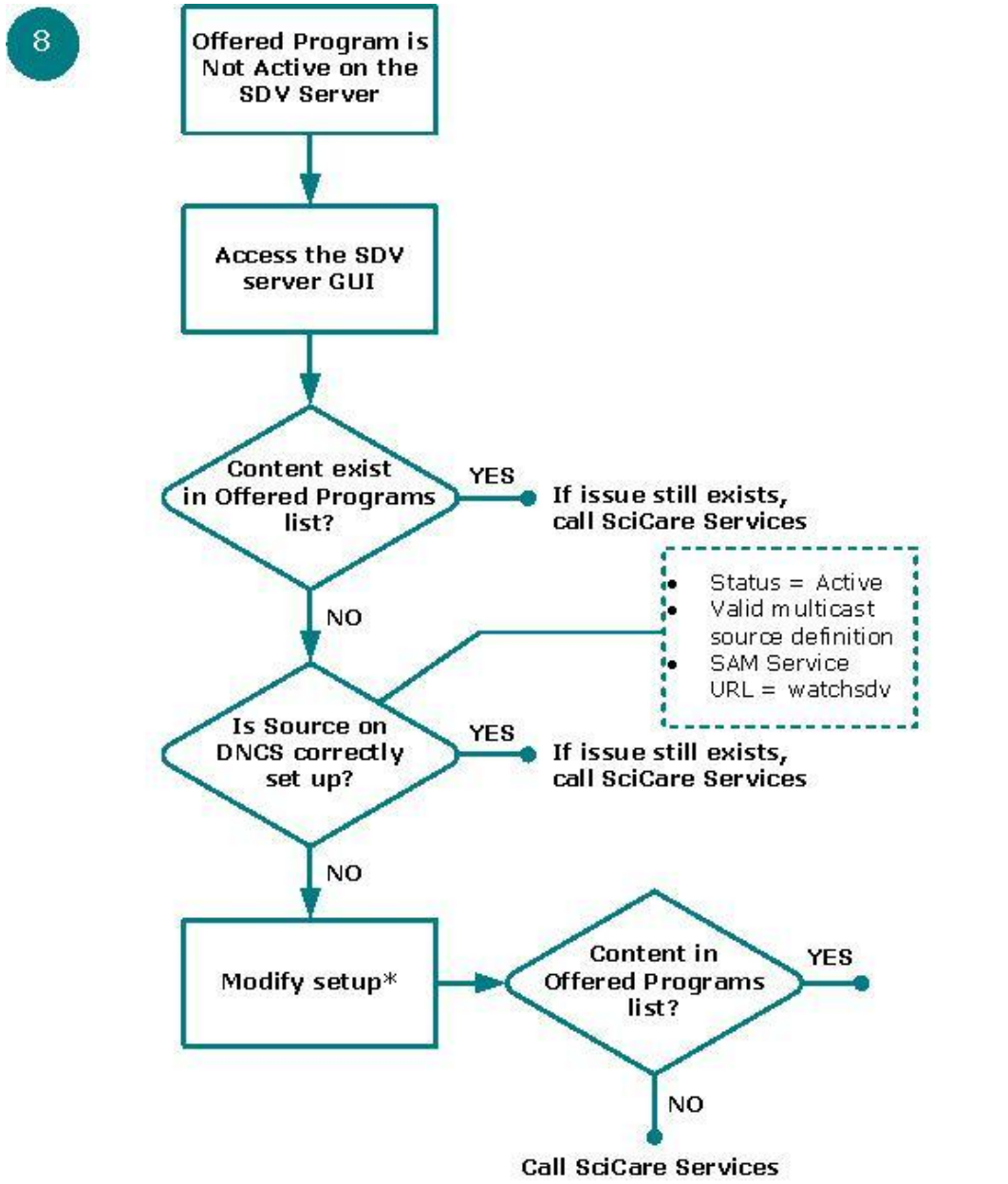

5
DHCT Unable to Read mini carousel from Service Group map file and BFS
From DNCS, run SdvBFSDumpFile script
Did MC "data dump"occur?
YES
Go to step 6
NO
Troubleshoot BFS; Problems?
YES
Call SciCare Services
NO
Go to step 6


6
DHCT Cannot Lock on GQAM Frequency
Access "RF Status" diagnostic page (page 5/x)
Current QAM Current Status = Locked?
YES
Go to step 7
NO
RF issue exists. Check cabling, communications, S/N ratio. If needed, call SciCare Services



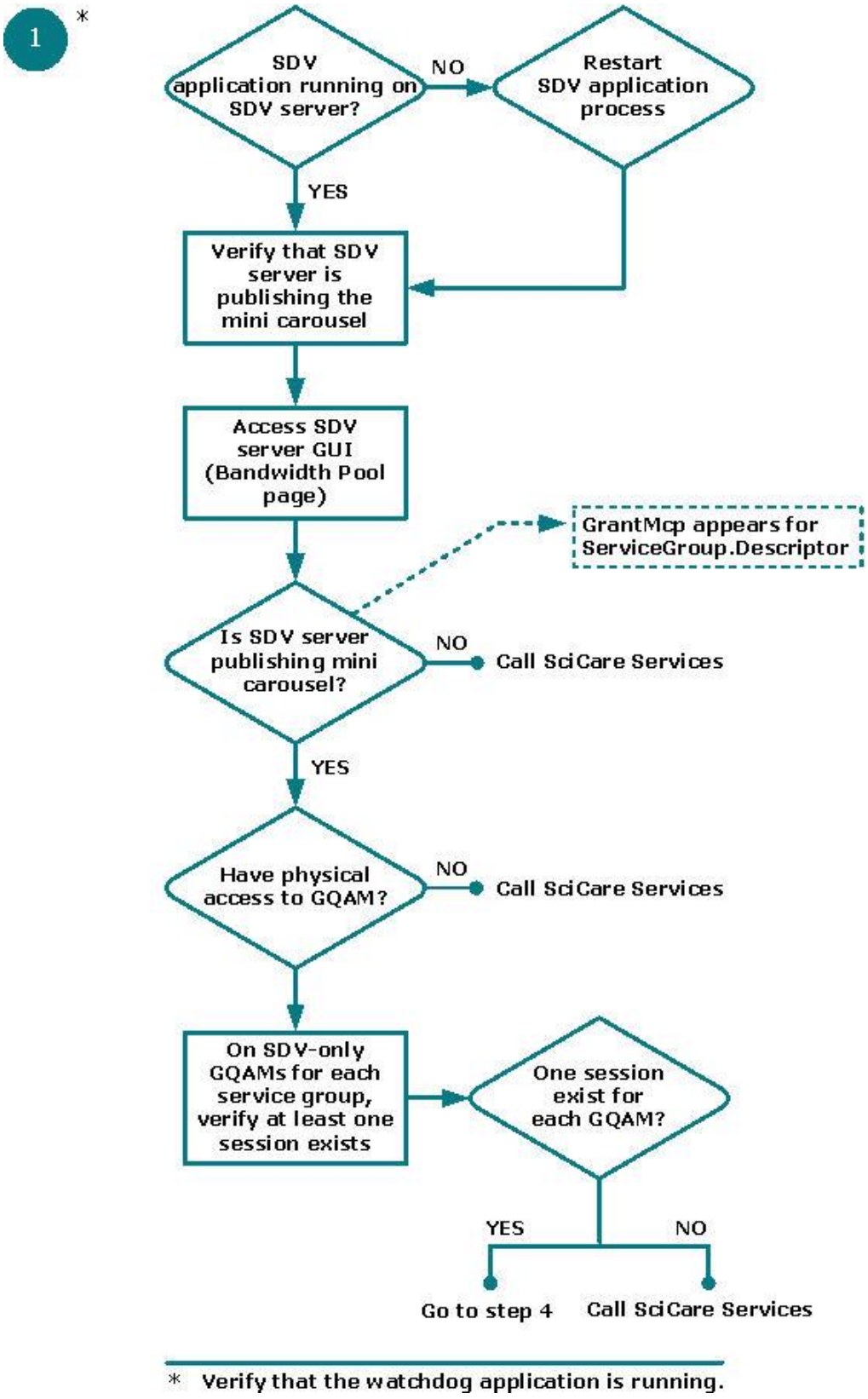
* Staging processors can include, but are not limited to, a DCM, Mentor, BMR, or Terayon device

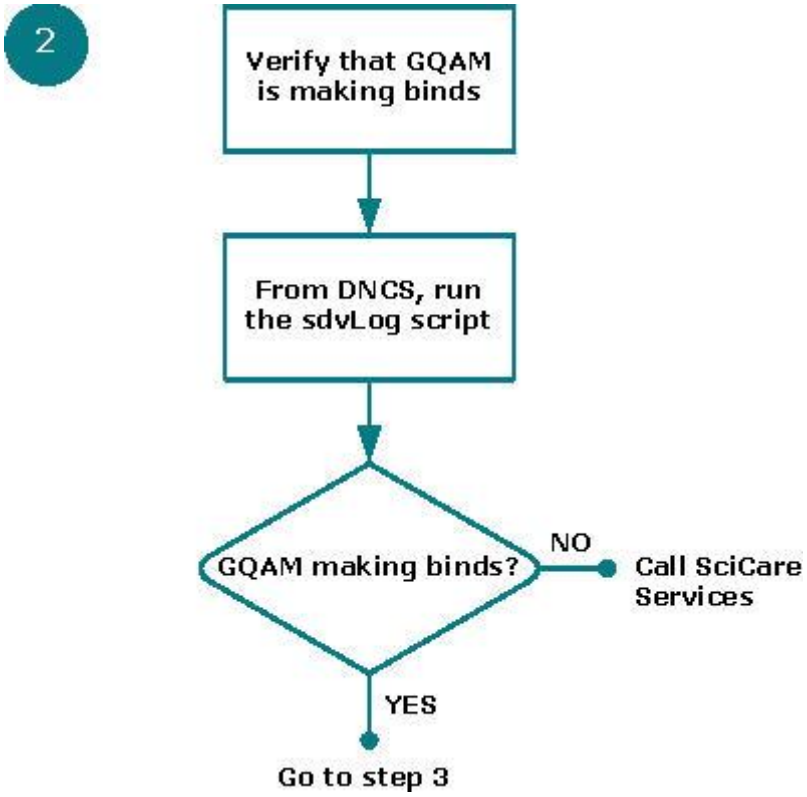
** If you are using a DCM, refer to the *DCM User's Guide*.

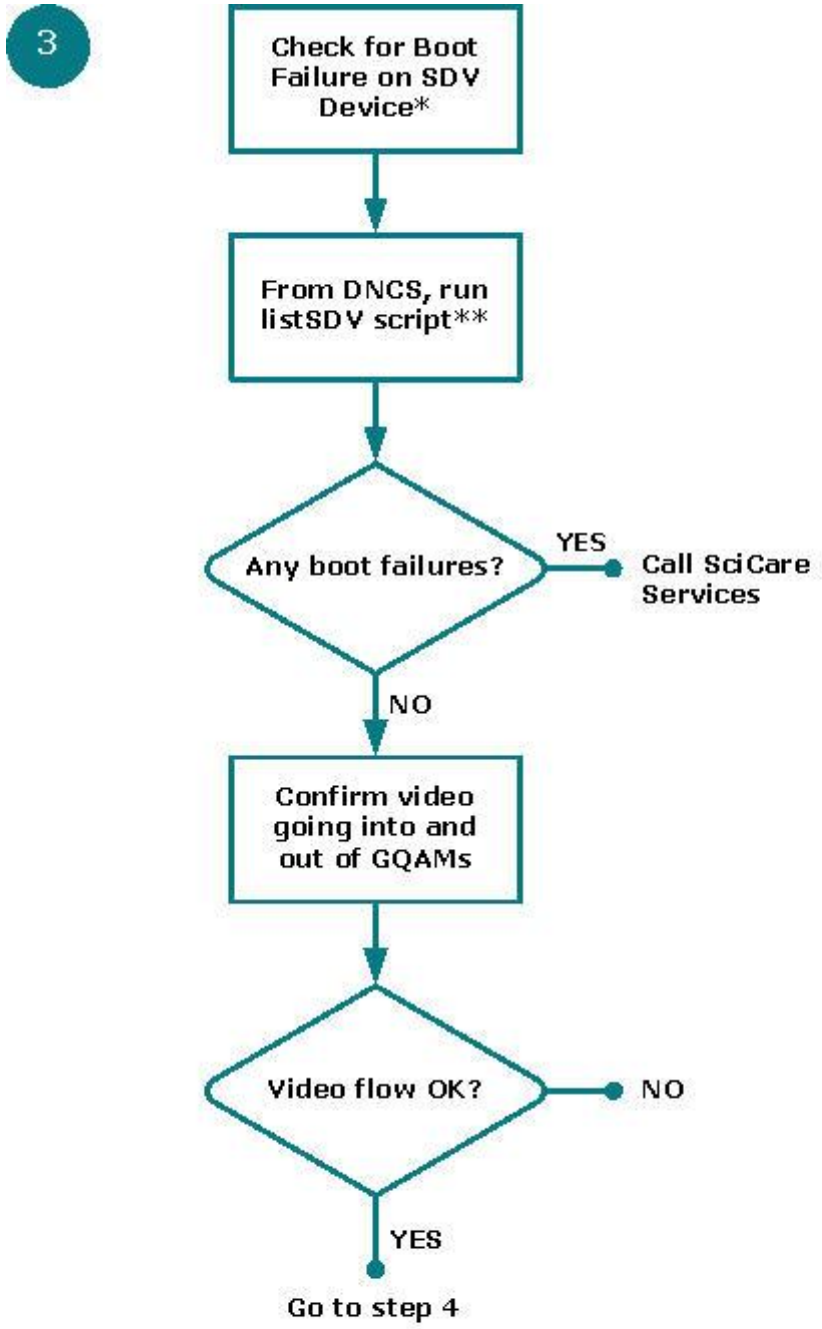


SDV Channel Not Available: Multiple Channels

Each flowchart within this sequence is a possible cause for the Channel Not Available issue to occur on multiple SDV channels. Each individual flowchart provides steps to determine whether or not a possible cause is causing this issue.

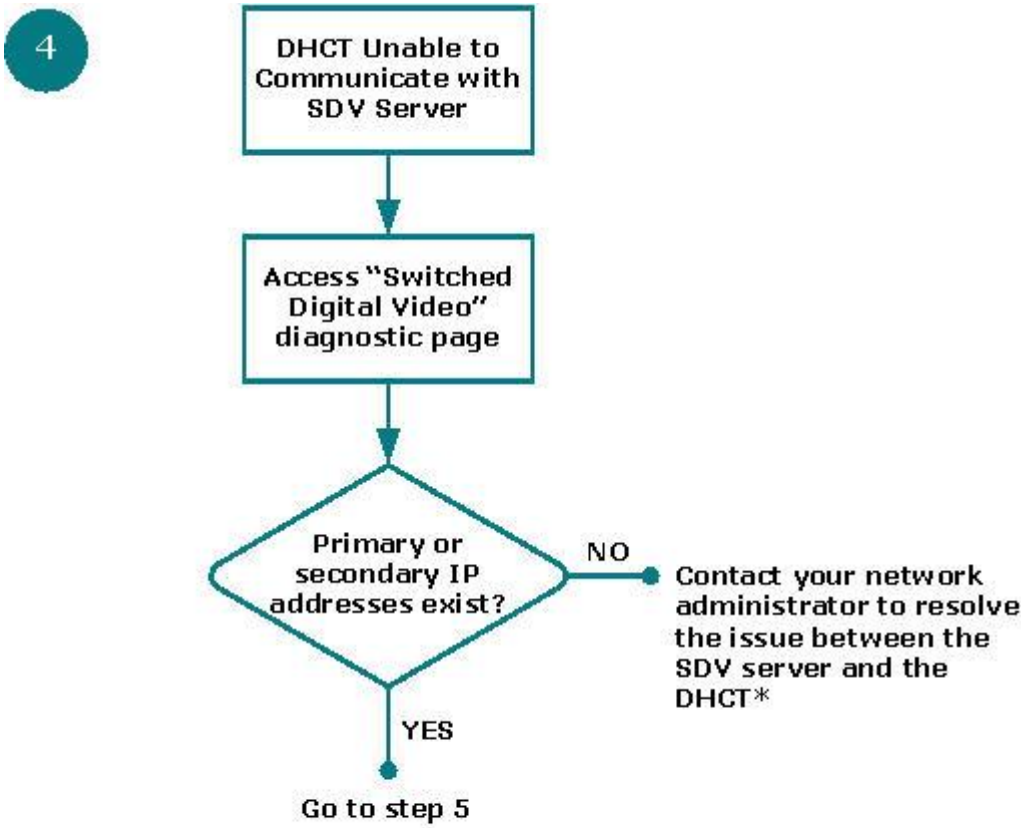

1 *
SDV application running on SDV server?
NO
Restart SDV application process
YES
Verify that SDV server is publishing the mini carousel
Access SDV server GUI (Bandwidth Pool page)
GrantMcp appears for ServiceGroup.Descriptor
Is SDV server publishing mini carousel?
NO
Call SciCare Services
YES
Have physical access to GQAM?
NO
Call SciCare Services
On SDV-only GQAMs for each service group, verify at least one session exists
One session exist for each GQAM?
YES
NO
Go to step 4
Call SciCare Services
* Verify that the watchdog application is running.


2
Verify that GQAM is making binds
From DNCS, run the sdvLog script
GQAM making binds?
NO
Call SciCare Services
YES
Go to step 3



* SDV devices include, but are not limited to, SDV servers, GQAMs, Netcrypt Bulk Encryptors, and staging processors.

** Use these utilities to verify the operational status of each SDV device.



* The UDP protocol is used for communication between the set-top and the SDV Server on port 23000.

* Could be as designed; please call SciCare Services

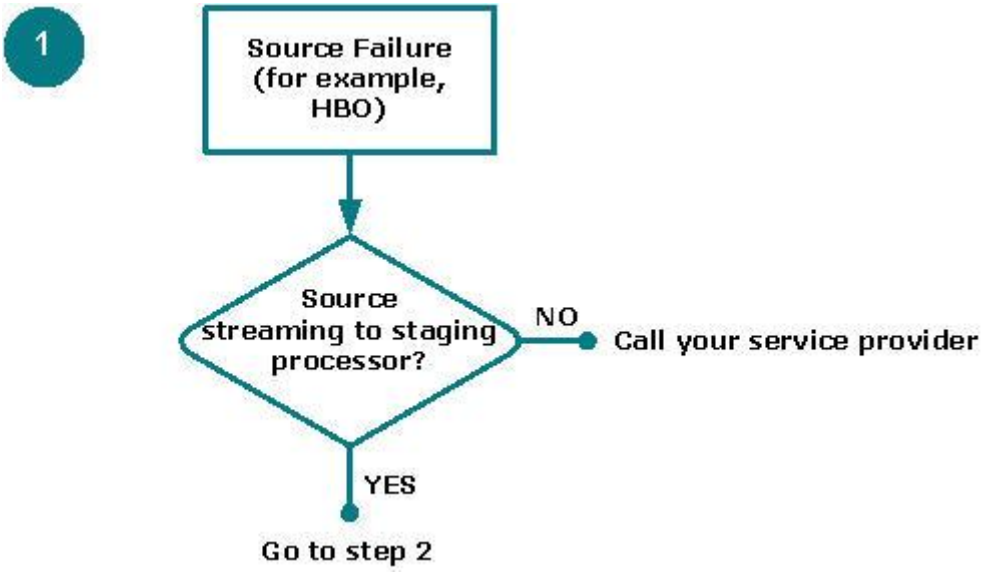
Black or Gray Screen Issue

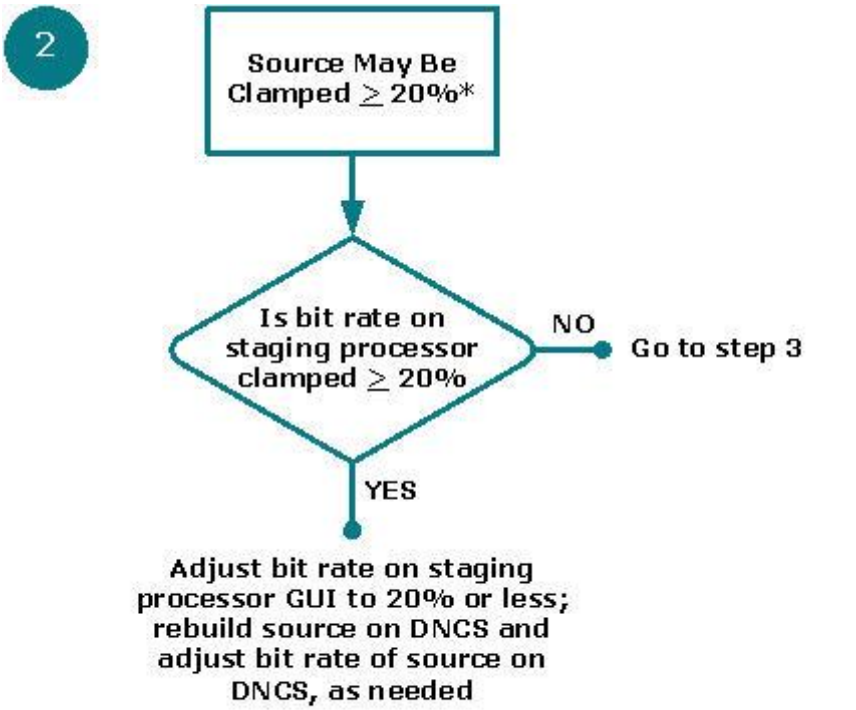
When subscriber tunes to an SDV channel, a black or gray screen appears on either a single SDV channel or on multiple SDV channels. To view the sequence of flowcharts for this issue, go to one of the following sections:

- ***Black or Gray Screen: Single Channel*** (on page 106)
- ***Black or Gray Screen: Multiple Channels*** (on page 110)

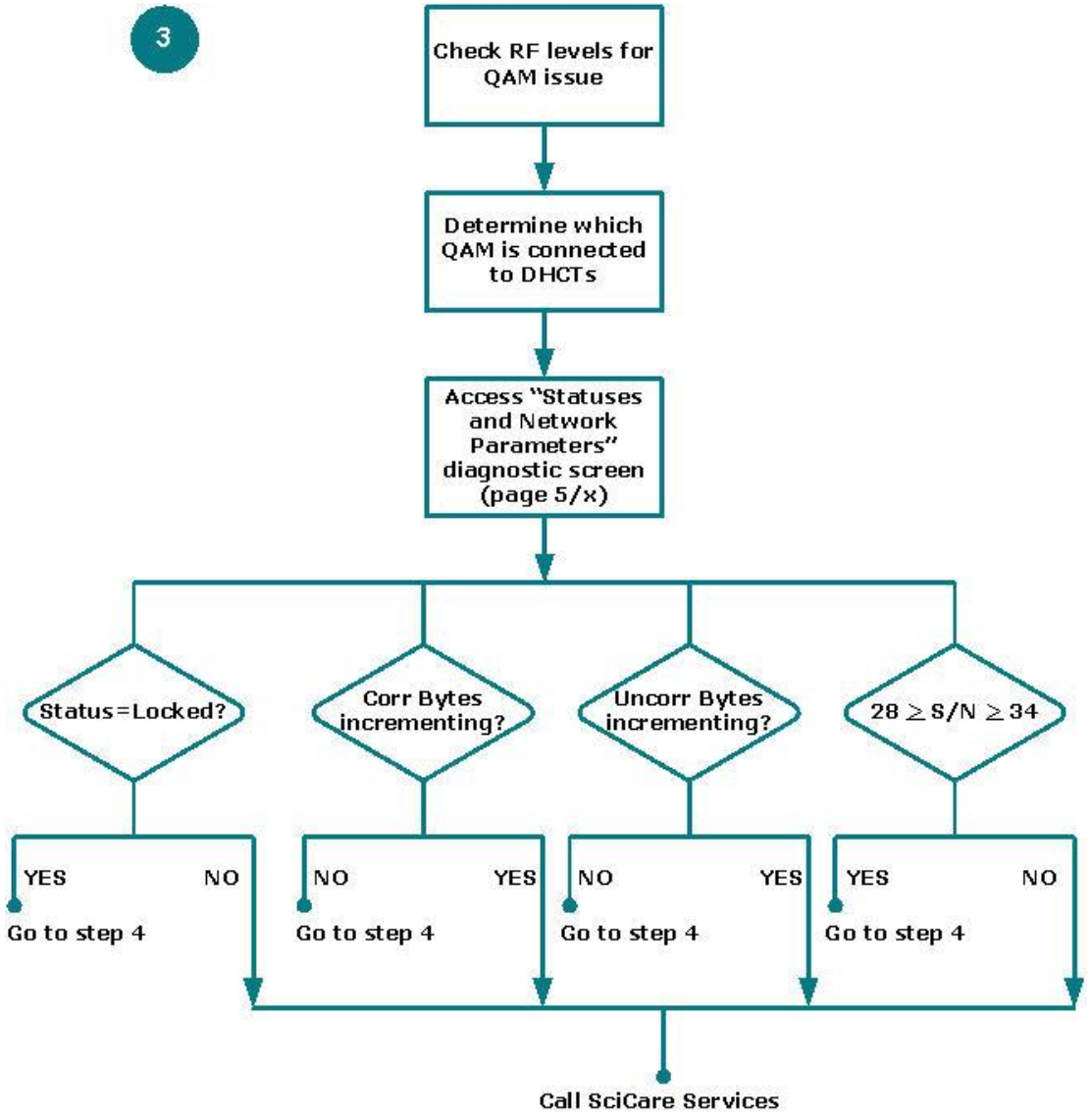
Black or Gray Screen: Single Channel

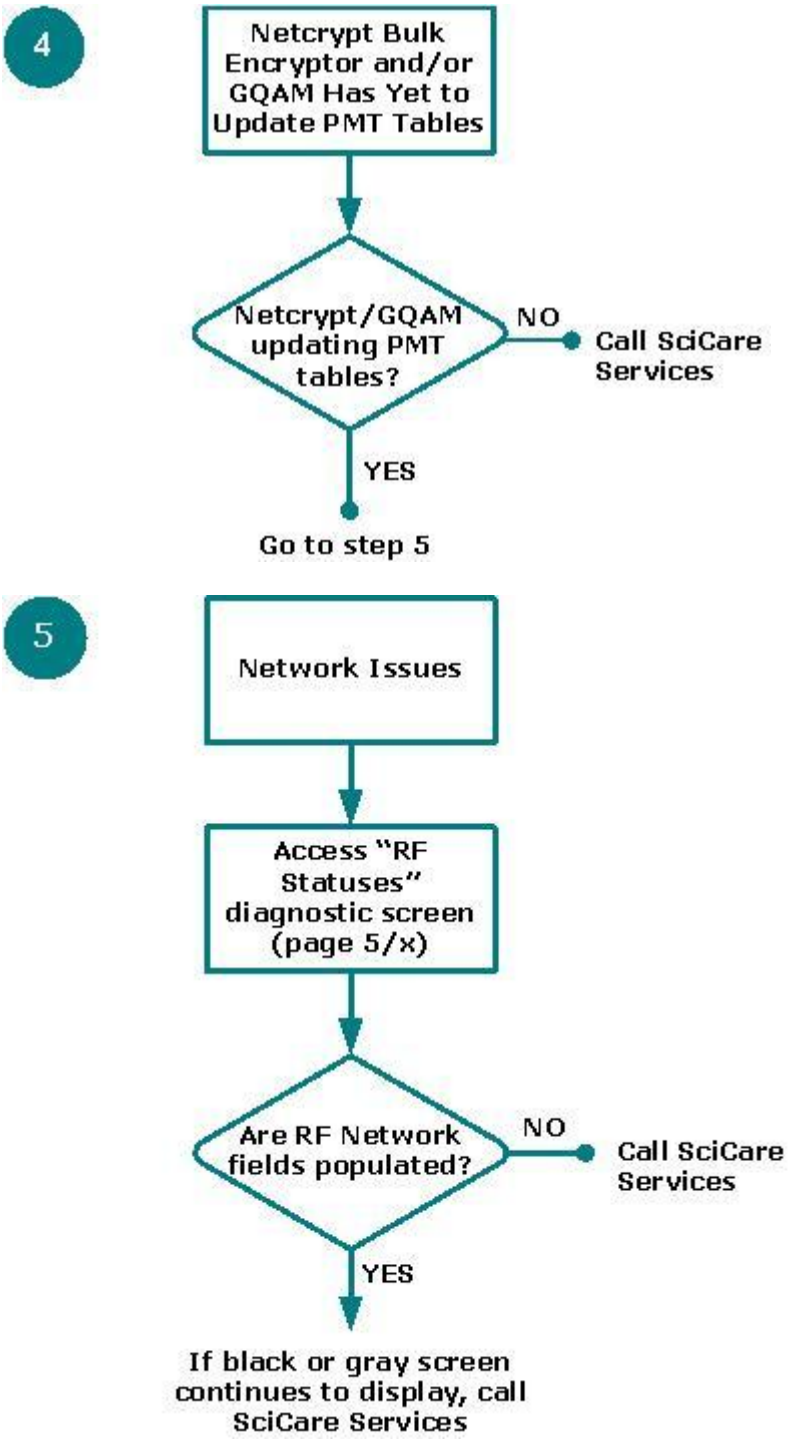
Each flowchart within this sequence is a possible cause for a black or gray screen to appear on a single SDV channel. Each individual flowchart provides steps to determine whether or not a possible cause is, in fact, causing this issue.





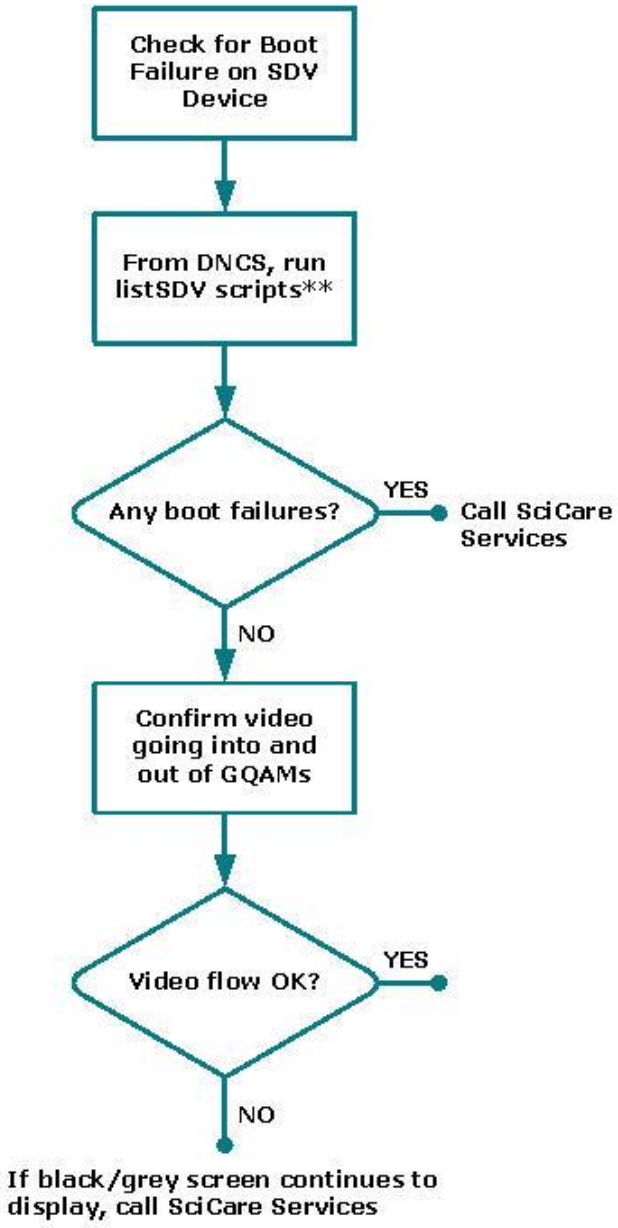
* From a DCM prospective, setting the bit rate to 20% or less serves only as a guideline.


3
Check RF levels for QAM issue
Determine which QAM is connected to DHCTs
Access "Statuses and Network Parameters" diagnostic screen (page 5/x)
Status=Locked?
Corr Bytes incrementing?
Uncorr Bytes incrementing?
28 ≥ S/N ≥ 34
YES
NO
Go to step 4
NO
YES
Go to step 4
NO
YES
Go to step 4
YES
NO
Go to step 4
Call SciCare Services


4
Netcrypt Bulk Encryptor and/or GQAM Has Yet to Update PMT Tables
Netcrypt/GQAM updating PMT tables?
NO
Call SciCare Services
YES
Go to step 5
5
Network Issues
Access "RF Statuses" diagnostic screen (page 5/x)
Are RF Network fields populated?
NO
Call SciCare Services
YES
If black or gray screen continues to display, call SciCare Services

Black or Gray Screen: Multiple Channels

Each flowchart within this sequence is a possible cause for a black or gray screen to appear on multiple SDV channels. Each individual flowchart provides steps to determine whether or not a possible cause is, in fact, causing this issue.



* SDV devices include, but are not limited to, SDV servers, GQAMs, Netcrypt Bulk Encryptors, and staging processors.

* Use these scripts to verify the operational status of each SDV device.

6

Customer Information

If You Have Questions

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

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

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

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

May 2012 Printed in USA

Part Number 4022446 Rev B