Cisco Series D9510 USRM Release 2.1.3 Release Note

Overview

Introduction

The Cisco Series D9510 Universal Session and Resource Manager (USRM) release 2.1.3 succeeds and carries forward all of the enhancements and features of prior USRM releases (2.1.2, 2.1.1, 2.1.0, 2.0.1, 1.7.3, 1.7.2, and 1.7.1).

Purpose

This release note is being provided for user support related to the installation and operation of USRM System Release 2.1.3.

Qualified Personnel

Only appropriately qualified and skilled service personnel should attempt to install, operate, maintain, and service this product.

WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

In This Document

General Information

Additional Features

Release 2.1.3 provides the following new features:

- **Full SDV and VOD support.** USRM Release 2.1.3 has full support for all SDV and VOD functionality. Service Group alignment is required for proper operation.
- **Centralized VSM with integrated and/or remote ERM support.** USRM 2.1.3 introduces the concept of a centralized VOD Session Manager (VSM) for use in systems that require a single interface to the VOD back office. This centralized VSM receives all VOD requests from all clients in the network. The Edge Resource Manager (ERM) can be either integrated with the VSM or remotely located (as in the case of existing USRMs deployed for SDV operations).
- **Remote ERM.** In USRM 2.1.3, an existing USRM in use as a Session Manager and ERM for SDV can also be used as an ERM for VOD Edge devices in the same service groups. Applicable Edge devices include QAMs, Netcrypts, and CA Managers (e.g., RCAS or DNCS).
- **Discovery Services.** In USRM 2.1.3, a new interface has been provided to communicate with remote ERMs. Session Manager applications such as VodSm can use this interface to send Resource allocation requests, which are then multicast to all ERMs.
- **Policy.** The simple video policy server existed in prior versions of USRM 2.x. It has been extensively tested for this release. It is also enhanced in this version with a new configuration setting in which the mode is explicitly configured. The available modes are ChannelBased, GuaranteeAll, and GuaranteeHighPri. See ***Appendix B: Policy*** (on page 16) for details.
- **Spreadsheet import.** USRM 2.1.3 provides the ability to import and export ERM resources (QAMs) and SDV offered programs in a csv (Microsoft Excel spreadsheet) file format. See ***Appendix C: Spreadsheet Import and Export*** (on page 18) for details.
- **GQIv2 PowerKEY QAM support.** USRM 2.1.3 has been enhanced with GQIv2 PowerKEY QAM support for Cisco RFGW-1 PowerKEY QAMs.
- **GQIv1.5 support for Announce and CreateSession2 (>256 ports).** USRM 2.1.3 has support for GQIv1.5-enabled QAMs. See ***Appendix D: GQI v1.5 Requirements and Settings*** (on page 21) for details.
- **Support for OCAI version 2.** USRM 2.1.3 supports OCAI version 2 which allows the USRM to obtain PowerKEY encryption information from a configured CA Manager, such as the RCAS, that also supports OCAI version 2.

- **Netcrypt support for VOD.** USRM 2.1.3 allows the addition of netcrypt devices as ERM resources to provide PowerKEY encryption on non-encrypting GQI QAM devices.
- **New web server look and feel.** USRM 2.1.3 features faster loading and support for large trees. Clicking on the splitter bar between the tree and content area now resizes the tree window to fit all tree elements without scrolling. You can now also search in the tree for specific titles using the search box at the top of the tree.
- **New Web pages for VodSm.** These new pages are for control and monitoring of VOD Session Management. See ***Appendix E: VodSm Web Pages*** (on page 22) for details.
- **Increased Max Service Group** to 2500 for an integrated VSM/ERM for VOD-only services. SDV max service groups remains 300 per USRM.
- **New tools – vodsessquery, ermtail, perftail.** See ***Appendix A: New Script Usage in opt/usrm/linux-tools*** (on page 12) for details.
- **MSA logging support.** USRM 2.1.3 supports MSA logging. Logs are created and stored in the /opt/msa/msa_logs directory on the VSM. These are configured under VodSm on the configuration page.
- **Resource Device Select Mode: Priority Encrypt vs. Priority Best Fit.** USRM 2.1.3 offers two modes of device selection, which can be set on the ERM's ResourceManager.Configuration page. The default setting is Priority Encrypt. In this mode, requests will use all available (native) PowerKey encrypting devices first to satisfy VOD requests and use clear QAMs with netcrypts last. Likewise, in this mode, SDV session requests use all clear QAM bandwidth first, saving the PowerKey encrypting devices for last. A new setting called PriorityBestFit uses all devices more or less equally, and according to the rules of a) the ResourceAllocationMode selected, and b) priority based on the location of the QAM entry in the Resource Manager list.

Enhancements and Corrections

Release 2.1.3 offers the following enhancements and corrections:

- The software has been enhanced to require three failed status queries before asserting failure. This will prevent unnecessary QAM or USRM audits in the case of temporary network glitches or outages.
- Increased RFGW-1 and GqiQam max sessions per carrier from 32 to 40. See ***Installation and Upgrade Guidelines*** (on page 6) and ***Downgrade Guidelines*** (on page 11) for details.
- Added ability to delete programs from the database that are not in the config file.
- Removed ability to add programs that do not belong to service groups on the server.
- Added new GqiQam36 model to support a 24x36 QAM device.

- Enhanced the code to properly detect NDS encryption type from the adaptation header of the request message for JCAS set-tops.
- Enhanced the code to properly select the correct encryption type when receiving multiple types of access criteria in a vasp's AddResourceRequest.
- Added a provisionable startup delay to GqiQams, similar to the existing setting on GQAMs.
- The application provides a service level setting for Encryption Overhead Bandwidth, if desired.
- The software has been updated to fix tree problems on DNCS Firefox versions.
- TTL default has been changed to 32.
- Resource type CaMgrDncs has been renamed to CaManagerPk. Systems running USRM 2.0 or later will need to rename the persistdata files upon upgrading to USRM 2.1.3. See ***Appendix F: Conversion from CaMgrDNCS to CaManagerPK*** (on page 24) for details and procedure.
- The software has been enhanced to support Fabrix Access Criteria for CVC.
- Changes have been made to support minimum SCGID and activation time. SCG_provision parameters have also been rearranged to satisfy RFGW-1.
- The software has been enhanced to properly handle RFGW-1 GbE ports during import.
- Implemented version 1.6 of TWC Log2 specification (added event codes 95, 96).
- SimulCrypt Synchronizer or SCS deprovision before session release. This will send an explicit SCG_deprovision message to tear down the SCG infrastructure.
- Deliver ISK only if a create session is successful.
- Local sync will occur on a VSM any time that the VSM is reset. This is in addition to the normal sync operations.
- Enhancements made for hanging connections. First found with connections to a broken BMS.
- Enhanced the MCMIS sync times.
- Changes made to properly pass all copy protection settings.
- Increased the ulimit as set by default by Linux. By default, Linux provides only 1024 file handles. In a system with more than 200 QAMs and other devices in the Resource Manager, we can exceed this number. Accordingly, a change included in the 2.1.3-9 release increases this limit to 4096 file handles.

- In the case of a network outage where multiple servers are recovering, the USRM has been enhanced to prevent a recovering primary server from connecting to a standby server that is not replacing the recovering primary. When a primary server recovers, it typically connects to the active standby in a mode referred to as transition mode, in order to get the current database and then transition to the online state. The software is enhanced so that a standby server will reject requests from a primary server that it is not currently replacing.

Open Issues and Known Restrictions

Release 2.1.3 has the following known open issues and restrictions:

- No commas, periods, or spaces can be used in any device name on the USRM.
  - Workaround: If multiple words are required, use an underscore in the place of the comma, period, or space.
- For users of Internet Explorer, logging out of the USRM WebUI requires the browser to be fully closed for logout to occur, as Internet Explorer (IE) caches the user.
- The version of Firefox included with DNCS 4.2 is not completely compatible with the enhanced WebUI used with 2.1.3.
  - Workaround: use IE or Firefox from an alternate source to view and manipulate the USRM WebUI.
- During initial configuration or any other operation that requires adding a large number of high density QAMs (e.g. 72 TSIDs or more) to a USRM database via a config file, we recommend adding a maximum of 15 QAMs per config file.
  - Workaround: Use the new spreadsheet (CSV) import feature.
- During Service Group migration or any other operation that requires removing a large number of Service Groups containing 6000 or more STBs from a USRM database via a config file, we recommend removing a maximum of 20 SGs per config file.
- The popup box for Server Sip Timeout states that the valid range is from 1 to 99999, but the field is actually limited to 10 to 99999.

Installation and Upgrade Guidelines

General Notes

An FTP or SSH server is required to download new software to the USRM.

Installation Requirements

Before performing the upgrade procedure, make sure the following requirements are met:

- The desired USRM software release has already been uploaded to the FTP server.
- If the DNCS is being used as the FTP or SSH server, make sure that the desired USRM release is located in the /export/home/dncs directory.
- If the DNCS is being used as an SSH server, make sure that the Provisionkeys application has been run on each of the servers.
- A backup of the existing USRM database has been completed prior to upgrading to be prepared in case a rollback to the previous version is desired. A backup can be created from any directory in the USRM by typing **usrmbackup** at the command line prompt. The backup file will be stored in the /root directory. We recommend that this backup file be copied to and saved in a secure location in case it is needed in the future.

Note: A downgrade from USRM 2.1.3 to USRM 1.x requires the installation of a 1.x database as part of the procedure. If a 1.x database does not exist, all persistdata will be lost during the downgrade.

New Requirement

With the introduction of VOD Session Management capabilities to the USRM, it is now required to keep track of all traffic on all GigE ports on all QAMs. With this in mind, we now require that the Edge Input IP address(es) be included for all QAMs.

If you have configuration files, the Edge Input address(es) should be added to these files.

Supervised vs. Auto Mode

USRM servers running the SdvSm application in a Cisco DNCS system should be run in Supervised mode. In this mode, the SDV Manager, which is part of the DNCS software release, provisions the USRM with information including the SDV Offered Programs table via SNMP, and also manages the servers from an HA perspective. USRM servers that run the VodSm application only should be run in Auto mode. High Availability still exists in Auto mode, but does not have a third party manager running it. All USRMs that are not in a Cisco DNCS environment should run in Auto mode.

Release 2.1.3 from Release 2.0 – 2.1.1 Upgrade Procedure

A database change between USRM 2.0 and USRM 2.1.3 requires that the connection between the Primary and Standby Servers be removed during the upgrade. Renaming of the persistdata files for CA Managers between 2.1.1 and 2.1.3 requires a special step detailed in the procedure below (step 4).

1. If you have not done so already, complete the steps listed under **Installation Requirements** above.
2. Download the software to the USRM Standby Server using *one* of the following procedures, a or b, as appropriate.
   a. If you typically upgrade your USRM from the USRM Software Upgrade page:
      - From the Standby Server WebUI, select **Platform -> ConfigManager -> Software Upgrade** page.
      - Select **DownloadProtocol = SSH** from the drop down menu.
      - Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString and ImageExecuteString fields with the appropriate information.
      - Click **Commit Changes** to save your changes.
      - Under InitiateDownload, select **Download**.
      - Click **Commit Changes** to download the software to the Standby USRM.
   b. If you typically upgrade your USRM from the DNCS SDV Server page:
      - From the DNCS, terminate the Standby Server process.
      - From the DNCS, terminate the USRM Server process, preferably from the USRM WebUI System.Reset page.

        Note: The Standby Server remains terminated until all of its Primary servers have been upgraded and rebooted.

3 Download the software to the USRM Primary Servers using *one* of the following procedures, a or b, as appropriate.

a If you typically upgrade your USRM from the USRM Software Upgrade page:

- From the Standby Server WebUI, select **Platform -> ConfigManager -> Software Upgrade** page.
- Select **DownloadProtocol = SSH** from the drop down menu.
- Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString and ImageExecuteString fields with the appropriate information.
- Click **Commit Changes** to save your changes.
- Under InitiateDownload, select **Download**.
- Click **Commit Changes** to download the software to the Standby USRM.

b If you typically upgrade your USRM from the DNCS SDV Server page:

- From the DNCS, terminate the Standby Server process.
- From the DNCS, terminate the USRM Server process, preferably from the USRM WebUI System.Reset page.

  Note: The Standby Server remains terminated until all of its Primary servers have been upgraded and rebooted.

4 Rename the CaMgrDncs persistdata files as follows:

a Open an ssh session to the Primary Server and go to the /opt/usrm/persistdata directory.

b Type the following to get a list of existing CA Manager files:

```
[persistdata]#  ls –ltr | grep CaMgrDncs
```

A (list of) file(s) will be returned with the following format, where xyz is the name assigned to the particular CA Manager CaMgrDncs.xyz.bin.

c Change the file name as shown below.

```
[persistdata] mv CaMgrDncs.xyz.bin CaManagerPk.xyz.bin
```

d Make the change for each CA Manager on the USRM, if more than one exists.

5 Install the rpm on the Primary Server as follows:

a In the same ssh session, go to the /tmp directory and manually install the rpm.

```
[usrm]# cd /tmp
[tmp]# rpm -Uvh usrm-2.1.3-8.i386.rpm --force
```

b Go to the /opt/usrm directory and verify that the rpm was successfully installed.

```
[tmp]# cd /opt/usrm
[usrm]# ./usrm –x
Universal Session & Resource Manager (USRM)
(c) Copyright 2006-2008 Cisco Systems, Inc., All Rights Reserved.
Configuration is VALID.
USRM Version 2.1.3-8
```

6 Start the PrimaryServer process as follows:

a From the ssh shell session in the /opt/usrm directory, start the usrm process in auto and daemon mode by typing *one* of the following, depending on whether the servers are in auto or supervised mode.

```
[usrm]# ./usrm  --auto -d
[usrm]# ./usrm  --supervised -d
```

7 After all primary USRMs in the cluster have been upgraded, install the rpm on the Standby Server as follows:

a Open an ssh session to the Standby Server, and then go to the /tmp directory and install the rpm manually.

```
[usrm]# cd /tmp
[tmp]# rpm -Uvh usrm-2.1.3-8.i386.rpm --force
```

b Go to the /opt/usrm directory and verify that the rpm was successfully installed.

```
[tmp]# cd /opt/usrm
[usrm]# ./usrm -x
Universal Session & Resource Manager (USRM)
(c) Copyright 2006-2008 Cisco Systems, Inc., All Rights Reserved.
Configuration is VALID.
USRM Version 2.1.3-8
```

8 Start the Standby Server process.

Important: Complete the upgrade on ALL primary USRMs before proceeding.

a From the ssh shell session in the /opt/usrm directory, start the usrm process in Auto and daemon mode by typing *one* of the following, depending on whether the servers are in auto or supervised mode.

```
[usrm]# ./usrm --auto -d
[usrm]# ./usrm  --supervised -d
```

Release 2.1.3 from Release 1.6 or 1.7 Upgrade Procedure

A database change between USRM 1.7 and USRM 2.1.3 requires that the connection between the Primary and Standby Servers be removed during the upgrade.

1 If you have not done so already, complete the steps listed under **Installation Requirements** above.

2 Download software to the USRM Standby Server as follows:

a From the Standby Server WebUI, select **Platform -> ConfigManager -> Software Upgrade** page.

b Select **DownloadProtocol = SSH** from the drop-down menu.

c Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString and ImageExecuteString fields with the appropriate information.

d Click **Commit Changes** to save your changes.

e Under InitiateDownload, select **Download**.

f Click **Commit Changes** to download the software to the Standby USRM.

3 Terminate the Standby Server process, preferably from the USRM WebUI System.Reset page.

Note: The Standby Server remains terminated until all of its Primary servers have been upgraded and rebooted.

4 Download and install the software to the USRM Primary Servers as follows:

- **a** From each Primary Server WebUI, select **Platform -> ConfigManager -> Software Upgrade** page.
- **b** Select **DownloadProtocol = SSH** from the drop-down menu.
- **c** Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString, and ImageExecuteString fields with the appropriate information.
- **d** Click **Commit Changes** to save your changes.
- **e** Under InitiateDownload, select **DownloadInstall**.
- **f** Click **Commit Changes** to download the software to the USRM.

  Note: The DownloadInstall option will cause the server to reset after the download is complete.

5 Install the rpm on the Standby Server as follows:

- **a** Open an ssh session to the Standby Server, and then go to the /tmp directory and manually install the rpm.

  [usrm]# cd /tmp

  [tmp]# rpm -Uvh usrm-2.1.3-8.i386.rpm --force
- **b** Go to the /opt/usrm directory and verify that the rpm was successfully installed.

```
[tmp]# cd /opt/usrm
[usrm]# ./usrm -x
Universal Session & Resource Manager (USRM)
(c) Copyright 2006-2008 Cisco Systems, Inc., All Rights Reserved.
Configuration is VALID.
USRM Version 2.1.3-8
```

- **c** Start the Standby Server process.

  Important: Complete the upgrade on *all* primary USRMs before proceeding.
- **d** From the ssh shell session in the /opt/usrm directory, start the usrm process in Auto and daemon mode by typing *one* of the following, depending on whether the servers are in auto or supervised mode.

```
[usrm]# ./usrm --auto -d
[usrm]# ./usrm  --supervised -d
```

Release 2.1.3 from Release 1.5 (or Earlier) Upgrade Procedure

A direct upgrade from USRM 1.5 to USRM 2.1.2 or greater is not supported. An interim upgrade to USRM 1.6 or later is required. Refer to previous release notes for those versions.

Downgrade Guidelines

Database changes between USRM 1.7 and USRM 2.1.3 require that the connection between the Primary and Standby Servers be removed during the downgrade. Also, all sessions must be removed on RFGW-1 and GQI QAMs. Lastly, any QAM that was created after the upgrade to USRM 2.1.3 will have to be recreated after the downgrade (it will not be in the old persistdata files).

Downgrading from USRM 2.1.3 to USRM 1.7

Perform the following procedure to downgrade from USRM 2.1.3 to USRM 1.7.

1. Locate the servers' previous USRM 1.7 database that was saved prior to the upgrade and place them in the servers' root directories, if they are not already there.
2. Download the software to each server according to the directions in the ***Installation and Upgrade Guidelines*** (on page 6).
3. Terminate the Standby Server.
4. On each Primary Server, release all sessions on all RFGW-1 and GQI QAMs.
5. Terminate the Primary Server.
6. Restore the USRM 1.7 persistdata files. Open an ssh session to the server and type the following from any directory:
   ```
   usrmrestore /root/goqam.tar.bz2
   ```
7. Install the rpm on the Primary Server.
8. Start up the Primary server.
9. After all Primary servers in a cluster are back online, open an ssh session to the standby server and install the rpm.
10. Start up the Standby Server.

Appendix A: New Script Usage in opt/usrm/linux-tools

This appendix describes scripting commands available with USRM Release 2.0.

USRM Platform

usrmbackup

This command creates a USRM database backup and causes the following files and directories to be TARed, compressed, and saved in the root directory:

- opt/usrm/ConfigFiles
- opt/usrm/persistdata
- home/dncs
- etc/sysconfig/network-scripts
- etc/sysconfig/network
- etc/hosts

You can run this command from any directory by typing **usrmbackup**. We recommend that you copy the backup file to a secure location in case of a catastrophic failure of the USRM hardware.

usrmrestore

Use this command to reinstall previously stored backup files onto the USRM.

This script requires you to specify the full path and filename of the backup file to be used. For example, the following usage restores the filename USRM01.25Aug2009.tar.bz2, which is stored in the root directory:

```
usrmrestore /root/USRM01.25Aug2009.tar.bz2
```

VOD

Perftail

Use this command to monitor the performance of the VOD requests. The results show the number of VOD Create and Release requests, how many succeeded and failed and why, and how many VOD sessions were active, over a series of one-minute intervals. The enumerated failures are Error 18 (no resource available), Error 32 (BMS could not build the session) and Error 6 (No Video PID in the PMT).

```
Tailing /opt/usrm/EventLog/13Jul2011_000001.txt ...

Time,ClntReqs,ClntCnfs,Succs,Fails,Err18s,Err32s,Err6s,ClntRelReqs,ClntRelCnfs,CS
ipMsgs,ActiveSessions

13:46,102,92,86,6,6,0,0,80,80,0,26

13:47,269,279,255,24,24,0,0,320,320,0,215

13:48,146,146,134,12,12,0,0,82,82,0,79
```

You can also use this script to evaluate a log file. However, the ActiveSessions count will not be correct, as this parameter is pulled real time from the running USRM software and not the log files. To use this script with a log file, use the following format:

```
Perftail <log filename>
```

You can also specify that this command run for a specified time period by using the following syntax:

```
perftail [-s <starttime>][-e <endtime>] [<logfile>]
```

sesstail

This command gives a listing of SSP Sessions for VOD. You can use this script to tail sessions in real time or to evaluate an existing log file. When evaluating a log file, you can specify start and end times to narrow the results of the evaluation. You must provide the full path to the log file to be evaluated.

The following are usage examples:

```
sesstail –s 10:00 –e 11:00 /opt/usrm/EventLog/09Sep2009_000000.txt

sesstail /opt/usrm/EventLog/09Sep2009_000000.txt

++++ 380ca8c00499/21 ++++

 RmCreateSession                  2009/09/09 07:44:57.775

 SspServerTxSISC                  2009/09/09 07:44:57.775  Rsp=0 TID=4110421
SGID=1194 nSes=1 uBW=3750000

PN=1097

 RmCmdExec                        2009/09/09 07:44:57.775  Cmd=CreateSession
RID=172.16.4.78 Tid=668

 RmCmdSuccess                     2009/09/09 07:44:57.800  Cmd=CreateSession
RID=172.16.4.78

 SspServerRxServerReleaseRequest  2009/09/09 07:45:07.806  TID=3eb869 reason=1

 RmSessionRelease                 2009/09/09 07:45:07.806  RID=172.16.4.78

 SspServerTxServerReleaseConfirm  2009/09/09 07:45:07.807  TID=3eb869 response=0

 RmCmdExec                        2009/09/09 07:45:07.807  Cmd=DeleteSession
RID=172.16.4.78 Tid=1

 RmCmdSuccess                     2009/09/09 07:45:07.847  Cmd=DeleteSession
RID=172.16.4.78

 ++++ 001d09fa6301/716599 ++++

 RmCreateSession                  2009/09/09 00:46:13.919

 RmCmdExec                        2009/09/09 00:46:13.919  Cmd=CreateSession
RID=172.16.4.78

 RmCmdSuccess                     2009/09/09 00:46:13.946  Cmd=CreateSession
RID=172.16.4.78

 RmSessionRelease                 2009/09/09 00:46:17.932  RID=172.16.4.78

 RmCmdExec                        2009/09/09 00:46:17.932  Cmd=DeleteSession
RID=172.16.4.78 Tid=1

 RmCmdSuccess                     2009/09/09 00:46:17.967  Cmd=DeleteSession
RID=172.16.4.78
```

sspsistail

This command gives a listing of SSP-SIS sessions. Use this tool to display real-time SSP-SIS operations or to evaluate an event log file.

The following are examples of both usages:

```
ssptail

sspsistail

 ++++++++++ 380ca8c003de/8 ++++++++++

RmCreateSession    2009/09/09 07:43:23.980 (RID=172.16.4.78 chan=7
EdgeIn=0.0.0.0)

SspServerTxSISC    2009/09/09 07:43:23.980 (RC=0 PN=1010)

 ++++++++++ 380ca8c003df/9 ++++++++++

SspServerRxSISR    2009/09/09 07:43:24.481 (SgId=1194 BW=3750000)

RmCreateSession    2009/09/09 07:43:24.482 (RID=172.16.4.78 chan=7
EdgeIn=0.0.0.0)

SspServerTxSISC    2009/09/09 07:43:24.482 (RC=0 PN=1011)
```

Use the following command to see data from a specific event log.

```
sspsistail /opt/usrm/EventLog/31Aug2009_000000.txt
```

vermtail

This command gives the statistics of Channel changes and QAM operations. Use this tool to display real-time channel change operations or to evaluate an event log file.

The following are examples of both usages:

```
Real time log tail.

vermtail

++++++++++ 0000000400 ++++++++++

VermServerRxSETUP    2009/08/31 14:25:44.031 (Service-Group: 1194
bit_rate=3750000)

RmCreateSession      2009/08/31 14:25:44.032 (sess=001d09fa6301/547245
RID=172.16.4.78 chan=6

EdgeIn=0.0.0.0)

VermServerTxRESPONSE 2009/08/31 14:25:44.032 (RC= OK)

 ++++++++++ 0000000804 ++++++++++

VermServerRxSETUP    2009/08/31 14:25:46.038 (Service-Group: 1194
bit_rate=3750000)

RmCreateSession      2009/08/31 14:25:46.038 (sess=001d09fa6301/547246
RID=172.16.4.78 chan=6

EdgeIn=0.0.0.0)

VermServerTxRESPONSE 2009/08/31 14:25:46.038 (RC= OK)

 ++++++++++ 0000000905 ++++++++++

VermServerRxSETUP    2009/08/31 14:25:46.540 (Service-Group: 1194
bit_rate=3750000)

RmCreateSession      2009/08/31 14:25:46.540 (sess=001d09fa6301/547247
RID=172.16.4.78 chan=7

EdgeIn=0.0.0.0)
```

```
VermServerTxRESPONSE 2009/08/31 14:25:46.540 (RC= OK)
```

```
vermtail /opt/usrm/EventLog/31Aug2009_000000.txt
```

vodsessquery

This command, run from an SSH shell on the VSM, prints all log messages on VSM, ERM, and RCAS (optional) that pertain to a given VOD session. You can run the command **vodsessquery <sessionId>** from any directory. An example is shown below.

To include the RCAS in the result, add the option **–r** before the session ID. Optionally, you can specify a date if the date of the session of interest is known. This will shorten the time it takes to search for the session.

You can find the various usages for this command using the following command:

Vodsessquery -h.

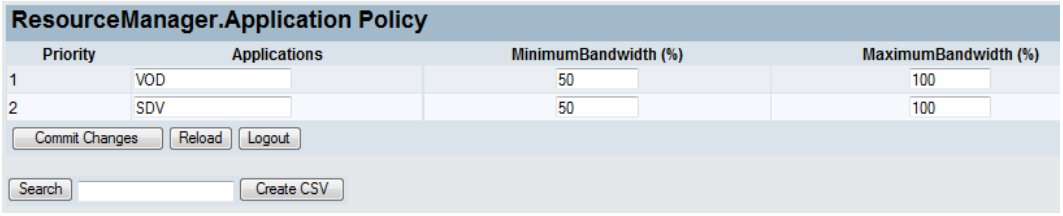
```
[root@VSM-02 linux-tools]# vodsessquery 0002de0d2614/1302298896
Checking VSM Logs for session 0002de0d2614/1302298896
Checking ERM Logs on server 192.168.12.153 for session 0002de0d2614/1302298896
Warning: Permanently added '192.168.12.153' (RSA) to the list of known hosts.
Checking RCAS Logs for session 00:02:DE:0D:26:14/1302298896
Skipping RCAS Log analysis, use the -r flag to enable
VSMLOG: 2011/04/08 17:41:36.392 SspUdpServerRxClntSessSetupReq,StbIp=192.168.12.192,StbMac=0x0002de0d2614,SesId=0002de0d2614/1302298896,VodIp=192.168.12.192,TID=1621114,casId=0
VSMLOG: 2011/04/08 17:41:36.392 VodSmClientRequest,StbIp=192.168.12.192,StbMac=0x0002de0d2614,SesId=0002de0d2614/1302298896,Server=192.168.12.192,TID=1621114
VSMLOG: 2011/04/08 17:41:36.392 VodSmServerSessionSetupIndication,StbIp=192.168.12.192,StbMac=0x0002de0d2614,SesId=0002de0d2614/1302298896,Server=192.168.12.192,TID=340060454,SessIndex=39270
VSMLOG: 2011/04/08 17:41:36.392 SspTcpServerTxSessionSetupIndication,StbIp=192.168.12.192,StbMac=0x0002de0d2614,SesId=0002de0d2614/1302298896,VodIp=192.168.12.192,TID=340060454
VSMLOG: 2011/04/08 17:41:36.411 SspTcpServerRxServerAddResReq,Server=192.168.12.192,SGID=15,BW=3750000,SesId=0002de0d2614/1302298896,TID=116725992,CasId=3584,tsid=0,MPN=0
VSMLOG: 2011/04/08 17:41:36.411 VodSmResourceRequest,SesId=0002de0d2614/1302298896,SGID=15,BW=3750000,CasId=3584,edgeCaInfoLength=0
VSMLOG: 2011/04/08 17:41:36.411 DiscSvcsTxResReq,sgid=15,bw=3750000,tid=340060454,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.412 DiscSvcsRxResReq,sgid=15,bw=3750000,tid=340060454,usrm=192.168.12.222,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.412 RmBwReq,SGID=15,BW=3750000,Svc=Demand,CAS=3584,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.413 RmResourceSelect,RID=172.16.4.8,TSID=1092,chan0=87,casId=3584,allocBW=3750000,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.414 RmCaMgrSelect,SesId=0002de0d2614/1302298896,CaMgr=192.168.6.1
ERM153: 2011/04/08 17:41:36.414 RmCmdQueue,Cmd=GetEncryptInfo,RID=192.168.6.1,queueDepth=1,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.414 RmCmdExec,Cmd=GetEncryptInfo,RID=192.168.6.1,Tid=211532978,SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:41:36.425 DiscSvcsRxResConf,status=success(0),sgid=15,bw=3750000,tid=340060454,destUsrm=192.168.12.153,SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:41:36.425 VodSmResourceReady,SesId=0002de0d2614/1302298896,TID=340060454,status=0
VSMLOG: 2011/04/08 17:41:36.425 SspTcpServerTxAddResConf,TID=116725992,Server=192.168.12.192,SesId=0002de0d2614/1302298896,resp=0,SGID=15,Udp=22730,EdgeIn=172.16.15.65,Pn=537,Freq=423000000,Tsid=1092
VSMLOG: 2011/04/08 17:41:36.425 SspTcpServerRxServerSessSetupResp,Server=192.168.12.192,TID=340060454,Resp=0,SesId=0002de0d2614/1302298896,privateDataLen=65
VSMLOG: 2011/04/08 17:41:36.425 VodSmServerSessSetupResp,TID=340060454,Resp=0,SesId=0002de0d2614/1302298896,edgeCaInfoLength=0,privateDataLen=65
VSMLOG: 2011/04/08 17:41:36.425 SspUdpServerTxClientSessSetupConf,TID=1621114,Resp=0,Client=192.168.12.192,Freq=423000000,Pn=537,Mod=16,SesId=0002de0d2614/1302298896,PrivateDataLen=65,casId=3584
ERM153: 2011/04/08 17:41:36.426 RmCmdSuccess,Cmd=GetEncryptInfo,RID=192.168.6.1,CmdTime=11ms,SesId=0002de0d2614/1302298896,Tid=211532978
ERM153: 2011/04/08 17:41:36.426 RmGetEncryptInfoSuccess,status=0,encryptorCaInfoLength=427,clientCaInfoLength=301,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.426 DiscSvcsTxResConf,status=success(0),sgid=15,bw=3750000,tid=340060454,destUsrm=192.168.12.222,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.426 RmCreateSession,SesId=0002de0d2614/1302298896,RID=172.16.4.8,chan0=87,MPN=537,Bw=3750000,EdgeIn=172.16.15.65,EdgeInPort=1
ERM153: 2011/04/08 17:41:36.426 RmCmdQueue,Cmd=CreateSession,RID=172.16.4.8,queueDepth=1,SesId=0002de0d2614/1302298896,chan0=87,MPN=537,BW=3750000,GDA=0.0.0.0,UDP=22730
ERM153: 2011/04/08 17:41:36.426 RmResourceReady,status=0,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36.426 RmCmdExec,Cmd=CreateSession,RID=172.16.4.8,Tid=340060454,SesId=0002de0d2614/1302298896,chan0=87,MPN=537,BW=3750000,GDA=0.0.0.0,UDP=22730
ERM153: 2011/04/08 17:41:36.428 RmCmdSuccess,Cmd=CreateSession,RID=172.16.4.8,CmdTime=2ms,SesId=0002de0d2614/1302298896,chan0=87,MPN=537,BW=3750000,GDA=0.0.0.0,UDP=22730,Tid=340060454
VSMLOG: 2011/04/08 17:42:17.025 SspUdpServerRxClientReleaseRequest,Client=192.168.12.192,TID=116726392,SesId=0002de0d2614/1302298896,PrivateDataLen=0
VSMLOG: 2011/04/08 17:42:17.025 VodSmClientReleaseRequest,Client=192.168.12.192,TID=116726392,Reason=0,SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:42:17.025 VodSmReleaseSession,SesId=0002de0d2614/1302298896,sessionIndex=39270
VSMLOG: 2011/04/08 17:42:17.025 DiscSvcsTxRelReq,TID=340062230,SesId=0002de0d2614/1302298896,retryCount=3,ermIp=192.168.12.153
VSMLOG: 2011/04/08 17:42:17.025 VodSmClientReleaseConfirm,Client=192.168.12.192,TID=116726392,Resp=0,SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:42:17.025 SspUdpServerTxClientReleaseConfirm,TID=116726392,Resp=0,Client=192.168.12.192,SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:42:17.025 VodSmServerReleaseIndication,Server=192.168.12.192,TID=116726392,Reason=0,SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:42:17.025 SspTcpServerTxServerReleaseIndication,Server=192.168.12.192,TID=116726392,SesId=0002de0d2614/1302298896,reason=0,PrivateDataLength=0
VSMLOG: 2011/04/08 17:42:17.025 DiscSvcsRxRelConf,status=success(0),ermIp=192.168.12.154,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:42:17.026 DiscSvcsRxRelReq,sesId=0002de0d2614/1302298896,retryCount=3,srcIp=192.168.12.216
ERM153: 2011/04/08 17:42:17.026 RmSessionRelease,RID=172.16.4.8,SesId=0002de0d2614/1302298896,chan0=87
ERM153: 2011/04/08 17:42:17.026 RmCmdQueue,Cmd=DeleteSession,RID=172.16.4.8,queueDepth=2,SesId=0002de0d2614/1302298896,chan0=87
ERM153: 2011/04/08 17:42:17.026 DiscSvcsTxRelConf,status=success(0),User=192.168.12.222,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:42:17.026 RmCmdExec,Cmd=DeleteSession,RID=172.16.4.8,Tid=211533178,SesId=0002de0d2614/1302298896,chan0=87
ERM153: 2011/04/08 17:42:17.035 RmCmdSuccess,Cmd=DeleteSession,RID=172.16.4.8,CmdTime=8ms,SesId=0002de0d2614/1302298896,chan0=87,Tid=211533178

For further analysis, check the following logfiles on the appropriate servers:
VSMLOG:  /opt/usrm/EventLog/08Apr2011_000006.txt
ERMLOG:  /opt/usrm/EventLog/08Apr2011_000000.txt on 192.168.12.153
RCSLOG:  on 192.168.6.1
```

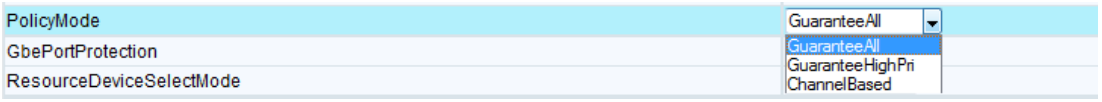
Appendix B: Policy

The simple video policy server that existed in prior versions of USRM 2.x. has been enhanced in USRM 2.1.3 with a new configuration setting in which the mode is explicitly configured. The modes are ChannelBased, GuaranteeAll, and GuaranteeHighPri.

You can enter and configure applications that will be governed by USRM Policy on the Resource manager under the ResourceManager.Application Policy tab. You can specify up to 16 separate applications for each USRM. For each application, you can also specify the minimum and maximum allowable bandwidth.

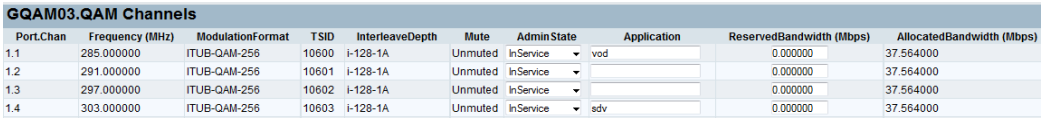


Once the applications are configured, you can specify the policy mode on the ResourceManager.Configuration page. You can choose one of three Policy Modes: Channel Based, Guarantee All, and Guarantee Higher Priority.



ChannelBased mode indicates that a QAM channel is configured for a specific application. Channel based should be used for siloed applications (i.e., specific TSIDs for VOD, specific TSIDs for SDV). If a TSID is not specified for a particular application, any application can use it on a first-come, first-serve basis. If Channel Based Mode is selected, the Minimum and Maximum Bandwidth settings on the Application Policy page are not necessary, and are ignored if they are set.

TSIDs are specified for each application on the ResourceManager.QAMs.QAM xyz.QAM Channels page. The example below shows a GQAM whose first carrier on output Port 1 is VOD-only, whose fourth carrier is SDV-only and whose second and third carrier can be used by either application.



Use **GuaranteeAll** or **GuaranteeHighPri** when QAM sharing between applications, such as VOD and SDV is enabled. Applications are allocated a specific percentage of total bandwidth. A percentage of minimum bandwidth and maximum bandwidth is specified for each application. These percentages apply to the total amount of bandwidth available to the service group. If a QAM or other edge device is OutOfService or otherwise unavailable, the USRM applies the percentages to the total amount of bandwidth available at the time of the service request.

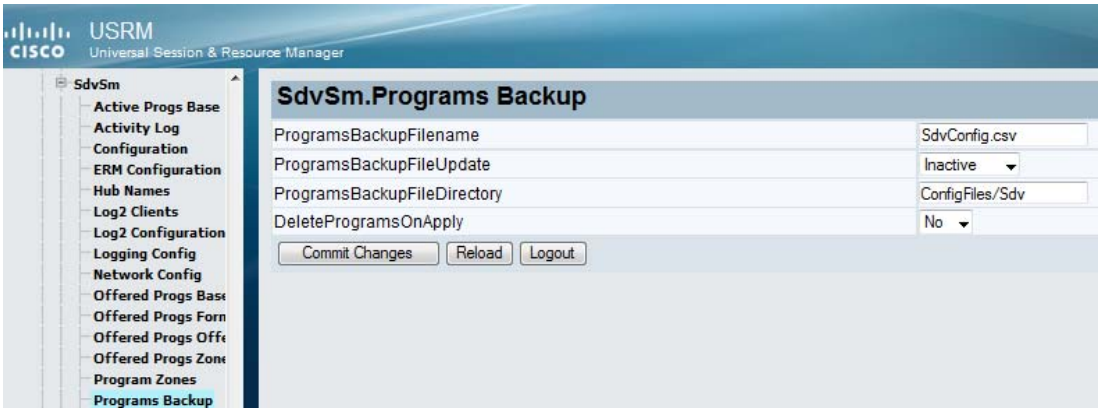
GuaranteeAll mode allows resource requests if all minimum bandwidth guarantee configurations can be satisfied.

GuaranteeHighPri mode allows resource requests if higher priority minimum bandwidth guarantee configurations are satisfied. The highest priority application (i.e., first in the list) will always get its requests satisfied, bandwidth permitting. Lower priority applications will then be satisfied if possible.

Appendix C: Spreadsheet Import and Export

In USRM 2.1.3, two directories are created on the USRM in the /opt/usrm/ConfigFiles directory, either manually by the user, or automatically upon writing a file for the first time. The ERM resource directory is called Qams; the SDV offered programs directory is called Sdv.

On the webUI, the spreadsheet import functionality can be accessed at ResourceManager.Resource Backup for the ERM QAM Resources, and Applications.SdvSm.Programs Backup for the SDV Offered Programs.



With Resource Backup, you can create a CSV file of all QAMs on a given server by selecting **Write** from the DeviceBackupFileUpdate drop-down menu. This file is written to the /opt/usrm/ConfigFiles/Qams directory. To view this file in Excel spreadsheet format, copy the file to a computer and open it in Excel. An example for a GQAM is shown below.

Server	MgmtIpAddr	GbePort	IpAddress	Virtual Address	RfPort	Service Group	Freq	TSID	Application	Usage	Freq	TSID	Application	Usage	Freq	TSID	Application	Usage	Freq	TSID	Application	Usage
Stuttgart	172.16.6.4	1	172.16.15.9		1	15	285	10600	vod	Enabled	291	10601		Enabled	297	10602		Enabled	303	10603	sdv	Enabled
					2	0	333	10604		Disabled	339	10605		Disabled	345	10606		Disabled	351	10607		Disabled
					3	0	525	10608		Disabled	531	10609		Disabled	537	10610		Disabled	543	10611		Disabled
					4	0	477	10612		Disabled	483	10613		Disabled	489	10614		Disabled	495	10615		Disabled

You can also read in a file that is located in the /opt/usrm/ConfigFiles/Qams directory and apply its settings by selecting **ReadApply** in the DeviceBackupFileUpdate drop-down menu. Prior to reading and applying a file's settings, you can preview the changes that will be made by selecting **Preview** from the drop-down menu. This causes the settings about to be changed to be printed to the Eventlog. You can then open an SSH session to the server and run **usrmlogtail**, filtering on ResourceBackupChange, to view these contents.

An example is shown below. In this case, the Admin States of the ports are being placed OutOfService.

```
usrmlogtail ResourceBackupChange
```

```
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.1,Value=15
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.2.1,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.2.2,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.2.3,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.2.4,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.3.1,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.3.2,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.3.3,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.3.4,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.4.1,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.4.2,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.4.3,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.4.4,Value=OutOfService
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0
2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0
```

Setting SendCmdsToDevice to **Yes** causes the USRM to provision the QAM devices with the settings in the CSV file. This only works for RFGW-1 QAMs.

Setting DeleteDevices to **No** causes the USRM to leave existing QAM resources in place when reading a file (ReadApply) whether they are in the file being read or not. If DeleteDevices is set to Yes and the USRM sees a QAM device in the USRM database that is not in the file being read, it will delete that device from the USRM database.

Programs Backup is similar to Resource Backup. The selections for ProgramsBackupFileDirectory are the same as for ResourceBackupFileDirectory (Write, ReadApply, and Preview). DeleteProgramsOnApply behaves similarly to DeleteDevices.

An example of the SDV Offered Programs table in Excel spreadsheet format is shown below.

SourceId	Name	ServiceGroup	Zone	SrcAddr1	SrcAddr2	SrcAddr3	DestAddr	Priority	B/W	Video	UdpPort	OfferState	AdminState
1216	HBO Comedy E							1				Dynamic	InService
				172.16.17.5	172.16.17.1	172.16.17.9	232.0.0.61		3.75	MPEG-2			InService
			4	172.16.17.5			232.1.1.16						InService
			5	172.16.17.9			232.2.2.16						InService
4032	SDV Cinemax HD2							1				Dynamic	InService
				172.16.17.1			232.0.1.32		15	MPEG-2	48304		InService
5056	Action Max 4							1				Dynamic	InService
				172.16.17.13			232.0.4.56		3.75	MPEG-2	48304		InService
1217	WMAX E							1				Dynamic	InService
				172.16.17.1	172.16.17.5	172.16.17.9	232.0.0.17		3.75	MPEG-2	48304		InService

Appendix D: GQI v1.5 Requirements and Settings

At the time of this writing, the only QAM that supports GQI v1.5 is the Arris D5 QAM. Contact your Arris representative for details on how to enable or disable announce messaging.

USRM Settings

1. Resource Manager "normal" logging mode will log success and failure announcements along with the source IP.
2. ResourceAdapter.GenericQamSrm "max" logging mode will give more details to the exact failure code(s).
3. Qam.Sessions page status column documents the source IP for a successful session create, or reports "failure" for an unsuccessful session create.

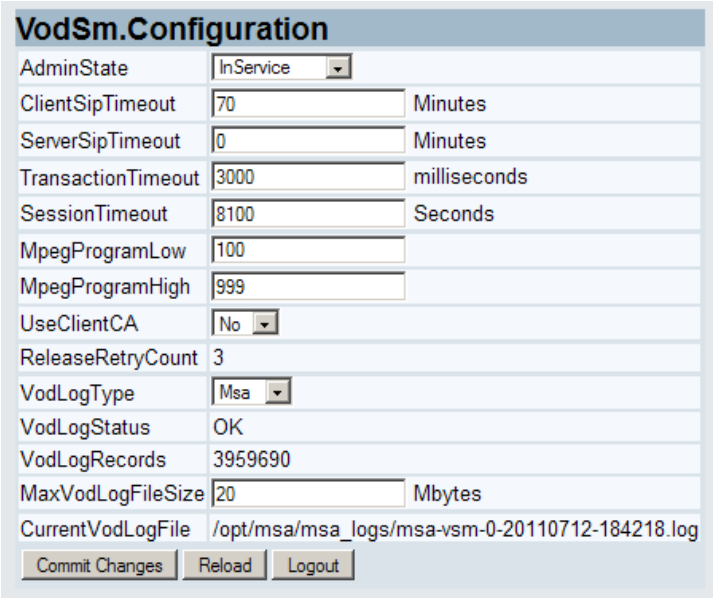
Appendix E: VodSm Web Pages

Use the VOD Session Manager (VodSm) configuration page to set the Session In Progress (SIP) timers for Clients and Server as well as the timeout for waiting for a response to a VOD session request.

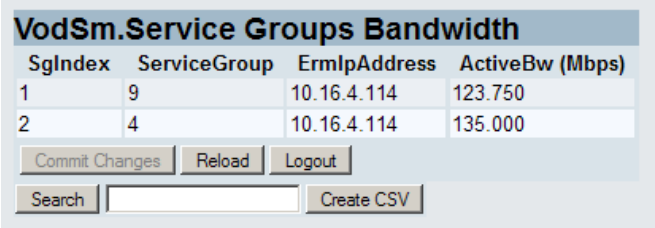
Use the SessionTimeout parameter to define a period of time that a session will be allowed to remain on a QAM before it is torn down due to a lack of SIPs.

Use the values for MpegProgram Low and High to define a range for VOD program numbers to help differentiate between SDV programs and VOD programs that may be built on a shared QAM.

Use the MaxVodLogFileSize field to limit the size of the created MSA log if the VodLogType parameter is set to Msa.



Use the Service Groups Bandwidth screen to get a snapshot of aggregate VOD BW usage for all service groups on this particular VSM at any point in time.



The Active Sessions screen displays a listing very similar to those on an SDV system showing all active VOD sessions. It shows the Session ID, Bandwidth used, Start Time for the session, Client IP Address, and the IP address of the BMS server servicing the session. There are also columns for Service group, Last Client SIP, and Last Server SIP.

VodSm.Active Sessions

Session	State	SessionId	AdminState	Bandwidth (Mbps)	StartTime	ClientAddress	ServerAddress	ErmAddress	ServiceGroupId	LastClientSIP	LastServerSIP
1021	Active	001bd7641238/1310562231	InService	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:51	2011/07/13 09:03:51
3911	Active	001bd763795e/1310562235	InService	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55
5101	Active	001bd763fe15/1310562231	InService	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:51	2011/07/13 09:03:51
9351	Active	001bd76378d4/1310562231	InService	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:51	2011/07/13 09:03:51
10201	Active	001bd7641ab1/1310562233	InService	3.750000	2011/07/13 09:03:53	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:53	2011/07/13 09:03:53
10711	Active	001bd765997c/1310562235	InService	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55
11901	Active	001bd7641b1c/1310562235	InService	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55
12411	Active	001bd763fddc/1310562236	InService	3.750000	2011/07/13 09:03:56	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:56	2011/07/13 09:03:56
13431	Active	001bd7659a61/1310562235	InService	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55
14451	Active	001bd763fd84/1310562236	InService	3.750000	2011/07/13 09:03:56	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:56	2011/07/13 09:03:56
15131	Active	001bd763fde1/1310562236	InService	3.750000	2011/07/13 09:03:56	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:56	2011/07/13 09:03:56
15471	Active	001bd765a19f/1310562231	InService	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:51	2011/07/13 09:03:51
15981	Active	001bd7659ad5/1310562234	InService	3.750000	2011/07/13 09:03:54	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:55	2011/07/13 09:03:55
16321	Active	001bd763fe58/1310562233	InService	3.750000	2011/07/13 09:03:53	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:53	2011/07/13 09:03:53

Appendix F: Conversion from CaMgrDNCS to CaManagerPK

Important: Perform this procedure only when upgrading from USRM Release 2.1.0 or 2.1.1 to Release 2.1.3-7 or above.

1. Terminate the USRM and its backup.
2. Rename the CaMgrDncs persistdata files.
3. Open an SSH session to the Primary Server and go to the /opt/usrm/persistdata directory.
4. Type the following to get a list of existing CA Manager files:
   ```
   [persistdata]#  ls –ltr | grep CaMgrDncs
   ```
5. A (list of) file(s) will be returned with the following format, where xyz is the name assigned to the particular CA Manager:
   ```
   CaMgrDncs.xyz.bin
   ```
6. Change the file name as shown below.
   ```
   [persistdata] mv CaMgrDncs.xyz.bin CaManagerPk.xyz.bin
   ```
7. Make the change for each CA Manager on the USRM, if more than one exists.

Note: See also the sections in ***Installation and Upgrade Guidelines*** (on page 6) for details on upgrading from releases prior to 2.1.3.

For 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.

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

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

September 2011 Printed in USA Part Number 4039593 Rev A